DES-7200

Basic Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 Command Line Interface Configuration

This chapter describes the method to use the command line interface(CLI). You can manage network devices by the command line interface.

This chapter covers the following topics:

- Command Mode
- Getting Help
- Abbreviating Commands
- Using **no** and **default** Options
- Understanding CLI Error Messages
- Using History Commands
- Using Editing Features
- Filtering and Looking Up CLI Output Information
- Using Command Alias
- Accessing CLI

1.1 Command Mode

The management interface of DES-7200 network devices falls into multiple modes. The command mode you are working with determines the commands you can use.

To list the usable commands in each mode, enter a question mark (?) at the command prompt.

After setting up a session connection to the network device management interface, you enter in the user EXEC mode first. In the user EXEC mode, only a few commands are usable with limited functions, for example, command **show**. The command results are also not saved.

To use all commands, enter the privileged EXEC mode with the privileged password. Then you can use all privileged commands and enter the global configuration mode.

Using commands in a configuration mode (for instance, global configuration or interface configuration) will influence the current configuration. If you have

saved the configuration information, these commands will be saved and executed when the system restarts. To enter any of the configuration modes, first enter the global configuration mode.

The following table lists the command modes, access methods, prompts, and exit methods. Suppose the equipment is named "*DES-7200*" by default.

Summary of main command modes:

Command mode	**Access method**	**Prompt**	**Exit or enter the next mode**	**Remark**
User EXEC	Log in.	DES-7200 >	Enter command **exit** to quit this mode. Enter command **enable** to enter the privileged EXEC mode.	Used for basic test and showing system information
Privileged EXEC	In the user EXEC mode, enter command **enable** .	DES-7200 #	To return to the user EXEC mode, enter command **disable**. To enter the global configuration mode, enter command **configure**.	Verify settings. This mode is password-protected.
Global configuration	In the privileged EXEC mode, enter command **configure terminal**.	DES-7200 (config)#	To return to the privileged EXEC mode, enter command **end** or **exit** or press Ctrl+C. To access the interface configuration mode, enter command **interface** with an interface specified. To access the VLAN configuration mode, enter command **vlan** *vlan_id*.	In this mode, you can execute commands to configure global parameters influencing the whole switch.
Interface configuration	In the global configuration mode, enter command **interface**.	DES-7200 (config-if)#	To return to the privileged EXEC mode, enter command **end** or press Ctrl+C. To return to the global configuration mode, enter command **exit**. Moreover, you need specify an interface in the **interface** command.	Configure various interfaces of the equipment in this mode.

Command mode	Access method	Prompt	Exit or enter the next mode	Remark
Config-vlan (Vlan Mode)	In the global configuration mode, enter command **vlan** vlan-id.	DES-7200 (config-vlan)#	To return to privileged EXEC mode, enter command **end** or press Ctrl+C. To return to the global configuration mode, enter command **exit**.	Configure VLAN parameters in this mode.

1.2 Getting Help

To obtain a list of commands that are available for each command mode, enter a question mark(?) at the command prompt. You can also obtain a list of command keywords beginning with the same character or parameters of each command. See the following table.

Command	Description
Help	Obtain the brief description of the help system under any command mode.
abbreviated-command-entry?	Obtain a list of commands that begin with a particular character string.(Do not leave a space between the keyword and question mark.) For example: DES-7200# **di?** dir disable
abbreviated-command-entry <Tab>	Complete a partial command name. For example: DES-7200# **show conf<Tab>** DES-7200# **show configuration**
Command ?	List a command's associated keywords.(Leave a space between the keyword and question mark.) For example: DES-7200# **show ?**
command keyword ?	List a command's associated arguments.(Leave a space between the keyword and question mark.) For example: DES-7200(config)# **snmp-server community ?** WORD SNMP community string

1.3 Abbreviating Commands

To abbreviate a command, simply enter part of the command that can uniquely identify the command.

For example, **show configuration** can be abbreviated as:

```
DES-7200# show config
```

If the entered command cannot be uniquely identified by the system, the system will prompt "Ambiguous command:".

For example, when you want to view the information about access lists, the following command is not complete.

```
DES-7200# show access
% Ambiguous command: "show access"
```

1.4 Using no and default Options

Almost all commands have the **no** option generally used to disable a feature or function or perform a reversed action of the command. For example, the **no shutdown** command turns on the interface, the opposite operation of the **shutdown** command. You can use the commands without the **no** option to enable the features that have been disabled or are disabled by default.

Most configuration commands have the **default** option that restores the command setting to its default. Most commands are disabled by default. In this case, the **default** and **no** options generally serve the same purpose. However, some commands are enabled by default. In this case, the **default** and **no** options serve different purposes, where the **default** option enables the command and restores the arguments to the default settings.

1.5 Understanding CLI Error Messages

The following table lists the error prompt messages that may occur when you use the CLI to manage equipments.

Common CLI error messages:

Error message	Meaning	How to obtain help
% Ambiguous command: "show c"	The switch cannot identify the unique command for you input insufficient characters.	Re-input the command with a question mark following the ambiguous word. The possible keywords will be listed.

Error message	Meaning	How to obtain help
% Incomplete command.	User has not input the required keywords or arguments.	Re-input the command with a space followed by a question mark. The possible keywords or arguments will be displayed.
% Invalid input detected at '^' marker.	The symbol "^" will indicate the position of the wrong words when user inputs a wrong command.	Input a question mark at the command prompt to show the allowed keywords of the command.

1.6 Using Historical Commands

The system records the commands you have input recently, which is very useful when you input a long and complex command again.

To re-execute the commands you have input from the historical records, perform the following operations.

Operation	Result
Ctrl-P or **Up**	Allows you to browse the previous command in the historical command records.
Ctrl-N or **Down**	Allows you to return to a more recent command in the historical command records.

Note

Standards-based terminals like VT100 series support arrow keys.

1.7 Using Editing Features

This section describes the editing functions that may be used for command line edit, including:

- Edit Shortcut Keys
- Sliding Window of Command Line

1.7.1 Editing Shortcut Keys

The following table lists the edit shortcut keys.

Function	Shortcut Key	Description

Function	Shortcut Key	Description
Move cursor in an editing line	Left direction key or Ctrl+B	Move the cursor to left by one character.
	Right direction key or Ctrl+F	Move the cursor to right by one character.
	Ctrl+A	Move the cursor to the beginning of the command line.
	Ctrl+E	Move the cursor to the end of the command line.
Delete the entered characters	Backspace	Delete the character to the left of the cursor.
	Delete	Delete the character where the cursor is located.
Scroll up by one line or one page	Return	Scroll up the displayed contents by one line and make the next line appear. This is used only before the end of the output.
	Space	Scroll up the displayed contents by one page and make the next page appear. This is used only before the end of the output.

1.7.2 Sliding Window of Command Line

You can use the sliding window to edit the commands that exceed the width of one line. When the editing cursor closes to the right border, the whole command line will move to the left by 20 characters. In this case, the cursor can still be moved back to the previous character or the beginning of the command line.

When editing a command line, you can move the cursor using the shortcut keys in the following table:

Function	Shortcut key
Move the cursor to the left by one character	Left direction key or Ctrl+B
Move the cursor to the head of a line	Ctrl+A
Move the cursor to the right by one character	Right direction key or Ctrl+F
Move the cursor to the end of a line	Ctrl+E

For example, the contents of the **mac-address-table static** command may exceed the screen width. When the cursor approaches the line end for the first time, the whole line move left by 20 characters, and the hidden beginning part is replaced by "$" on the screen. The line moves left by 20 characters when the cursor reaches the right border.

```
mac-address-table  static  00d0.f800.0c0c  vlan  1  interface
$tatic  00d0.f800.0c0c  vlan  1  interface  fastEthernet
```

```
$static  00d0.f800.0c0c  vlan  1  interface  fastEthernet  0/1
```

Now you can press **Ctrl+A** to return to the beginning of the command line. In this case, the hidden ending part is replaced by "$".

```
-address-table  static  00d0.f800.0c0c  vlan  1 interface  $
```

Note

The default line width on the terminal is 80 characters.

Combined with historical commands, the sliding window enables you to invoke complicated commands repeatedly. For details about shortcut keys, see Edit Shortcut Keys.

1.8 Filtering and Looking UP CLI Output Information

1.8.1 Filtering and Looking Up the Information Outputted by the Show Command

To look up the specified message in the information outputted by the **show** command, execute the following command:

Command	Description
DES-7200# **show** *any-command* | **begin** *regular-expression*	Look up the specified content from the information outputted by the **show** command and output all information of the first line that contains this content and subsequent lines.

Caution

1.You can execute **show** command in any mode.

2.The information to be looked up is case sensitive, and the following is the same.

To filter the specified content in the information outputted by the **show** command, execute the following commands:

Command	Description
DES-7200# **show** *any-command* **| exclude** *regular-expression*	Filter the content from the information outputted by the **show** command and output other information excluding the line that includes the specified content.

Command	Description
DES-7200#**show** *any-command* **| include** *regular-expression*	Filter the content from the information outputted by the **show** command and output the line that includes the specified content. Other information will be filtered.

Note

To look up and filter the contents outputted by the **show** command, it is necessary to input the pipeline sign (vertical line, "|") followed by lookup and filtration rules and contents (characters or strings). The contents to be looked up and filtered are case sensitive.

1.9 Using Command Alias

The system provides the command alias function. Any word can be specified as the alias of a command. For example, you can define the word "mygateway" as the alias of "ip route 0.0.0.0 0.0.0.0 192.1.1.1". Inputting this word is equal to inputting the whole string.

You can use one word to replace one command by configuring an alias for the command. For example, you can define an alias to represent the front part of one command, and then continue to enter the following part.

The command that an alias represents must run under the mode you have defined in the current system. In the global configuration mode, you can enter **alias?** to list all command modes that can configure alias.

```
DES-7200(config)#alias ?

  aaa-gs              AAA server group mode

  acl                 acl configure mode

  bgp                 Configure bgp Protocol

  config              globle configure mode

......
```

An alias supports help information. An alias appears with an asterisk (*) before it in the following format:

```
*command-alias=original-command
```

For example, in the EXEC mode, the alias "s" indicates the **show** command by default. Enter "s?" to obtain the help information on the command and the aliases beginning with 's'.

```
DES-7200#s?

*s=show  show  start-chat  start-terminal-service
```

If the command that an alias represents has more than one word, the command will be included by the quotation marks. As shown in the following example, configure the alias “sv” to replace the **show version** command in the EXEC mode.

```
DES-7200#s?

*s=show  *sv=”show version” show  start-chat

start-terminal-service
```

An alias must begin with the first character of the command line entered without any blank before it. As shown in the above example, the alias is invalid if you have inputted a blank before the command.

```
DES-7200# s?

show  start-chat  start-terminal-service
```

An alias can also be used to get the help information on obtaining command parameters. For example, the alias “ia" represents “ip address” in the interface configuration mode.

```
DES-7200(config-if)#ia ?

  A.B.C.D  IP address

  dhcp     IP Address via DHCP

DES-7200(config-if)#ip address
```

Here lists the parameter information after the command “**ip address**”, and replaces the alias with the actual command.

An alias must be inputted fully for use. Otherwise, it can not be identified.

Use the **show aliases** command to view the setting of aliases in the system.

1.10 Accessing CLI

Before using CLI, you need to use a terminal or PC to connect with the network device. Power on the network device. After the initialization of hardware and software, you can use CLI. If the network device is used for the first time, you can only connect the network device through the serial port (Console), which is referred to as out-band management. In addition, you can connect and manage the network device through Telnet virtual terminal by performing corresponding configuraitons. In either case, you can access the command line interface.

2 Basic Switch Management Configuration

2.1 Overview

This chapter describes how to manage our switches:

- Command Authorization-based Access Control
- Logon Authentication Control
- System Time Configuration
- Scheduled Restart
- System Name and Command Prompt Configuration
- Banner Configuration
- System Information Displaying
- Console Rate Configuration
- Telnet Configuration
- Connection Timeout Configuration
- Commands Execution in Batch in the Executable File
- Service Switch Configuration

Note For more information about the usage and description of the CLI commands mentioned in this chapter, see the *Reference Configuration of Switch Management Command*.

2.2 Command Authorization-based Access Control

2.2.1 Overview

A simple way to manage the terminals' access to a network is to use passwords and assign privileged levels. Password restricts access to a network or network devices. Privileged levels define the commands users can use after they have logged in to a network device.

From the perspective of security, password is stored in the configuration file. Password must be safe when the configuration file is transmitted, for example, over TFTP, across a network. Password is encrypted before being stored into the configuration file, and the clear text password is changed to the cipher text password. The **enable secret** command uses a private encryption algorithm.

2.2.2 Configuring Default Password and Privileged Level

No password at any level is configured by default. The default priviledged level is 15.

2.2.3 Configuring/Changing the Passwords at Different Levels

Our prodects provide the following commands for configuring or changing the passwords at different levels.

Command	Purpose
DES-7200(config)# **enable password** [**level** *level*] {*password* | *encryption-type encrypted-password*}	Set a static password. You can only set a level-15 password only when no level-15 security password is configured. If a non- level -15 password is set, the system will show a prompt and automatically convert it into a security password. If you have set the same level-15 static password as the level 15 security password, the system will show a warning message.

Command	Purpose
DES-7200(config)# **enable secret** [**level** *level*] {*encryption-type encrypted-password*}	Set the security password, which has the same function but better password encryption algorithm than the static password. For the purpose of security, it is recommended to use the security password.
DES-7200# **enable** [*level*], and DES-7200# **disable** [*level*]	Switch over between user levels. To switch over from a lower level to a higher level, you need to input the password for the higher level.

During the process of setting a password, the keyword "**level**" is used to define the password for a specified privileged level. After setting, it is only applicable for the users who are at that level.

2.2.4 Configuring Multiple Privileged Levels

By default, the system has only two password-protected levels: normal user (level 1) and privileged user (level 15). You can configure up to 16 hierarchical levels of commands for each mode. By configuring different passwords at different levels, you can use different sets of commands by different levels.

When no password is set for the privileged user level, you can enter the privileged mode without password authentication. For security, you are recommended to set the password for the privileged user level.

2.2.4.1 Configuring Command Authorization

To expand the usage range of a command, you can assign it to the users at lower level. On contrary, to narrow the usage range of a command, you can assign it to the users at higher level.

You can use the following commands to authorize users to use a command:

Command	Purpose
DES-7200# **configure terminal**	Enter the global configuration mode.

Command	Purpose
DES-7200(config)# **privilege mode** [**all**] {**level** *level* **| reset**} *command-string*	Set the privileged level for a command. **mode** – The CLI command mode at which you are authorizing the command. For example, **config** indicates the global configuration mode, **exec** indicates the privileged command mode, and **interface** indicates the interface configuration mode. **all** – Change the privileges of all the sub-commands of the specified commands into the same level. **level** *level* – Authorization level in the range from 0 to 15. **Level** 1 is for the normal user level. **Level** 15 is for the privileged user level. You can switch over between various levels by using the **enable/disable** command. *command-string* - The command to be authorized.

To restore the configuration for a specified command, use the **no privilege mode** [**all**] **level** *level command* in the global configuration mode.

2.2.4.2 Example of Command Authorization Configuration

The following is the configuration process that sets the **reload** command and all its sub-commands to be level 1, and brings level 1 into effective (by setting the command as "**test**"):

```
DES-7200# configure terminal
DES-7200(config)# privilege exec all level 1 reload
DES-7200(config)# enable secret level 1 0 test
DES-7200(config)# end
```

Enter the level 1, you can see the command and its subcommands:

```
DES-7200# disable 1
DES-7200> reload ?
  at                  reload at a specific time/date
  cancel               cancel pending reload scheme
  in                  reload after a time interval
  <cr>
```

The following is the configuration process that restores the privilege settings of the **reload** command and all its sub-commands to the default value:

```
DES-7200# configure terminal
DES-7200(config)# privilege exec all reset reload
DES-7200(config)# end
```

Enter the level 1, the privilege setting for the command is removed.

```
DES-7200# disable 1
DES-7200> reload ?
% Unrecognized command.
```

2.2.5 Configuring Line Password Protection

Our products offer password authentication for remote logons (such as Telnet). A password is required for the protection purpose. Execute the following command in the line configuration mode:

Command	Purpose
DES-7200(config-line)# **password** *password*	Specify a line password.
DES-7200(config-line)# **login**	Enable the line password protection.

Note

If no logon authentication is configured, the password authentication on line layer will be ignored even when the line password is configured. The logon authentication will be described in the next section.

2.2.6 Supporting Session Locking

Our products allow you to lock the session terminal temporarily using the **lock** command, so as to prevent access. To this end, enable the terminal locking function in the line configuration mode, and lock the terminal using the **lock** command in the EXEC mode of the terminal:

Command	**Purpose**
DES-7200(config-line)# **lockable**	Enable the function of locking the line terminal
DES-7200# **lock**	Lock the current line terminal

2.3 Logon Authentication Control

2.3.1 Overview

In the previous section, we have described how to control the access to network devices by configuring the locally stored password. In addition to line password protection and local authenticaion, in AAA mode, we can authenticate users' management privilege based on their usernames and passwords on some servers when they log on to the switch, take RADIUS server for example.

With RADIUS server, the network device sends the encrypted user information to the RADIUS server for authentiction rather than autenticates them with the locally stored credentials. The RADIUS server configures user information consistently like user name, password, shared key, and access policy to

facilitate the management and control of user access and enhance the security of user informaiton.

2.3.2 Configuring Local Users

Our products support local database-based identify authentication system used for local authentication of the method list in AAA mode and local authentication of line login management in non-AAA mode.

To enable the username identity authentication, run the following specific commands in the global configuration mode:

Command	Function
DES-7200(config)# **username** *name* [**password** *password* | **password** *encryption-type encrypted password*]	Enable the username identity authentication with encrypted password.
DES-7200(config)# **username** *name* [**privilege** *level*]	Set the privilege level for the user (optional).

2.3.3 Configuring Line Logon Authentication

To enable the line logon identity authentication, run the following specific commands in the line configuration mode:

Command	Function
DES-7200(config-line)# **login local**	Set local authentication for line logon in non-AAA mode.
DES-7200(config-line)# **login authentication** {**default** | *list-name*}	Set AAA authentication for line logon in AAA mode. The authentication methods in the AAA method list will be used for authentication, including Radius authentication, local authentication and no authentication.

Note

For more information on how to set AAA mode, configure Radius service and configure the method list, see the sections for AAA configuration.

2.4 System Time Configuration

2.4.1 Overview

Every switch has its system clock, which provides date (year, month, day) and time (hour, minute, second) and week. When you use a switch for the first time, you must configure the system clock manually. Of course, you can adjust the system clock when necessary. System clock is used for such functions as system logging that need recording the time when an event occurs.

2.4.2 Setting System Time and Date

You can configure the system time on the network device manually. Once configured, the clock will be running continuously even if the network device is powered off. Therefore, unless you need to modify the time of device, it is not necessary to configure the time again.

However, for the network devices that don't provide the hardware clock, manually setting time actually configures software clock, which only takes effect for this operation. When the network devices are powered off, the manually set time will not be valid.

Command	Function
DES-7200# **clock set** *hh:mm:ss month date day year*	Set system date and time.

For example, change the system time to10:10:12, 2003-6-20:

```
DES-7200# clock set 10:10:12 6 20 2003                    //Set system time and
date.
DES-7200# show clock                                       //Confirm the
                                                            modification takes
                                                            effect.
clock: 2003-6-20 10:10:54
```

2.4.3 Showing System Time and Date

You can show system time and date by using the **show clock** command in the privileged mode. The following is the format:

```
DES-7200# sh clock                        //Show the current system time and
date.
clock: 2003-5-20 11:11:34
```

2.4.4 Updating Hardware Clock

Some platforms use hardware clock (calendar) to implement software clock. Since battery enables hardware clock to run continuously, even though the device is closed or restarts, hardware clock still runs.

If hardware clock and software clock are asynchronous, then software clock is more accurate. Execute **clock update-calendar** command to copy date and time of software clock to hardware clock.

In the privileged mode, execute **clock update-calendar** command to make software clock overwrite the value of hardware clock.

Command	Function
DES-7200# **clock update-calendar**	Update hardware clock via software clock.

Execute the command below to copy current date and time of software clock to hardware clock.

```
DES-7200# clock update-calendar
```

2.5 Scheduled Restart

2.5.1 Overview

This section describes how to use the **reload** [*modifiers*] command to schedule a restart scheme to restart the system at the specified time. This function facilitates user's operation in some circumstance (for the purpose of test, for example). *Modifiers* is a set of options provided by the **reload** command, making the command more flexible. The optional *modifiers* includes **in**, **at** and **cancel**. The following are the details:

1. **reload in** *mmm* | *hhh:mm* [*string*]

This command sets the system restart in fixed intervals in the format of *mmm* or *hhh:mm*. *string* is a help prompt. You can give the scheme a memorable name by the string to indicate its purpose. string is a prompt. For example, to reload the system at the interval of 10 minutes for test, type **reload in *10 test***.

2. **reload at** *hh:mm day month year* [*string*]

This command sets the system restart at the specified time in the future ,which must not be more than 200 days from the curent system time . The usage of *string* is just like above. For example, if the current system time is 14:31 on January 10, 2005, and you want the system to reload tomorrow, you can input **reload at *08:30 11 1 2005 newday***. If the current system time is 14:31 on

December 10, 2005, and you want the system to reload at 12:00 a.m. on January 1, 2006, you can input **reload at *12:00 1 1 2006 newyear.***

3. reload cancel

This command deletes the restart scheme specified by the user. As mentioned above, you have specified the system to reload at 8:30 a.m. tomorrow, the setting will be removed after you input **reload cancel**.

Note

Only if the system supports clock function can users use option **at**. Before the use, it is recommended to configure the system clock according to your needs. If a restart scheme has been set before, the subsequent settings will overwrite the previous settings. If the user has set a restart scheme and then restarts the system before the scheme takes effect, the scheme will be lost.

The span from the time in the restart scheme to the current time shall be within 200 days and must be greater than the current system time. Besides, after you set reload, you should not set the system clock. Otherwise, your setting may fail to take effect, such as setting system time after reload time.

2.5.2 Specifying the System to Restart at the Specified Time

In the privileged mode, you can configure the system reload at the specified time using the following commands:

Command	Function
DES-7200# **reload at** *hh:mm day month year* [*reload-reason*]	The system will reload at hh:mm,month day,year. *reload-reason* (if any) indicates the reason that the system reloads.

The following is an example specifying the system reload at 12:00 a.m. January 11, 2005 (suppose the current system clock is 8:30 a.m. January 11,2005):

```
DES-7200# reload at 12:00 1 11 2005 midday   //Set the reload time and date.
DES-7200# show reload                        //Confirm the modification
                                             takes effect.
Reload scheduled for 2005-01-11 12:00  (in 3 hours 29 minutes)16581 seconds.
At 2005-01-11 12:00
Reload reason: midday
```

2.5.3 Specifying the System to Restart after a Period of Time

In the privileged mode, you can configure the system reload in the specified time with the following commands:

Command	Function

Command	Function
DES-7200# **reload in** *mmm* [*reload-reason*]	Configure the system reload in *mmm* minutes, where the reload reason is described in *reload-reason* (if inputted)
DES-7200# **reload in** *hhh:mm* [*reload-reason*]	Configure the system reload in *hhh* hours and *mm* minutes, where the reload reason is described in *reload-reason* (if inputted)

The following example shows how to reload the system in 125 minutes (assumes that the current system time is 12:00 a.m. January 10, 2005):

```
DES-7200# reload in 125 test     //Set the system reload time
```

Or

```
DES-7200# reload in 2:5 test     //Set the system reload time
DES-7200# show reload            //Confirm whether the restart time change
takes effect
Reload scheduled System will reload in 2 hours and 4 minutes7485 seconds.
```

2.5.4 Immediate Restart

The **reload** command without any parameters will restart the device immediately. In the privileged mode, the user can restart the system immediately by typing the **reload** command.

2.5.5 Deleting the Configured Restart Scheme

In the privileged mode, use the following command to delete the configured restart scheme:

Command	**Function**
DES-7200# **reload cancel**	Delete the configured restart scheme.

If no reload scheme is configured, you will see an error message for the operation.

2.6 Configuring a System Name and Prompt

2.6.1 Overview

For easy management, you can configure a system name for the switch to identify it. If you configure a system name of more than 32 characters, the first 32 characters are used as the system prompt. The prompt varies with the system name. By default, the system name and command prompt are specific device names.

2.6.2 Configuring a System Name

Our products provide the following commands to configure a system name in the global configuration mode:

Command	Function
DES-7200(Config)# **hostname** *name*	Configure a system name with printable characters less than 255 bytes.

To restore the name to the default value, use the **no hostname** command in the global configuration mode. The following example changes the equipment name to DES-7210:

```
DES-7200# configure terminal       //Enter the global configuration mode.
DES-7200(config)# hostname DES-7210     //Set the equipment name to DES-7210
DES-7210(config)#                       //The name has been modified
successfully.
```

2.6.3 Configuring a Command Prompt

System name will be the default prompt if you have not configured command prompt. (if the system name exceeds 32 characters, intercept the first 32 characters) The prompt varies with the system name.You can use the **prompt** command to configure the command prompt in the global configuration mode, and the command prompt is only valid in the EXEC mode.

Command	Function
DES-7200# **prompt** *string*	Set the command prompt with printable characters. If the name exceeds 32 characters, intercept the first 32 characters.

To restore the prompt to the default value, use the **no prompt** command in the global configuration mode.

2.7 Banner Configuration

2.7.1 Overview

When the user logs in the switch, you may need to tell the user some useful information by configuring a banner. There are two kinds of banners: message-of-the-day (MOTD) and login banner. The MOTD is specific for all users who connect with switches. And when users log in the switch, the notification message will appear on the terminal. MOTD allows you send some urgent messages (for example, the system is to be shut down) to network users. The login banner also appears on all connected terminals. It provides some

common login messages. By default, the MOTD and login banner are not configured.

2.7.2 Configuring a Message-of-the-Day

You can create a notification of single or multi-line messages that appears when a user logs in the switch. To configure the message of the day, execute the following commands in the global configuration mode:

Command	Function
DES-7200(Config)# **banner motd** *c message c*	Specify the message of the day, with c being the delimiter, for example, a pound sign (&). After inputting the delimiter, press the **Enter** key. Now, you can start to type text. You need to input the delimiter and then press **Enter** to complete the type. Note that if you type additional characters after the end delimiter, these characters will be discarded by the system. Also note that you cannot use the delimiter in the message and the message length should be no more than 255 bytes.

To delete the MOTD, use the **no banner motd** command in the global configuration mode. The following example describes how to configure a MOTD. The # symbol is used as the delimiter, and the text is “Notice: system will shutdown on July 6th.”

```
DES-7200(config)# banner motd #                          //Start delimiter.
Enter TEXT message.  End with the character '#'.
Notice: system will shutdown on July 6th.#              //End delimiter.
DES-7200(config)#
```

2.7.3 Configuring a Login Banner

To configure a login banner, executing the following commands in the global configuration mode:

Command	Function
DES-7200(Config)# **banner login** *c message c*	Specify the text of the login banner, with c being the delimiter, for example, a pound sign (&). After inputting the delimiter, press the **Enter** key. Now, you can start to type text. You need to input the delimiter and then press **Enter** to complete the type. Note that if you type additional characters after the end delimiter, these characters will be discarded by the system. Also note that you cannot use the delimiter in the text of the login banner and the text length should be no more than 255 bytes.

To delete the login banner, use the **no banner login** command in the global configuration mode.

The following example shows how to configure a login banner. The pound sign (#) is used as the starting and end delimiters and the text of the login banner is "Access for authorized users only. Please enter your password."

```
DES-7200(config)# banner login #      //Start delimiter
Enter TEXT message. End with the character '#'.
Access for authorized users only. Please enter your password.
#                                     //End delimiter
DES-7200(config)#
```

2.7.4 Displaying a Banner

A banner is displayed when you log in the network device. See the following example:

```
C:\>telnet 192.168.65.236
 Notice: system will shutdown on July 6th.
 Access for authorized users only. Please enter your password.
 User Access Verification
Password:
```

As you can see, “Notice: system will shutdown on July 6th." is a MOTD banner and "Access for authorized users only. Please enter your password." is a login banner.

2.8 Viewing System Information

2.8.1 Overview

You can view some system information with the **show** command on the command-line interface, such as version, device information, and so on.

2.8.2 Viewing System Information and Version

System information consists of description, power-on time, hardware version, software version, BOOT-layer software version, CTRL-layer software version, and so on. System information helps you know the system You can show the system information with the following commands in the privileged mode.

Command	Function
DES-7200# **show version**	Show system information.

Note

For sequence number ,run the **show version** command on the main program interface to view SYSTEMUPTIME in the form of DD:HH:MM:SS.

Note

During upgrading, the running software version may be different from the version in the file system. In this case, the main program version shown by running the **show version** command is the one running in the memory, but the Boot/Ctrl version is the one saved in Flash.

2.8.3 Viewing Hardware Entity Information

Hardware information refers to the information on physical devices as well as slots and modules assembled in a device. The information on a device itself includes description, number of slots,slot information, slot number, description of the module on the slot (empty description if no module is plugged on the slot), number of physical ports of the module on the slot, and maximum number of ports possibly supported on the slot (number of ports of the module plugged). You may use the following commands to show the information of the device and slots in the privileged mode:

Command	Function
DES-7200# **show version devices**	Show device information.
DES-7200# **show version slots**	Show the information about slots and modules.

2.9 Setting Console Rate

2.9.1 Overview

The switch comes with a console interface for management. When using the switch for the first time, you need to execute configuration through the console interface.You can change the console rate on the equipment if necessary. Note that the rate of the terminal used to managing the switch must be the same as that of the console interface on the switch.

2.9.2 Setting Console Rate

In the line configuration mode, execute the following command to set the console rate:

Command	Function

Command	Function
DES-7200(config-line)# **speed** *speed*	Set transmission rate in bps on the console interface. For a serial interface, you can only set the transmission rate to one of 9600, 19200, 38400, 57600 and 115200 bps, with 9600 bps by default.

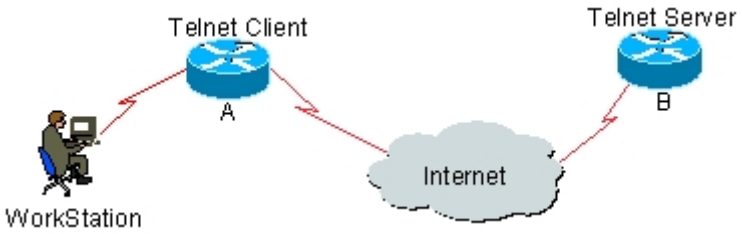
This example shows how to configure the baud rate of the serial interface to 57600 bps:

```
DES-7200# configure terminal              //Enter the global configuration
mode.
DES-7200(config)# line console 0          //Enter the console line
configuration mode
DES-7200(config-line)# speed 57600        //Set the console rate to 57600bps
DES-7200(config-line)# end                //Return to the privileged mode
DES-7200# show line console 0             //View the console configuration
CON    Type    speed   Overruns
* 0    CON    57600   0
Line 0, Location: "", Type: "vt100"
Length: 25 lines, Width: 80 columns
Special Chars: Escape  Disconnect  Activation
            ^^x    none       ^M
Timeouts:   Idle EXEC   Idle Session
            never        never
History is enabled, history size is 10.
Total input: 22 bytes
Total output: 115 bytes
Data overflow: 0 bytes
stop rx interrupt: 0 times
Modem: READY
```

2.10 Configuring Telnet

2.10.1 Overview

Telnet, an application layer protocol in the TCP/IP protocol suite, provides the specifications of remote logon and virtual terminal communication functions. The **Telnet Client** service is used by the local or remote user who has logged onto the local network device to work with the Telnet Client program to access other remote system resources on the network. As shown below, after setting up a connection with Switch A through the terminal emulation program or Telnet, users can log on the Switch B for management and configuration with the **telnet** command.



2.10.2 Using Telnet Client

You can log in to a remote device by using the **telnet** command on the switch.

Command	Function
DES-7200# **telnet** *host* [port] [/**source** {**ip** *A.B.C.D* **ipv6** *X:X:X::X* | **interface** *interface-name*}] [/**vrf** *vrf-name*]	Log on to a remote device via Telnet. *host* may be an IPv4 or IPv6 host name or an IPv4 or IPv6 address. For supported optional parameters, refer to relevant Telnet command section in *Basic Configuration Management Command*.

The following example shows how to establish a Telnet session and manage the remote device with the IP address 192.168.65.119:

```
DES-7200# telnet 192.168.65.119    //Establish the telnet session to the
remote device
Trying 192.168.65.119 ... Open
User Access Verification      //Enter into the logon interface of the remote
device
Password:
```

The following example shows how to establish a Telnet session and manage the remote device with the IPv6 address 2AAA:BBBB::CCCC:

```
DES-7200# telnet 2AAA:BBBB::CCCC   //Establish the telnet session to the
remote device
Trying 2AAA:BBBB::CCCC ... Open
User Access Verification      //Enter into the logon interface of the remote
device
Password:
```

2.11 Setting Connection Timeout

2.11.1 Overview

You can control the connections that a device has set up (including the accepted connections and the session between the devece and a remote terminal) by configuring the connection timeout time for the device. When the

idle time exceeds the set value and there is no input or output, this connection will be interrupted.

2.11.2 Connection Timeout

When there is no information traveling through an accepted connection within a specified time, the server will interrupt this connection.

Our products provide commands to configure the connection timeout in the line configuration mode.

Command	Function
DES-7200(Config-line)#**exec-timeout** *20*	Configure the timeout for the accepted connection. When the configured time is due and there is no input, this connection will be interrupted.

The connection timeout setting can be removed by using the **no exec-timeout** command in the line configuration mode.

```
DES-7200# configure terminal            //Enter the global configuration
mode.
DES-7200# line vty 0                    //Enter the line configuration mode
DES-7200(config-line)#exec-timeout 20   //Set the timeout to 20min
```

2.11.3 Session Timeout

When there is no input for the session established with a remote terminal over the current line within the specified time, the session will be interrupted and the remote terminal becomes idle.

DES-7200 provides commands in the line configuration mode to configure the timeout for the session set up with the remote terminal.

Command	Function
DES-7200(Config-line)#**session-timeout** *20*	Configure the timeout for the session set up with the remote terminal over the line. If there is no input within the specified time, this session will be interrupted.

The timeout setting for the session set up with the remote terminal over the line can be removed by using the **no exec-timeout** command in the line configuration mode.

```
DES-7200# configure terminal            //Enter the global configuration
mode.
DES-7200(config)# line vty 0            //Enter the line configuration
mode
DES-7200(config-line)# session-timeout 20  //Set the session timeout to
20min
```

2.12 Executing the Commands in the Executable File in Batch

In system management, sometimes it is necessary to enter multiple configuration commands to manage a function. It takes a long period of time to enter all the commands on CLI, causing error or mission. To resolve this problem, you can encapsulate all the commands in a batch file according to configuration steps. Then, you can execute the batch file for configuration when necessary.

Command	Function
DES-7200# **execute {[flash:]** *filename***}**	Execute a batch file.

For example, the batch file line_rcms_script.text enables the reversed Telnet function on all the asynchronous interfaces as shown below:

```
configure terminal
line tty 1 16
transport input all
no exec
end
```

Result:

```
DES-7200# execute flash:line_rcms_script.text
executing script file line_rcms_script.text ......
executing done
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# line vty 1 16
DES-7200(config-line)# transport input all
DES-7200(config-line)# no exec
DES-7200(config-line)# end
```

Note

The file name and contents of a batch file can be specified. Once edited, users send the batch file to the FLASH of the network device in TFTP. The contents of the batch file will simulate the input completely. Hence, it is necessary to edit the contents of the batch file by the sequence that CIL commands are configured. Furthermore, for some interactive commands, it is necessary to write corresponding response information in the batch file, guaranteeing that the commands can be executed normally.

2.13 Setting Service Switch

During operation, you can adjust services dynamically, enabling or disabling specified services (SNMP Server/SSH Server/Telnet Server/Web Server).

Command	Function

Command	Function
DES-7200(Config)# **enable service snmp-agent**	Enable SNMP Server.
DES-7200(Config)# **enable service ssh-sesrver**	Enable SSH Server.
DES-7200(Config)# **enable service telnet-server**	Enable Telnet Server
DES-7200(Config)# **enable service web-server**	Enable Http Server.

In the configuration mode, you can use the **no enable service** command to disable corresponding services.

```
DES-7200# configure terminal                //Enter the global
configuration mode.
DES-7200(config)# enable service ssh-server     //Enable SSH Server
```

2.14 Setting HTTP Parameters

When using the integrated Web for management, you can adjust HTTP parameters, and specify service port or login authentication method.

Command	Function
DES-7200(Config)# **ip http port** *number*	Specify HTTP service port, 80 by default.
DES-7200(Config)# **ip http authentication {enable | local}**	Set Web login authentication method, enable by default. enable: Use the password set by the **enable password** or **enable secret** command for authentication, where the password must be 15 levels. local: Use the username and password set by the **username** command for authentication, where the user must be bound with 15-level right.

In the configuration mode, you can use the **no** form of the command to restore the setting to the default value. The following example enables the HTTP Server, sets the service port to 8080, and uses the local username for login authentication.

```
DES-7200# configure terminal                //Enter the global
configuration mode.
DES-7200(config)# enable service web-server http    //Enable http Server
DES-7200(config)# username name password pass //Set local user
DES-7200(config)# username name privilege 15    //Bind user right
DES-7200(config)# ip http port 8080             //Set service port
```

```
DES-7200(config)# ip http authentication local //Set authentication method
```

Use the following command to configure HTTPS service port.

Command	Function
DES-7200(Config)# **ip http secure-port** *number*	Specify the HTTP service port. (default:443)

In the configuration mode, you can use the **no** form of the command to restore the setting to the default value. The following example enables the HTTP Server, sets the service port to 4443.

```
DES-7200# configure terminal                //Enter the global
configuration mode.
DES-7200(config)# enable service web-server https//Enable https Server
DES-7200(config)# ip http secure-port 4443
```

Use the following command to verify the status of WEB server.

```
DES-7200# show web-server status
http server status : enabled
http server port : 8080
https server status:  enabled
https server port: 4443
```

Caution

Avoid configuring http service port and https service port to the same value. If https service is enabled after http service has been enabled, and the port is accidentally configured to the same port used by http service, then the user can only access https service through this port, and http service will be blocked temporarily until https service port is changed or the service is disabled.

2.15 Setting Multi-boot Function

2.15.1 Overview

By default, the device searches for the main program file and boot it in the embedded FLASH. If the main program file is damaged for some reason, for instance, upgrad failure, formatted FLASH and the like, the device will fail to boot the system.

Some products of D-Link Corporation come with multi-boot function to support multiple main programs. When the device starts, the system boots the main programs by boot pirority in descending order until it boots successfully or all programs are filed. Multi-boot function is mandatory for some environments with higher demands on reliability and availability.

This following sections describe how to use multi-boot for redundant backup of main program.

2.15.2 Configuring the Boot Main Program

You can use the following command to configure the boot main program and specify its boot priority. The system will boot the corresponding main program by priority in descending order with 1 being the highest and 10 being the lowest.

Command	Function
DES-7200(Config)#**boot system** *priority prefix:/* [directory/] *filename*	Set the boot main program and specify its priority. The boot priority is in the range of 1 to 10, with 1 being the highest.

Caution

Using URL prefix to locate a file is only supported on 10.4(2) and higher version. For details, refer to File System Configuration Guide. Path is used to locate a file on the version lower than 10.4(2), for example, flash:/firmware.bin indicates the firmware.bin file under the Flash root directory.

Supported URL prefixes vary by platforms. To show the URL prefixes supported at present, run the following command:

DES-7200 (config) # **boot system** 2 ?

flash: Boot from flash: file system

By default, the bootable main program is flash:/firmware.bin with the priority of 5.

Caution

Since the system uses the configuration of this command in the early stage of boot, the configuration is saved in the Boot ROM rather than in the configuration file.

The following example sets the file on the local FLASH as the main program.

```
DES-7200(config)# boot system 5 flash:/firmware.bin
```

Note

When you specify the local file through prefix, the path behind ":" must be absolute path.

When you configure the **boot system** command, the systme will check the vailidty of the main program on the local FLASH. Only the main program meets the following requirements can you configure the command successfully.

- The main program must be existent.
- The main program is legal firmware main program.

- The main program is complete and pass CRC check.

If any requirement is not met, the systme will prompt error, for instance:

DES-7200(config)# **boot system** *5* **flash***:/foo.bin*

Set boot system file error:[**flash***:/foo.bin*] does not exist!

In addition, a priority can be set for more than one main program, or otherwise the system will prompt error and print the current main program list for your selection. For instnace:

DES-7200(config)# **boot system** *5* **flash***:/firmware.bin*

DES-7200(config)# **boot system** *5* **flash***:/firmware_bak.bin*

Set boot system file error: priority 5 was assigned to file [**flash***:/firmware.bin*] already.

```
Boot system config:
=====================================================
Prio     Size            Modified  Name
---- --------- ------------------- -----------------
  1
  2
  3
  4
  5    3205120 2008-08-26 05:22:46 flash:/firmware.bin
  6
  7
  8
  9
 10
=====================================================
DES-7200(config)# boot system 6 flash:/firmware_bak.bin
```

2.15.3 Modifying the Boot Priority of Main Program

The **boot system** command can also modify the boot priority of main program. Aussme that the configured boot mian program list is shown below:

```
DES-7200# show boot system
Boot system config:
=====================================================
Prio     Size            Modified  Name
---- --------- ------------------- -----------------
  1
  2
  3
```

```
 4
 5    3205120 2008-08-26 05:22:46 flash:/firmware.bin
 6
 7
 8    3205120 2008-08-26 05:25:09 flash:/firmware_bak.bin
 9
10
=====================================================
```

To set the boot priority of flash:/firmware_bak.bin to 1, run the following command:

```
DES-7200(config)# boot system 1 flash:/firmware_bak.bin
File [flash:/firmware_bak.bin] has been configured with
priority 8,
Change the priority to [1]? [yes] yes
```

The result is that:

```
DES-7200# show boot system
Boot system config:
=====================================================
Prio     Size             Modified  Name
---- --------- ------------------- -----------------
 1    3205120 2008-08-26 05:25:09 flash:/firmware_bak.bin
 2
 3
 4
 5    3205120 2008-08-26 05:22:46 flash:/firmware.bin
 6
 7
 8
 9
10
=====================================================
```

2.15.4 Deleting the Boot Main Program

You can use the following command to delete the boot main program.

Command	Function
DES-7200(Config)# no **boot system** [*priority*]	Delete the boot main program. The boot priority is in the range of 1 to 10 . if the priority is not set, all the boot main programs will be reset.

Use the following command to delete the main program with the prioirty of 8. While deletion, the systme prints the corresponding main program name and ask for confirmation.

```
DES-7200(config)# no boot system 8
Delete boot system config: [Priority: 8; File Name:
flash:/firmware_bak.bin]? [no] yes
```

Use the following command to clear all the boot main programs.

```
DES-7200(config)# no boot system
Clear ALL boot system config? [no] yes
```

Caution

If you have not configured the boot main program after using the **no boot system** command to clear all boot main programs, the system will automatically restore to the default setting next booting (the bootable main program is flash:/firmware.bin with the priority of 5).

2.15.5 Showing the Configuration of Multi-boot

You can use the following command to show the configuration of multi-boot.

Command	Function
DES-7200# **show boot system**	Show the configuration of the boot main program.

Use the following command to show the main program and its boot priority.

```
DES-7200# show boot system
Boot system config:
=====================================================
Prio     Size            Modified  Name
---- --------- ------------------- -----------------
  1
  2
  3
  4
  5    3205120 2008-08-26 05:22:46 flash:/firmware.bin
  6
  7
  8    3205120 2008-08-26 05:25:09 flash:/firmware_bak.bin
  9
 10
=====================================================
```

Note

If the corresponding main program does not exist when running the **show boot system** command, the length and modification time of the file is also shown as N/A.

2.15.6 Configuration Example

The following example shows how to boot from the firmware.bin under the root directory in FLASH, and how to boot from backup firmware_bak.bin when firmware.bin is damaged or lost.

Step 1: Configure the default main program.

```
DES-7200(config)# boot system 5 flash:/firmware.bin
```

Since the device is cnfigured with the main program flash;/firmware.bin with priority of 5 during intialization, this step can be skipped.

Generally, it is recommended to set the priority of active main program to be medium so that you can flexibly configure other main program with higher or lower priroity in future.

Step 2: configure the backup main program.

The priority of backup main program should be slightly lower than the active main program.

```
DES-7200(config)# boot system 8 flash:/firmware_bak.bin
```

Step 3 Verify configuration.

You can run the **show boot system** command to view confiugration.

```
DES-7200# show boot system
Boot system config:
=====================================================
Prio     Size            Modified  Name
---- --------- ------------------ -----------------
  1
  2
  3
  4
  5    3205120 2008-08-26 05:22:46 flash:/firmware.bin
  6
  7
  8    3205120 2008-08-26 05:25:09 flash:/firmware_bak.bin
  9
 10
=====================================================
```

2.16 Setting Start Confiugration File

2.16.1 Overview

Some products of D-Link Corporation offer the capability to speficy start configuration file, which can be stored in FLASH< mobile storage device (for instance, U-shape disk, SD card) or remote TFTP server and the like.

After configuration, a deviced can get configuration file from a specific place as the start configuration file.

This following sections describe how to specify start configuration file.

2.16.2 Configuring the Start Configuration File

You can use the following command to configure the start configuration file.

Command	Function
DES-7200(Config)#**boot config** *prefix:/* [directory/] *filename*	Set the start configuration file.
DES-7200(Config)#**no boot config**	Clear the start configuration file.

Note

You can view the configuration file by the command line help, for instance:

DES-7200(config)#**boot config** ?

flash: Startup-config filename

usb0: Startup-config filename

usb1: Startup-config filename

The systme loads configuration file by the following principles:

- If the **service config** command is not configured, the configuration file is loaded by the following order-the start configuration file configured by the **boot config** command, /config.text, the network start configuration file cofnigured by the **boot network** command, and the default factory configuration (null configuration).
- If the **service config** command is configured, the configuration file is loaded by the following order- the network start configuration file cofnigured by the **boot network** command, the start configuration file configured by the **boot config** command, /config.text, and the default factory configuration (null configuration).

- In the course of loading the configuration file by order, the system will not load other configuration files as long as one configuration file is loaded successfully.

Caution

- For the **service config** and **boot config** commands, refer to the following sections.
- Since the system needs to use the configuration of this command in the early stage of boot, this configuration is stored in Boot ROM rather than the configuration file.

When using the **write [memory]** command to store the start configuration file, the system will save it by the following principles:

- If the **boot config** command is not used to configure the start configuration file, by default the systme saves the configuration into the flash:/config.text file in embedded FLASH.
- If the **boot config** command is used to configure the start configuration file and the file exists, the system saves the configuration into the start configuration file.
- If the **boot config** command is used to configure the start configuration file but the configuration file does not exist, then:

  1 If the device where the configuration file locats exists, the system will automatically create the specified configuration file and save it into the system configuration.

  2 If the device where the configuration file locats does not exist (for instnace, the start cofniguration file is saved in the mobile storage device like U-shape disc or SD card, but the device is not loaded when the system runs the **wirte [memory]** command), the systme will ask whether to save the configuration into the default start configuration file *flash:/config.text* and execute corresponding action according to response.

The following example sets the file on the U-shape disk as the start configuration file and demonstrates the actions of running the **write** command before and after removing U-shape disk.

Set the file on the U-shape disk as the start configuration file.

```
DES-7200(config)# boot config usb1:/config.text
```

Run the **write** command before removing U-shape disk to save the current configuation into the file specified by the **boot config** command.

```
DES-7200# write
Building configuration...
Write to boot config file: [usb1:/config.text]
[OK]
```

Run the **write** command after removing U-shape disk. The system will ask whether to save the current configuration into the default start configuraiton file /config.

```
DES-7200# usb remove 1
0:1:1:38 DES-7200: USB-5-USB_DISK_REMOVED: USB Device <USB
Mass Storage Device> Removed!
DES-7200# write
Building configuration...
Write to boot config file: [usb1:/config.text]
[Failed]
The device [usb1] does not exist, write to the default config
file [flash:/config.text]? [no] yes
Write to the default config file: [flash:/config.text]
[OK]
```

2.16.3 Configuring the Network Start Configuration File

You can use the following command to configure the network start configuration file.

Command	Function
DES-7200(Config)# **boot network tftp ://** location / *filename*	Configure the network start configuration file.
DES-7200(Config)#**no boot network**	Clear the network start configuration file.

When the device starts, the system loads the cofniguration file by following principles;

- If the **service config** command is not configured, the configuration file is loaded by the following order-the start configuration file configured by the **boot config** command, /config.text, the network start configuration file cofnigured by the **boot network** command, and the default factory configuration (null configuration).
- If the **service config** command is configured, the configuration file is loaded by the following order- the network start configuration file cofnigured by the **boot network** command, the start configuration file configured by the **boot config** command, /config.text, and the default factory configuration (null configuration).
- In the course of loading the configuration file by order, the system will not load other configuration files as long as one configuration file is loaded successfully.

Caution

- The system can get remote files through TFTP only after you run the **bootip** command to configure the local IP address of the device used for initiation, or otherwise TFTP transmission will fail during initiation.
- Since the system needs to use the configuration of this command in the early stage of boot, this configuration is stored in Boot ROM rather than the configuration file.

The following figure sets the boot IP address of the device and designates the network start configuration file.

```
DES-7200(config)# boot ip 192.168.7.11
DES-7200(config)# boot network
tftp://192.168.7.24/config.text
```

2.16.4 Configuring Preferrably Using the Network Start Configuration File

By default, the device preferably loads the local start configuration file specified by the **boot config** command. In some case, if the device needs to use the network start configuration file, run the **service config** command.

Command	Function
DES-7200(Config)# **service config**	Enable the device to preferably load the start configuration file from the remote network server.
DES-7200(Config)#**no service config**	Disable the device to preferably load the start configuration file from the remote network server.

This command should use in conjunction with the **boot config** and **boot network** commands.

When the device starts, the system loads the cofniguration file by following principles;

- If the **service config** command is not configured, the configuration file is loaded by the following order-the start configuration file configured by the **boot config** command, /config.text, the network start configuration file cofnigured by the **boot network** command, and the default factory configuration (null configuration).
- If the **service config** command is configured, the configuration file is loaded by the following order- the network start configuration file cofnigured by the **boot network** command, the start configuration file configured by the **boot config** command, /config.text, and the default factory configuration (null configuration).

- In the course of loading the configuration file by order, the system will not load other configuration files as long as one configuration file is loaded successfully.

Caution Since the system needs to use the configuration of this command in the early stage of boot, this configuration is stored in Boot ROM rather than the configuration file.

The following example preferably loads the configuration file from the remote network server and configure the network start configuration name.

```
DES-7200(config)# service config
DES-7200(config)# boot network
tftp://192.168.7.24/config.text
```

2.16.5 Showing the Configuration of Start Configuration File

You can use the following command to show the configuration of start configuration file.

Command	Function
DES-7200# **show boot config**	Show the configuration of the start configuration file.
DES-7200# **show boot network**	Show the configuration of the network start configuration file.

The following example shows the configuration of the start configuration file.

```
DES-7200# show boot config
Boot config file: [flash:/config_main.text]
Service config: [Disabled]
```

The following example shows the configuration of the network start configuration file.

```
DES-7200# show boot network
Network config file: [tftp://192.168.7.24/config.text]
Service config: [Enabled]
```

2.16.6 Configuration Example

The following example sets the device to preferrably get the configuration file from the remote TFTP server or to use the backup configuration file in built-in FLASH when it fails to get the configuration file from the remote TFTP server.

Step 1: Configure the device to preferrably load the configuration file from the network server and configure the boot IP address.

```
DES-7200(config)# service config
DES-7200(config)# boot ip 192.168.7.11
```

Step 2: Configure the network start configuration file.

```
DES-7200(config)# boot network
tftp://192.168.7.24/router_1.text
```

Step 3: Configure the local start configuration file.

```
DES-7200(config)# boot config flash:/router_1.text
```

Step 3: Show the configuration.

```
DES-7200# show boot network
Network config file: [tftp://192.168.7.24/router_1.text]
Service config: [Enabled]
DES-7200# show boot config
Boot config file: [flash:/router_1.text]
Service config: [Enabled]
```

3 SSH Terminal Service Configuration

3.1 About SSH

SSH is the shortened form of Secure Shell. The SSH connection functions like a Telnet connection, except that all transmissions based on the connection are encrypted. When the user logs onto the device via a network environment where security cannot be guaranteed, the SSH feature provides safe information guarantee and powerful authentication function to protect the devices from IP address fraud, plain password interception and other kinds of attacks.

DES-7200 SSH sevice supports both the IPv4 and IPv6 protocols.

3.2 DES-7200's SSH Support Algorithms

Support algorithm	SSH1	SSH2
Signature authentication algorithm	RSA	RSA, DSA
Key exchanging algorithm	RSA public key encryption based key exchanging algorithm	KEX_DH_GEX_SHA1 KEX_DH_GRP1_SHA1 KEX_DH_GRP14_SHA1
Encryption algorithm	DES, 3DES, Blowfish	DES, 3DES, AES-128, AES-192, AES-256
User authentication algorithm	User password based authentication method	User password based authentication method
Message authentication algorithm	Not supported	MD5, SHA1, SHA1-96, MD5-96
Compression algorithm	NONE (uncompressed)	NONE (uncompressed)

3.3 DES-7200's SSH Supports

Caution

DES-7200 supports only the SSH server (compatible with the SSHv1 and SSHv2) but do not support the SSH client.

3.4 SSH Configuration

3.4.1 Default SSH Configurations

Item	Default value
SSH service end status	Off
SSH version	Compatible mode (supporting versions 1 and 2)
SSH user authentication timeout period	120s
SSH user re-authentication times	3

3.4.2 User Authentication Configuration

1） For the consideration of the SSH connection security, the login without authentication is forbidden. Therefore, in the login authentication of the users, the login authentication mode must have password configured (no-authentication login allowed for telnet).

2） The username and password entered every time must have lengths greater than zero. If the current authentication mode does not need the username, the username can be entered randomly but the entry length must be greater than zero.

3.4.3 Enabling SSH Server

The SSH Server is disabled by default. To enable the SSH Server, run the **enable service ssh-server** command in the global configuration mode while generating SSH key.

Command	Description
configure terminal	Enter the global configuration mode.
enable service ssh-server	Enable SSH Server.
crypto key generate {rsa|dsa}	Generate the key

Caution

To delete the key, use the **crypto key zeroize** command rather than the **[no] crypto key generate** command.

3.4.4 Disabling SSH Server

When the SSH Server is enabled, if the public key on the server is deleted, the SSH Server is automatically closed. To delete the public key, run **no enable service ssh-server** in the global configuration mode to disable the SSH Server.

Command	Description
configure terminal	Enter the global configuration mode
no enable service ssh-server	Delete the key to disable SSH Server.

3.4.5 Configuring the Supported SSH Server Version

By default, the SSHv1 and SSHv2 are compatible. Run the following commands to configure the SSH version.

Command	Description
configure terminal	Enter the configuration mode
ip ssh version {1|2}	Configure the supported SSH version.
no ip ssh version	Restore the SSH default version.

3.4.6 Configuring SSH User Authentication Timeout

By default, the user authentication timeout period of the SSH SERVER is 120 seconds. Run the following commands to configure the SSH user authentication timeout period.

Command	Description
configure terminal	Enter the configuration mode
ip ssh time-out *time*	Configure the SSH timeout period (1-120sec)
no ip ssh time-out	Restore the SSH default user authentication timeout period 120 seconds.

3.4.7 Configuring SSH Re-authentication Times

This command is used to set the authentication attempts for SSH user requesting connections to prevent illegal actions such as malicious guesswork.

The authentication attempts are 3 for the SSH Server by default. In other words, it allows the user to enter the username and password for three times to attempt the authentication. Run the following commands to configure the SSH re-authentication times:

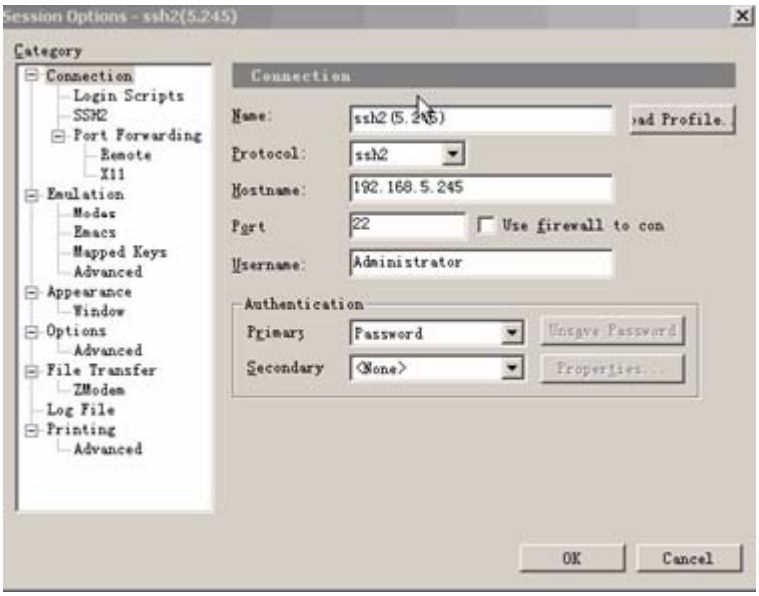
Command	Description
configure terminal	Enter the configuration mode
ip ssh authentication-retries *retry times*	Configure SSH re-authentication times (range 0-5)
no ip ssh authentication-retries	Restore the default SSH re-authentication times as 3.

Note For details of the above commands, see *SSH Command Reference Manual.*

3.5 Using SSH for Device Management

You may use the SSH for device management by first enabling the SSH Server function that is disabled by default. Since the Telnet that comes with the Windows does not support SSH, third-party client software has to be used. Currently, the clients with sound forward compatibility include Putty, Linux and SecureCRT. With the client software SecureCRT as an example, the SSH client configuration is described as follows (see the UI below):

Figure-1

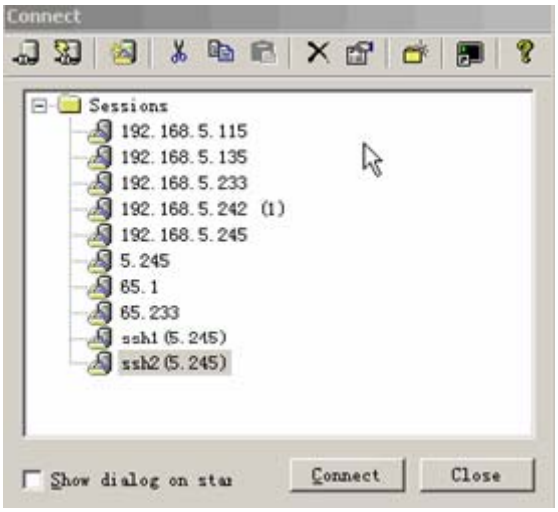


As shown in Figure-1, protocol 2 is used for login, so SSH2 is chosen in “Protocol”. “Hostname” indicates the IP address of the host that will log in,

192.168.5.245. Port 22 is the default number of the port for SSH listening. “Username” indicates the username, and does not take effect when the device only requires password. “Authentication” indicates the authentication mode, and the username/password authentication is supported here. The used password is the same as the Telnet password.

Click “OK” to pop up the following dialog:

Figure-2



Click “Connect” to log into the host just configured, as shown below:

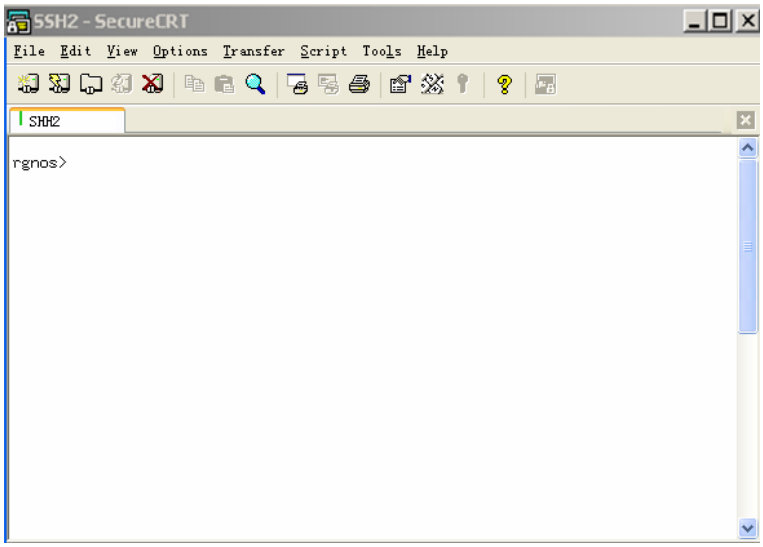
Figure-3

Ask the machine that is logging into the host 192.168.5.245 to see whether the key from the server end is received or not. Select “Accept & Save” or “Accept Once” to enter the password confirmation dialog box, as shown below:

Figure-4

Enter the Telnet login password to enter the UI that is the same as the Telnet. See the diagram below:

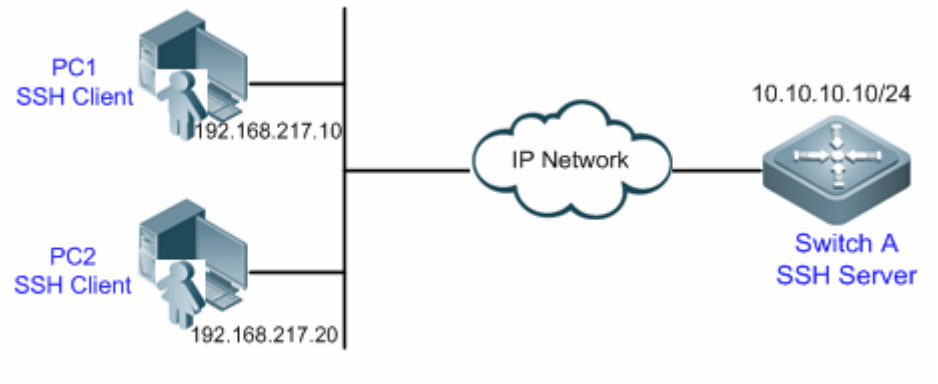
Figure-5



3.6 Typical SSH Configuration Examples

3.6.1 Example of SSH Local Authentication Configurations

3.6.1.1 Topological Diagram



Networking diagram for SSH local password protection

3.6.1.2 Application Requirements

As shown above, to ensure the security of information exchange, PC1 and PC2 serve as SSH clients which will login the SSH Server of Switch A through SSH protocol. The specific requirements are shown below:

1. SSH users adopt line password authentication.
2. 0-4 lines are enabled at the same time. The login password for line 0 is "passzero", and the login password for other four lines is "pass". Any user name can be used.

3.6.1.3 Configuration Tips

SSH Server configuration tips are shown below:

1. Globally enable SSH Server. By default, SSH Server supports SSH1 and SSH2.
2. Configure key. The SSH server will use this key to decrypt the encrypted password received from SSH client, and compare the decrypted plain text with the password stored on the server before giving the reply about successful or failed authentication. SSH1 uses RSA key, while SSH 2 uses RSA or DSA key.

3. Configure the IP address of the VLAN interface of SSH server. SSH client will use this address to connect SSH server. The route from SSH client to SSH server shall be reachable.

Configurations on SSH Client:

There are many SSH client programs, such as Putty, Linux, OpenSSH and etc. Here we will only take the client software of SecureCRT as the example to introduce how to configure SSH Client. The configuration details are given in "Configuration Steps".

3.6.1.4 Configuration Steps

Configure SSH Server (Switch A)

Before configuring relevant SSH features, make sure the route from SSH client to SSH server is reachable. The IP addresses of respective interfaces are shown in the topological diagram, and the steps of IP and route configuration are omitted herein.

Step 1: Enable SSH Server

```
DES-7200(config)# enable service ssh-server
```

Step 2: Generate RSA key

```
DES-7200(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

Step 3: Configure the address of interface VLAN 1. The client will use this address to connect SSH server.

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 10.10.10.10 255.255.255.0
DES-7200(config-if-VLAN 1)#exit
```

Step 4: Configure login password for lines

! Configure the login password for line 0 as "passzero"

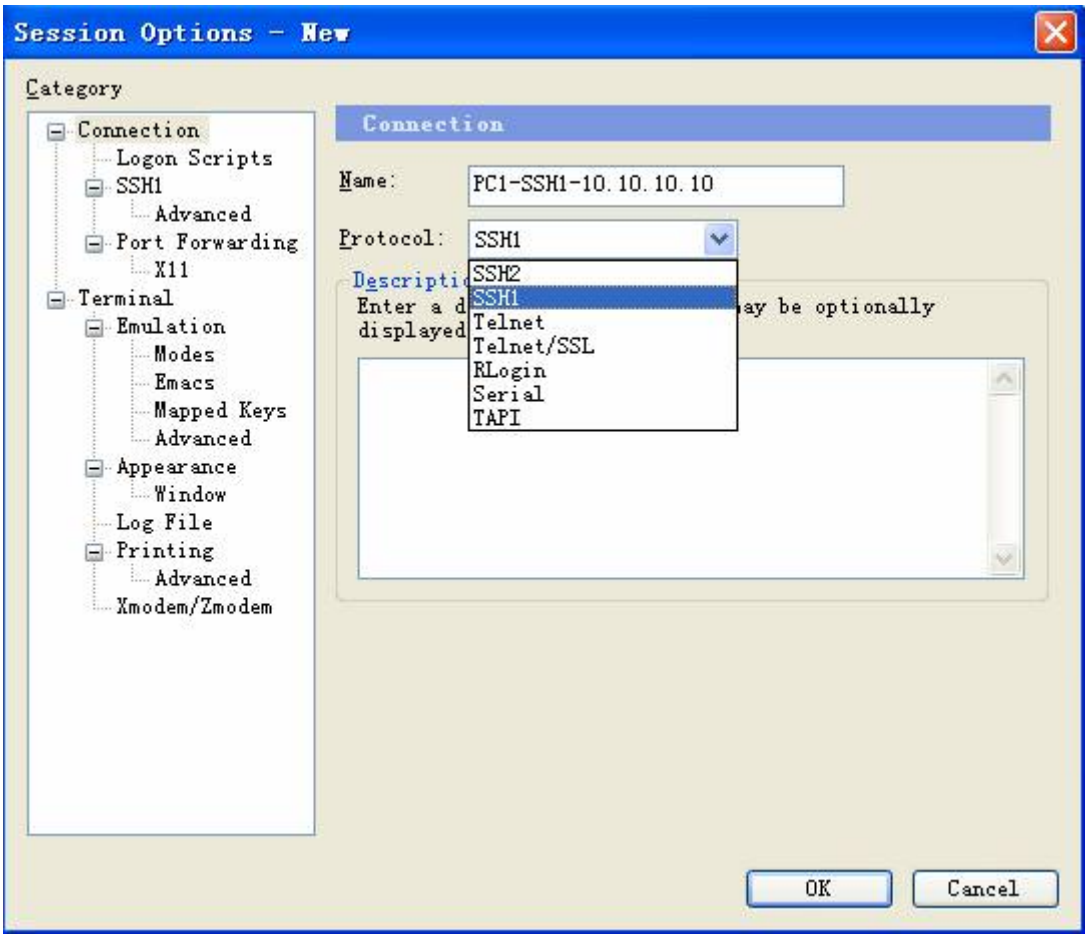
```
DES-7200(config)#line vty 0
DES-7200(config-line)#password passzero
DES-7200(config-line)#privilege level 15
DES-7200(config-line)#exit
```

! Configure the login password for line 1-4 as "pass"

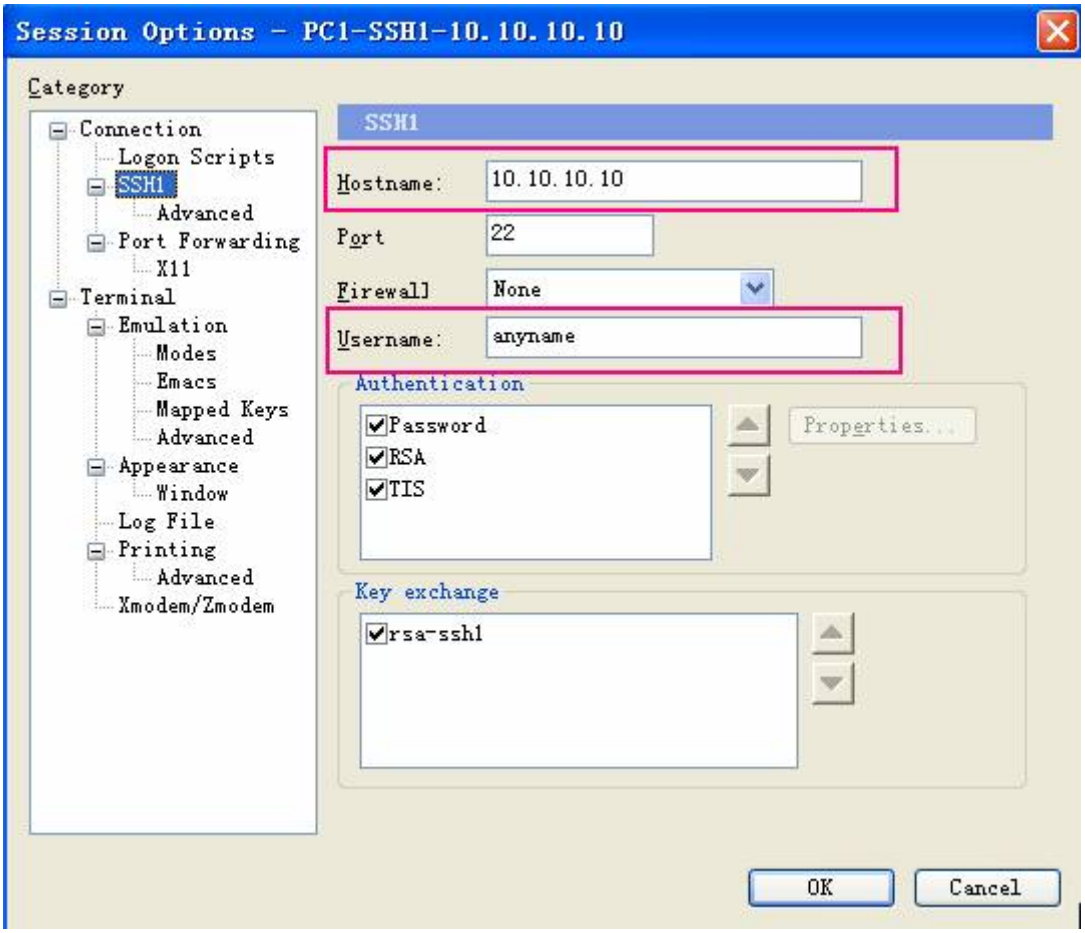
```
DES-7200(config)#line vty 1 4
DES-7200(config-line)#password pass
DES-7200(config-line)#privilege level 15
DES-7200(config-line)#exit
```

Configure SSH Client (PC1/PC2)

Open SecureCRT connection dialog box, as shown below. Use SSH1 for login authentication. Any session name can be specified (here the session name is configured as PC1-SSH1-10.10.10.10).



Configure SSH attributes. The host name is the IP address of SSH server (10.10.10.10 in this example). Since user name is not required by the currently-used authentication mode, you can type in any user name in the field of "User Name", but this field cannot be left blank (the user name is "anyname" in this example).



3.6.1.5 Verify Configurations

Verify the configurations of SSH Server

Step 1: Execute "show running-config" command to verify the current configurations:

```
DES-7200#show running-config

Building configuration...
vlan 1
!
enable secret 5 $1$eyy2$xs28FDw4s2q0tx97
enable service ssh-server
!
interface VLAN 1
 no ip proxy-arp
 ip address 10.10.10.10 255.255.255.0
line vty 0
 privilege level 15
 login
 password passzero
```

```
line vty 1 4
 privilege level 15
 login
 password pass
!
end
```

Verify the configurations of SSH Client

Step 1: Establish remote connection.

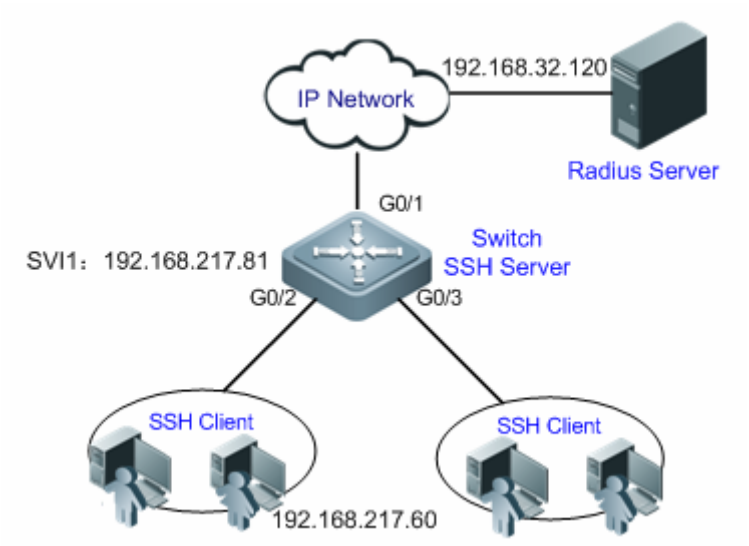
Establish connection and type in the correct password in order to enter the operating interface of SSH Server. The login password for line 0 is "passzero", and the login password for other four lines is "pass".

Step 2: Display login user.

```
DES-7200#show users
    Line       User       Host(s)           Idle      Location
   0 con 0                 idle              00:03:16
   1 vty 0                 idle              00:02:16   192.168.217.10
*  2 vty 1                 idle              00:00:00   192.168.217.20
```

3.6.2 Example of Configuring AAA Authentication for SSH

3.6.2.1 Topological Diagram



Networking diagram for AAA authentication for SSH

3.6.2.2 Application Requirements

As shown above, to ensure the security of information exchange, PC serves as SSH clients which will login the SSH Server of Switch using SSH protocol.

To better implement security management, SSH client adopts the AAA authentication mode. Meanwhile, for stability consideration, two authentication methods are configured in the AAA authentication method list: Radius server authentication and local authentication. Radius server will always be selected first, and the local authentication method will be selected later if no reply is received from Radius server.

3.6.2.3 Configuration Tips

1. The route from SSH client to SSH server and the route from SSH server to Radius client shall be reachable,
2. Complete SSH Server related configurations on Switch. The configuration tips have been described in the previous example, and won't be further introduced herein.
3. Complete AAA authentication related configurations on Switch. AAA defines ID authentication and type by creating the method list, which is then applied to the specific service or interface. Details are given in the section of "Configuration Steps".

3.6.2.4 Configuration Steps

The route from SSH client to SSH server and the route from SSH client to Radius server shall be reachable. Route related configurations won't be further introduced. Please refer to the section of route configuration in this manual.

Configure relevant SSH features on Switch

Step 1: Enable SSH Server

```
DES-7200(config)# enable service ssh-server
```

Step 2: Generate the key

! Generate RSA key

```
DES-7200(config)#crypto key generate rsa
% You already have RSA keys.
% Do you really want to replace them? [yes/no]:
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
```

```
% Generating 512 bit RSA1 keys ...[ok]
% Generating 512 bit RSA keys ...[ok]
```

! Generate DSA key

```
DES-7200(config)#crypto key generate dsa
Choose the size of the key modulus in the range of 360 to 2048 for your
Signature Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]:
% Generating 512 bit DSA keys ...[ok]
```

Step 3: Configure the IP address of device. The client will use this address to connect SSH server.

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
DES-7200(config-if-VLAN 1)#exit
```

Configure relevant features of AAA authentication on Switch

Step 1: Enable AAA on the device

```
DES-7200#configure terminal
DES-7200(config)#aaa new-model
```

Step 2: Configure information about Radius server (the shared key used by device for communicating with RADIUS server is "aaaradius"

```
DES-7200(config)#radius-server host 192.168.32.120
DES-7200(config)#radius-server key aaaradius
```

Step 3: Configure AAA authentication method list

! Configure login authentication method list (Radius first, followed by Local), and the name of method list shall be "method".

```
DES-7200(config)#aaa authentication login method group radius local
```

Step 4: Apply this method list to the line

```
DES-7200(config)#line vty 0 4
DES-7200(config-line)#login authentication method
DES-7200(config-line)#exit
```

Step 5: Configure local user database

! Configure local user database (configure user name and password, and bind the privilege level)

```
DES-7200(config)#username user1 privilege 1 password 111
DES-7200(config)#username user2 privilege 10 password 222
DES-7200(config)#username user3 privilege 15 password 333
```

! Configure local enable command for local enable authentication

```
DES-7200(config)#enable secret w
```

3.6.2.5 Verify Configurations

Step 1: Execute "show running-config" command to verify the current configurations:

```
DES-7200#show run

aaa new-model
!
aaa authentication login method group radius local
!
vlan 1
!
username user1 password 111
username user2 password 222
username user2 privilege 10
username user3 password 333
username user3 privilege 15

no service password-encryption
!
radius-server host 192.168.32.120
radius-server key aaaradius
enable secret 5 $1$hbgz$ArCsyqty6yyzzp03
enable service ssh-server
!
interface VLAN 1
 no ip proxy-arp
 ip address 192.168.217.81 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 192.168.217.1
!
line con 0
line vty 0 4
 login authentication method
!
end
```

Step 2: Configure Radius Server. This example configures the SAM server.

1. In "System Management-Device Management", type in device IP of "192.168.217.81" and device key of "aaaradius";

2. In "Security Management - Device Management Privilege", configure the privilege level for the login user;

3. In "Security Management - Device Administrator", type in the user name of "user" and password of "pass".

Step 3: Establish remote SSH connection on the PC.

1. SSH client configuration and connection establishment: please refer to the previous example.

2. Type in the correct password: "user" for SSH user name and "pass" for password. The user will login successfully.

Step 4: Display login user.

```
DES-7200#show users
   Line        User        Host(s)           Idle      Location
  0 con 0                  idle             00:00:31
 * 1 vty 0    user         idle             00:00:33   192.168.217.60
```

4 LINE Mode Configuration

4.1 Overview

This chapter describes some operations in LINE mode:

- Enter the LINE mode
- Increase/decrease LINE VTY
- Configure the protocols to communicate on the line
- Configure the ACLs on the line

4.2 Configuring LINE Mode

4.2.1 Entering the LINE mode

After entering the specific LINE mode, you can configure the specified line. Execute the following commands to enter the specified LINE mode:

Command	Function
DES-7200(config)# **line [console | vty]** *first-line* [*last-line*]	Enter the specified LINE mode.

4.2.2 Increasing/Decreasing LINE VTY

By default, the number of line vty is 5. You can execute the following commands to increase or decrease line vty, up to 36 line vty is supported.

Command	Function
DES-7200(config)# **line vty** *line-number*	Increase the number of LINE VTY to the specified value.
DES-7200(config)# **no line vty** *line-number*	Decrease the number of LINE VTY to the specified value.

4.2.3 Configuring the Protocols to Communicate on the Line

To restrain the communication protocol type supported on the line, you can use this command. By default, a VTY supports the communication of all protocols while a TTY do not support the communication of any protocol.

Command	Description
configure terminal	Enter the configuration mode.
line vty *line number*	Enter the line configuration mode.
transport input {**all	ssh	telnet	none**}	Configure the protocol to communicate on the line.
no transport input	Disable the communication of any protocol on the line.
default transport input	Restore the setting to the default value.

4.2.4 Configuring the Access Control List on the Line

To configure the access control list on the line, you can use the command. By default, no access control list is configured on the line.That is, all incoming and outgoing connections are permitted.

Command	Description
configure terminal	Enter the configuration mode.
line vty *line number*	Enter the line configuration mode.
access-class *access-list-number* **{in	out}**	Configure the access control list on the line.
no access-class *access-list-number* **{in	out}**	Remove the configuration.

5 System Upgrade Configuration

5.1 Understanding Program Image in the System

The system image contains DES-7200 firmware. All D-Link network devices are embedded with specific version of images before distribution. The user may upgrade such images to upgrade the device to the latest version. Use "show version" command to find out the version of images running on the device and the name of various main programs.

DES-7200 firmware involves the following types of images:

Main program: Also called MAIN, it is a complete image software package. It may contain such images as boot program, line card program and etc. It will be loaded and implement various services when device starts up. Users are generally using and operating on the main program.

BOOT： The most fundamental device initialization and boot program. This image is first image run on the device, and generally cannot be upgraded to ensure the system can always be initialized, guided and upgraded (CTRL) correctly. This image only exists in switching devices and line cards of the switch.

CTRL： This is a boot program provided with network functions. This program image is initialized by BOOT, and features network communication function and main program booting and upgrading function.

Bootloader: Device initialization, network communication and main program booting and upgrading function. This is the first image loaded when the device is powered on, and can boot the main program after device initialization. Routing devices only have Bootloader and Main program. Bootloader has all functions of BOOT and CTRL.

Among the aforementioned program images, only the main program can be viewed, upgraded and modified through file system commands. BOOT/CTRL/Bootloader programs are generally stored in the parallel flash and cannot be managed directly by user. For chassis devices, all line cards have BOOT and CTRL programs, while some

line cards may have the main program for line card. Generally, to have new features of a device, you will need to upgrade the main program of the device. In order to maintain the compatibility of BOOT, CTRL and Main programs, as well as the compatibility of the Main program of management board and line card, the upgrade function provides the guarantee to automatic compatibility. Incompatible parts will be upgraded automatically without the need to download upgrade image separately. During the upgrade process, images incompatible with the new-version software will be upgraded automatically. Therefore, the upgrade information of such images will be shown during the upgrade process.

5.1.1 Overview of Upgrade Function

5.1.1.1 Upgrading Image Set

Users generally expect to obtain a more reliable software version and more software features through upgrade. In most cases, these features are related to the main program. The device may contain multiple program images with different functions (such as BOOT/CTRL for booting), and these program images will only work in coordination. Therefore, the upgrade function not only provides the support to main program upgrade, but also allows the automatic synchronized upgrade of respective program images on the device, so that the overall device can maintain good compatibility.

Therefore, the upgrade file contains not only the main program for rendering primary services, but also the BOOT/CTRL images used in conjunction with the main program. When implementing upgrade, these images will be extracted from the upgrade file and upgrade the corresponding images on the device.

5.1.1.2 Auto-Installation

For devices like DES-7200, dynamic plug of linecards shall be supported. If the embedded image version of linecard plugged is incompatible with that of the device, the system will automatically upgrade the image of this linecard before it can work. Some versions of line cards can automatically download image to run from the master management board. This function avoids the need to consider the compatibility between different linecards and the device. The system can well guarantee image compatibility and consistency without the intervention of user.

5.1.1.3 Operating Principle

The firmware image release for DES-7200 devices is a self-extracting executable program. The firmware image carries the main program image for the device. For cabinet devices, the firmware image contains main program and boot program; for chassis devices, the firmware image contains the main program and boot program for respective line cards.

During the upgrade process, the user will first need to operate in the file system to copy the new-version firmware image to the device. The user can use this new program image to install the device. During the installation process, the system will automatically search for image to be upgraded and upgrade them one by one. The system will automatically guarantee the compatibility of respective images after the upgrade. No further identification by the user is needed.

As for the upgrade of stacked devices, when the main programs of member devices are different in version, the automatic installation process will start as well. The firmware image on the master device will be synchronized to salve devices having the inconsistent version of image, and installation will commence on these devices. After the installation, the entire stack of devices will be reset. When all devices enter into ready state, they will be running the identical main program.

As for chassis devices (such as DES-7200 series), the installation may be activated when a new line card is plugged. In case a line card is plugged when the device is still running, the service of this line card will be started if the system detects that this line card is compatible with the program image of current device, or use the line card program image contained in the firmware stored in the master management board to upgrade this line card or download the image if incompatible. The line card will be reset after the upgrade (no need to reset during image download) and will then enter into ready state. For such devices, the image used by line card or slave board always needs to maintain compatible with the program run on the master management board.

During system upgrade, the user may choose two different means: automatic installation and manual installation. The corresponding processes are shown below:

- Automatic installation: The new-version file is copied to the device -> reset device -> wait until device installation is completed
- Manual installation: The new-version file is copied to the device -> input install command -> reset device

Manual installation is only supported in version 10.4(2) and subsequent software versions for DES-7200 series. The advantage of manual installation is that the system services will not be affected during installation. If any accident incurs during the installation, as long as the device is powered on, the installation operation can be repeated without leading to any risk. Once the installation is completed successfully, the device can function immediately after restart. The manual installation is featured by shorter offline time and higher security.

Automatic installation is easy to operate, and no intervention by user is needed once the upgrade process commences.

Caution

For chassis devices, if the current boot/main program of master management board is upgraded, this upgrade file will also upgrade and replace the boot/main program of slave management board. However, if ISSU function is enabled, the system will no longer automatically upgrade the boot program of slave board, and manual upgrade by the user will be needed.

Note

Version 10.4(2) has well optimized and improved the upgrade function, including: safer and more reliable upgrade process, less times of device reset and service interruption, and easy-to-understand upgrade interface. Therefore, the upgrade interface is quite different before and after Version 10.4(2), but the operation steps of upgrade are compatible.

5.1.1.4 Protocol Specification

NA

5.2 Default Configurations

NA

5.3 Upgrade Steps

Device upgrade will require the following steps:

- Preparation before upgrade
- Copy image file to the device
- Device installation and upgrade
- Verify device installation

Note

Do not carry out upgrade or hot-plug/reset the line card when the device is extremely busy (with CPU utilization rate > 70%). This may lead to unsuccessful upgrade or boot failure of line card, including:

1. Reset line card or dynamically plug in the line card. If the CPU utilization rate is excessively high, the automatic upgrade of this line card or image distribution may fail. Please try to reset the line card again after the CPU utilization rate goes down, until the line card is successfully upgraded or booted.

2. During the process of manual upgrade, high CPU utilization rate will lead to the failure of upgrade. By this time, the user will need to retry manual upgrade after the CPU utilization rate goes down.

5.3.1 Preparation Before Upgrade

Make the following preparations before implementing device upgrade:

- Confirm the method of file download
- Confirm the space of file system
- Backup configuration file

Caution

The upgrade may fail if implemented when the device is busy or being attacked. Please use "show cpu" command to verify whether the system is busy or not, and implement upgrade when the CPU utilization rate is lower than 20%.

5.3.1.1 Confirm the Method of file Download

There are following means to download firmware image to the device:

- Download via TFTP server

This is the most commonly used method, which allows remote upgrade. First, make sure the server is already running TFTP server software (working in server mode), and then specify the directory for file download, which will need to store the firmware image file downloaded. Finally, confirm the TFTP server address and ensure the device side can visit this TFTP server.

Note

When user uses "copy tftp" command to download upgrade file from tftp server to the device (master management board) and at the same time overwrites the boot/main program, the system will check the validity of the upgrade file downloaded (i.e., whether inappropriate upgrade file is downloaded, or whether the upgrade file is corrupted). Upgrading of boot/main program via other means (such as ftp, xmodem and other file system commands) will not result in validity check. In addition, using "copy tftp" command to overwrite the boot image of slave board won't lead to the corresponding check as well.

Therefore, when selecting the download method, it is generally recommended to use "copy tftp" command to overwrite the boot image (master management board) of the device, as it is the safest upgrade method.

If the user doesn't want to use this download method, for device like DES-7200, we recommend you to adopt manual installation ("upgrade system" installation command) after copying the upgrade file to the device. Manual installation is safer, and allows the user to quickly discover image problems and timely correct such problems.

Caution

TFTP only supports the transfer of files with size below 32M. If the file size is larger than 32M, the file will have to be downloaded via FTP or flash disk.

- Download via xmodem

Xmodem download is applicable to some exceptional cases, such as the failure in network connection. Before using xmodem download, make sure the device is linked to console with serial line. In order to obtain faster download speed, the baud rate of connection can be increased. At the same time, make sure the terminal software supports xmodem transmission.

Caution

Using this method to copy upgrade file will not lead to validity check. In addition, this method cannot be used when there are two management boards.

- Copy via flash disk

Plug the flash disk stored with firmware image to the USB port. Make sure the device has found this USB apparatus.

Caution

Using this method to copy upgrade file will not lead to validity check. In addition, this method cannot be used when there are two management boards.

Supported by all devices provided with USB port.

- Download via FTP

Set the device as FTP server, and use FTP client to download upgrade file.

Caution

Using this method to copy upgrade file will not lead to validity check. In addition, this method cannot be used when there are two management boards.

5.3.1.2 Confirm the Space of File System

The user may use "show file system" or "dir" command to learn the space and its usage of the existing file system.

If the target file system has sufficient space to store both new and old program images, then during the upgrade process, the original boot/main program will be renamed as "original filename.bak". When the CTRL version is 10.4 or above, this file will be used as the backup image of new program image. When the new program image fails, the system will boot with this back image. This can save the rollback operation required in the case of upgrade failure.

When the system has hardly any residual space, the user will need to clean up the file system in order to make sure the upgrade is successful. Unnecessary files can be deleted using "del" command. While upgrading chassis device with dual management boards, the file system space of the slave board shall also be verified. The URL prefix of file system space of the slave board is "slave:".

Caution

When file system space is insufficient to store two program images, the backup file of original program image will not be generated.

Caution

Timely cleanup of file system will facilitate quick completion of upgrade. When the number and size of files in the file system are comparatively large, the booting speed of device will be subject to great influence. Before upgrade, delete unnecessary files as far as possible.

Installation of software with version older than 10.4(2) will leave such files as install_xxxx.bin on the management board of chassis device. After the software is upgraded to 10.4(2) or higher version, these files will become useless and shall be deleted manually in order not to slow down booting speed of system.

5.3.1.3 Backup Configuration File

Backup of configuration files is needed before the upgrade. Since different versions of software may contain different default configurations, the newly added default configurations may conflict with the current configurations. In order to ensure successful upgrade, please backup the original configuration file before the upgrade. After successful upgrade, verify whether there is any conflict in configurations.

5.3.2 Typical Upgrade Process

5.3.2.1 Manual Upgrade of Chassis Device

To ensure reliable upgrade, chassis devices generally adopt manual upgrade, which is supported by DES-7200 series of devices with current software version being 10.4(2) or above.

Steps of manual upgrade are shown below:

- Copy the new-version software to the device
- Input manual installation command to implement local installation
- Reset the device

The following is the example of manual installation:

Use "copy tftp" command to download software from tftp server to the device, and make sure the device and TFTP server are able to ping each other.

```
DES-7200#copy tftp://192.168.201.98/firmware.bin flash:firmware.bin
Accessing tftp://192.168.201.98/firmware.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 21525888 bytes.
Verify the system boot image .....[ok]
Upgrading system boot image on slave:/
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK -
21,525,888 bytes]
Waiting for image installed........Complete

CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20060062
  PRODUCT DESCRIPTION: DES-7200 High-density IPv6 10G Core Routing Switch(DES-7210)
By D-Link Corporation

SUCCESS: UPGRADING OK.
```

Note

When the device is plugged with two management boards, use "copy tftp" command will overwrite the boot/main program with new-version upgrade file, and the system will also synchronize this upgrade file to the slave board.

If "copy tftp" based installation is not used, the user will need to manually copy the upgrade file to the slave board to overwrite the boot image of the slave board (the filename of boot image of the slave board shall be learned in advance).

For example:

```
Copy flash:/firmwarebak.bin slave:/firmware.bin
```

After the new-version software is successfully downloaded to the device, use "upgrade" command to upgrade the system:

```
DES-7200#upgrade system firmware.bin
These images in linecard will be updated:
   Slot    image    linecard
   ----    -----    ----------------
      1    MAIN    7200-24
      6    MAIN    7200-24
-------------------------------------
(Slot 1): Installing MAIN
(Slot 1): Download image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!![OK - 8,003,872 bytes]
Waiting for image installed....Complete
(Slot 1): MAIN installed.
(Slot 1): All images have been installed.
(Slot 6): Installing MAIN
(Slot 6): Download image!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!![OK - 8,003,872 bytes]
Waiting for image installed....Complete
(Slot 6): MAIN installed.
(Slot 6): All images have been installed.
```

After the device is reset, the device will be running the new-version software.

Caution

After manual installation and before system reset, if you use "show version" command to check the software version, you may find out that versions of BOOT/CTRL images have been upgraded, while the version of main program image remains unchanged. This is because the system hasn't been reset to load and run the new main program image.

Caution

The user cannot use "upgrade system" command to degrade the system to software version older than 10.4(2). If the manually installed software is of version older than 10.4(2), the system will prompt the following error:

```
File [chars] format error. It's not an install package.
```

Therein, [chars] means the filename of current master program.

Caution

The interface prompts in the VSU status are different from that in the single-machine mode, such as the “Slot 1/2” indicates the card on the slot2 of the chassis1, while there is no chassis number in the single-machine mode.

5.3.2.2 Upgrade of Cabinet Device

Steps to upgrade the cabinet device:

- Copy the new-version software to the device
- Reset the device
- Wait for device installation

Upgrade to 10.4(2) or higher version

Copy the new-version software to the device:

```
DES-7200#copy tftp://192.168.201.98/DES-7200_V10.4(2)_R64047.bin
flash:firmware.bin
Accessing tftp://192.168.201.98/ DES-7200_V10.4(2)_R64047.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!
Other members are not present, quit synchronize...
Checking file, please wait for a few minutes ....
Check file success.

Transmission finished, file length 7243040

THE PROGRAM VERSION: 10.4.*, Release(64047)
Upgrade Master CM main program OK.
```

```
CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20110010
  PRODUCT DESCRIPTION: DES-7200 Gigabit Security & Intelligence Access Switch  By
D-Link Corporation

SUCCESS: UPGRADING OK.
```

Reset the device:

```
DES-7200# reload
```

Wait for device installation after device reboot:

In most cases, when upgrading older version to 10.4(2) or higher version, the device will become usable at once without any installation after device reset. The installation process will only show up in very few cases, and the system will display the following prompt of BOOT or CTRL image upgrade:

```
Upgrading CTRL...
DO NOT POWER OFF!
Erasing device...eeeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash #################### [OK - 1,215,488 bytes]
*Apr  1 07:32:44: %UPGRADE-5-LOCAL_FIN: New software image installed in flash.
```

Caution

When the system prompts any flash operation (such as "Erasing device" or "Writing flash" as shown above), never turn the device off. Any power failure during flash operation will lead to boot failure of device, and such failure cannot be recovered.

Degrade to 10.4(1) or older version

The degrading steps are exactly same as the upgrading steps. Only the interface of installation waiting process is different.

Copy the new-version software to the device:

```
DES-7200#copy tftp://192.168.201.98/s26_64047_install_10_4_1.bin
flash:firmware.bin
Accessing tftp://192.168.201.98/s26_64047_install_10_4_1.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 6128032 bytes.
Verify the system boot image .[ok]



CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20110010
  PRODUCT DESCRIPTION: DES-7200 Gigabit Security & Intelligence Access Switch  By
D-Link Corporation

SUCCESS: UPGRADING OK.
```

Reset the device:

```
DES-7200#reload
```

Wait for device installation after device reboot:

After reboot, the device will automatically commence local image installation. For example:

```
Prepare installation data ...
Load install package file firmware.bin OK!
Installation is in process ...
ATTENTION: Do not restart your machine before finish !
Upgrading main ...
Size of main file firmware.bin is 10406464 Bytes
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Checking file, please wait for a few minutes ....
Check file success.
Upgrade main succeed.
Installation process finished successfully ...
```

Upon completion of automatic installation, the system will reset the device automatically.

```
SYS-5-RESTART: The device is restarting. Reason: Upgrade product !.
```

After the reset, the device will enter into ready state.

5.3.2.3 Automatic Upgrade of Chassis Device

Upgrade steps

Steps to upgrade the chassis device:

- Copy the new-version software to the device
- Reset the device
- Wait for device installation

Upgrade to 10.4(2) or higher version

Copy the new-version software to the device:

```
DES-7200#copy tftp://192.168.201.97/firmware.bin flash:firmware.bin
Accessing tftp://192.168.201.97/firmware.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!Checking file, please wait for a few minutes ....
Check file success.

Transmission finished, file length 22655264

THE PROGRAM VERSION: 10.4.*, Release(64046)

Upgrade file to Module(s) in slot: [M2]
Please wait......
Upgrade file to Module in slot [M2] OK!
Upgrade Master CM main program OK.

CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20060062
  PRODUCT DESCRIPTION: DES-7200 High-density IPv6 10G Core Routing Switch(DES-7210)
By D-Link Corporation

SUCCESS: UPGRADING OK.
```

Reset the device:

```
DES-7200#reload
```

Wait for automatic installation of device:

After entering the main program, the main management board will implement local installation first:

```
*Apr  1 07:32:17: %UPGRADE-5-LOCAL_BEG: Installing: 'flash: CTRL'.
*Apr  1 07:32:17: %UPGRADE-5-LOCAL: Upgrading CTRL.
Upgrading CTRL...
DO NOT POWER OFF!
Erasing device...eeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ################### [OK - 1,215,488 bytes]
*Apr  1 07:32:44: %UPGRADE-5-LOCAL_FIN: New software image installed in flash.
```

Upon completion of local installation, the system will verify whether the boot/ctrl/main programs of all line cards and the slave board need to be installed and complete the corresponding installation automatically. This automatic installation process will generally take place when the current device version is lower than 10.4(2).

```
These images in linecard will be updated:
Slot    image    linecard
----    -----    ----------------
  3     MAIN       7200-24
 M2     CTRL       7200-CM4
--------------------------------
*Aug  7 07:46:25: %UPGRADE-5-SLOT_BEG: (Slot 3): Installing MAIN
(Slot 3): Download image
*Aug  7 07:47:21: %UPGRADE-5-SLOT_SUCC: (Slot 3): MAIN installed.
*Aug  7 07:47:21: %UPGRADE-5-SLOT_FIN: (Slot 3): All images is installed.
*Aug  7 07:47:21: %UPGRADE-5-RESET_CARD: (Slot 3): Reset.
*Aug  7 07:47:26: %UPGRADE-5-SLOT_BEG: (Slot M2): Installing CTRL
(Slot M2): Download image!!!!!!!!!!!!!!!!!!![OK - 1,215,232 bytes]
Waiting for image installed...Complete
Erasing device...eeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ################# [OK - 1,215,488 bytes]
*Aug  7 07:48:00: %UPGRADE-5-SLOT_SUCC: (Slot M2): CTRL installed.
*Aug  7 07:48:00: %UPGRADE-5-SLOT_FIN: (Slot M2): All images is installed.
*Aug  7 07:48:00: %UPGRADE-5-RESET_CARD: (Slot M2): Reset.
```

The upgrade of old-version line card will need two reboots. The line card will reboot automatically after the main program has been installed. After reentering the main program, the boot or ctrl image will be installed.

```
These images in linecard will be updated:
   Slot    image    linecard
   ----    -----    ----------------
```

```
      3   CTRL   7200-24
-------------------------------------
*Aug  7 07:48:09: %UPGRADE-5-SLOT_BEG: (Slot 3): Installing CTRL
(Slot 3): Download image!!!!!!!!!!!!!!!!!![OK - 1,087,744 bytes]
Waiting for image installed...Complete
Erasing device...eeeeeeeeeeeeeeeeeeeeeeeeee [ok]
Writing flash ################ [OK - 1,088,0 bytes]
*Aug  7 07:48:37: %UPGRADE-5-SLOT_SUCC: (Slot 3): CTRL installed.
*Aug  7 07:48:37: %UPGRADE-5-SLOT_FIN: (Slot 3): All images is installed.
*Aug  7 07:48:37: %UPGRADE-5-RESET_CARD: (Slot 3): Reset.
```

Upon completion of installation, normal services can start directly without the need to reset the device.

Degrade to 10.4(1) or older version

Copy the new-version software to the device:

Use "copy" command to copy the old edition software of 10.4(1) to the device.

```
DES-7200#copy tftp://192.168.201.97/firmware.bin flash:firmware.bin
Accessing tftp://192.168.201.97/ firmware.bin ...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 22815872 bytes.
Verify the system boot image .....[ok]
Upgrading system boot image on slave:/
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!![OK - 22,815,872 bytes]
Waiting for image installed........Complete

CURRENT PRODUCT INFORMATION :
  PRODUCT ID: 0x20060062
```

```
  PRODUCT DESCRIPTION: DES-7200 High-density IPv6 10G Core Routing Switch(DES-7210)
By D-Link Corporation


SUCCESS: UPGRADING OK.
```

Reset the device:

```
DES-7200#reload
```

Wait for automatic installation of device:

The following installation information will prompt after device reboot:

```
Prepare installation data ...

Load install package file firmware.bin OK!

Installation is in process ...

ATTENTION: Do not restart your machine before finish !

Upgrading main ...

Size of main file firmware.bin is 8914464 Bytes

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

Checking file, please wait for a few minutes ....

Check file success.

Upgrade main succeed.

Upgrading file install_lc_200e0020.bin ...

Write executable file install_lc_200e0020.bin to file system.

Checking file, please wait for a few minutes ....

Check file success.

Upgrade file install_lc_200e0030.bin succeed.

Upgrading file install_lc_20070010.bin ...
```

```
Write executable file install_lc_20070010.bin to file system.

Checking file, please wait for a few minutes ....

Check file success.

Upgrade file install_lc_20070010.bin succeed.

Installation process finished successfully ...
```

The system will reset automatically upon completion of installation:

```
SYS-5-RESTART: The device is restarting. Reason: Upgrade product !.
```

After entering into the main program, the master management board will synchronize new-version program image to line cards:

```
*Apr   1 06:11:30: %7: Card in slot [1] CPU 0 need to do version
synchronization ...Current software version :

*Apr  1 06:11:30: %7:  BOOT VERSION: 10.4.63238

*Apr  1 06:11:30: %7:  CTRL VERSION: 10.4.63967

*Apr  1 06:11:30: %7:  MAIN VERSION: 10.4.63967

*Apr  1 06:11:30: %7: Need update to software version :

*Apr  1 06:11:30: %7:  BOOT VERSION: 10.4.59831

*Apr  1 06:11:30: %7:  CTRL VERSION: 10.4.59831

*Apr  1 06:11:30: %7:  MAIN VERSION: 10.4.61477

*Apr  1 06:11:41: %7: Install package transmission begin, wait please ...

*Apr  1 06:11:41: %7: Transmitting install package file to slot [1] ...

*Apr  1 06:11:41: %7: Transmitting file install_lc_20070010.bin;

*Apr  1 06:12:02: %7: Transmitting install package file to slot [1] OK ...

*Apr  1 06:12:02: %7: Install package transmission finished, system will reset
cards ...

*Apr  1 06:12:03: %7: Reset card in slot [1]

*Apr  1 06:12:03: %7: Software installation is in process, wait please ...

*Apr  1 06:12:03: %7: Installing, wait please !

*Apr  1 06:12:04: %OIR-6-REMCARD: Card removed from slot 1, interfaces disabled.

*Apr  1 06:12:13: %7: Installing, wait please !

*Apr  1 06:14:03: %7: Installing, wait please !

*Apr  1 06:14:13: %7: Installing, wait please !

*Apr  1 06:14:18: %OIR-6-INSCARD: Card inserted in slot 1, interfaces are now
online.
```

```
*Apr  1 06:14:18: %AUTO_UPGRADE-6-VER_SYNC_SUCCEED: Version synchronization for
line card in slot [1] has been succeeded.
```

5.3.2.4 Dynamic Linecard Plug-in

When linecard is dynamically inserted in DES-7200 device, the system will automatically check the software version of this linecard. If its software version is incompatible with that of master management board, then this card will be automatically upgraded by the system before operation.

The following is an example of dynamically inserting a line card with incompatible software version in the DES-7200 device (running 10.4(1) or older version):

```
*Apr  1 06:17:31: %7: MODULE-6-INSTALL: Install Module 7200-24 in slot 5.
*Apr  1 06:17:33: %OIR-6-INSCARD: Card inserted in slot 5, interfaces are now
online.
*Apr  1 06:17:33: %7: Card in slot [5] CPU 0 need to do version
synchronization ...Current software version :
*Apr  1 06:17:33: %7:  BOOT VERSION: 10.4.59831
*Apr  1 06:17:33: %7:  CTRL VERSION: 10.4.64046
*Apr  1 06:17:33: %7:  MAIN VERSION: 10.4.63967
*Apr  1 06:17:33: %7: Need update to software version :
*Apr  1 06:17:33: %7:  BOOT VERSION: 10.4.59831
*Apr  1 06:17:33: %7:  CTRL VERSION: 10.4.59831
*Apr  1 06:17:33: %7:  MAIN VERSION: 10.4.61477
*Apr  1 06:17:33: %7: Install package transmission begin, wait please ...
*Apr  1 06:17:33: %7: Transmitting install package file to slot [5] ...
*Apr  1 06:17:33: %7: Transmitting file install_lc_20070010.bin;
*Apr  1 06:17:59: %7: Transmitting install package file to slot [5] OK ...
*Apr  1 06:17:59: %7: Install package transmission finished, system will reset
cards ...
*Apr  1 06:17:59: %7: Reset card in slot [5]
*Apr  1 06:17:59: %7: Software installation is in process, wait please ...
*Apr  1 06:17:59: %7: Installing, wait please !
*Apr  1 06:18:01: %OIR-6-REMCARD: Card removed from slot 5, interfaces disabled.
*Apr  1 06:18:09: %7: Installing, wait please !
*Apr  1 06:19:29: %7: Installing, wait please !
*Apr  1 06:19:39: %7: Installing, wait please !
*Apr  1 06:19:49: %7: Installing, wait please !
*Apr  1 06:19:59: %7: Installing, wait please !
*Apr  1 06:20:08: %OIR-6-INSCARD: Card inserted in slot 5, interfaces are now
online.
```

```
*Apr  1 06:20:08: %AUTO_UPGRADE-6-VER_SYNC_SUCCEED: Version synchronization for
line card in slot [5] has been succeeded.
```

The following is an example of dynamically inserting a line card with incompatible software version in the DES-7200 device (running 10.4(2) or higher version):

```
These images in linecard will be updated:

   Slot    image    linecard

   ----    -----    ----------------

      3    MAIN    7200-24

-------------------------------------

*Aug  7 07:46:25: %UPGRADE-5-SLOT_BEG: (Slot 3): Installing MAIN

(Slot 3): Download image

*Aug  7 07:47:21: %UPGRADE-5-SLOT_SUCC: (Slot 3): MAIN installed.

*Aug  7 07:47:21: %UPGRADE-5-SLOT_FIN: (Slot 3): All images is installed.

*Aug  7 07:47:21: %UPGRADE-5-RESET_CARD: (Slot 3): Reset.
```

The following is an example of dynamically inserting a line card with compatible software version (only when the master management board is running 10.4(2) or higher version):

```
*Apr  2 07:39:06: %UPGRADE-5-DISPATCH_BEGIN: Dispatch image to slot 3.

Download image to slot 3: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

!!!!!!!!!!!!!!!!!!!![OK - 8,007,680 bytes]
```

Waiting for image installed....Complete

Caution

When line card inserted cannot be supported by the existing master management board, the system will prompt:

```
UPGRADE-4-CARDNOTSUPPORT: The linecard in slot 1/4 is not
supportted by current version.
```

5.3.2.5 Upgrade of Stacked Devices

Upgrade of stacked devices will be activated under the following two circumstances:

- Upgrade of all stacked devices

This case is applicable to the upgrade of devices having completed stacking. The upgrade steps are same as those of cabinet devices.

- Upgrade during the stacking process

The stacked devices are required to have the same software version. Otherwise, the system will automatically upgrade devices with inconsistent software version during the stacking process (subject to the software version of master device or the highest version).

During the automatic installation process of stacked devices, apart from the installation information of master device, the interface will also prompt the installation information of slave devices:

```
*Jan 2 00:01:39:%STACK-5-INST: (Device 2): Install  CTRL.
*Jan 2 00:03:39:%STACK-5-INST: (Device 2): Install  SYSINFO.

*Jan 2 00:06:40:%STACK-5-FINISH: All software images installed.
```

When the system prompts "`All software images installed`", it means that all stacked devices have completed installation, and system service can be expanded.

5.3.3 Verify Device Installation

After the system installation, the user may use the **show version** command to verify the conditions of device upgrade, and make sure the version of main program is same as the anticipated version. It is normal that the versions of BOOT, CTRL and Bootloader programs and the image of line card may be different from the version of the main program package.

The diaplayed main program version indicates the version number of main program being run in the system. Therefore, in the case of manual installation, the displayed version number of main program is not the version number of software newly installed, but the version number of software run currently.

For cabinet device, if the line card automatic installation process begins, the line card will be reset and execute the new program. The user needs to wait until the line card enters into UP state and then uses **show version** command to verify its version number.

The following is an example of executing **show version** command on DES-7200 device with two management boards and two line cards:

```
DES-7200#sh version
System description     : DES-7200 High-density IPv6 10G Core Routing
Switch(DES-7210) By D-Link Corporation
System start time      : 2008-01-04 3:20:23
System uptime          : 0:15:35:55
System hardware version : 1.0
```

```
System software version : 10.4(2) Release(64533)
System BOOT version    : 10.4 Release(59831)
System CTRL version    : 10.4(2) Release(64533)
Module information:
  Slot-7 : 7200-48
    Hardware version : 1.0
    Software version : 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4(2) Release(64533)
  Slot-8 : 7200-24GE
    Hardware version : 2.0
    Software version : 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4(2) Release(64533)
  Slot-M1 : 7200-CM4
    Hardware version : 1.0
    Software version : 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4(2) Release(64533)
  Slot-M2 : 7200-CM4
    Hardware version : 1.0
    Software version : 10.4(2) Release(64533)
    BOOT version    : 10.4 Release(59831)
    CTRL version    : 10.4(2) Release(64533)
```

Note

When using "show version" command to show the version number of image with version older than 10.4(2), the system cannot display the release version marking of this image. The release version marking indicates the release time of this image, and is shown in the brackets after the version number. For example, in the version number of 10.4(2), "2" is the release version marking.

For instance, when using "show version" command, versions older than 10.4(2) will display the version number of 10.4 Release (59831) or 10.4.59831, while the versions higher than 10.4(2) will display the version number of 10.4(2) release (59381).

Caution

For versions higher than 10.4(2), no reset operation will be needed after the installation. To verify whether the automatic installation process of chassis device is completed, check if the installation list information shown during the installation process indicates the end of operation, or use "show version" command to check whether each card on the device is ready.

5.4 Common Upgrade Problems

5.4.1 Loss of Main Program of Master Management Board

The user may accidentally delete the boot/main program of the file system, and the system will give the following warning information:

```
Warning: System boot file firmware.bin is missing.
```

However, if the user doesn't notice such loss of main program and dynamically inserts a new line card during the subsequent use, the system will prompt:

```
*Aug 25 13:21:50: %UPGRADE-3-DISPATCH_FAIL: Dispatch program to slot 3 failed.
```

Caution

The aforementioned prompt and function are only supported by products running 10.4(2) or higher version.

5.4.2 Unsupported Line cards

If the line card detected be device is not supported by the current software version, the system will prompt:

```
*Jan 2 00:00:39: %UPGRADE-4-CARDNOTSUPPORT: The linecard in slot [dec/dec/...] is
not supportted by current version.
```

In such a case, support to such type of line card as specified in the release of current software version shall be verified. If this line card needs to be supported, then the current software shall be upgraded.

Caution

The potential problem of degrading is: line card supported by higher version software may not be supported by the degraded software version. In such a case, when using "copy tftp" command to copy lower version software to the device, the system will give the following warning:

```
Warning: 7200-24 in slot 1 is not support by firmware.bin
```

5.4.3 Insufficient File System Space

Insufficient file system space may take place during download or file copying. The system will prompt:

```
Insufficient file system space。
```

By this time, useless files on the file system shall be cleaned up. For device with smaller file system space, the current boot/main program can be deleted as long as the device is powered on, and then use "copy tftp" command to copy the new upgrade file to the device as the new boot/main program.

5.4.4 Boot/main Program not Overwritten during Upgrade

If the boot/main program is not upgraded during the upgrade, the new program will not run after system reboot.

As for the slave board, please verify the name of boot/main program before upgrade. If the boot/main program is not upgraded, the software versions of master and slave boards may be inconsistent after system reboot.

5.4.5 Boot/main Program Name Error

The user may use the **boot system** command to set a nonexistent boot/main program.

```
Warning: System boot file xxx is missing.
```

By this time, the user needs to verify whether the configured filename is correct, and shall especially pay attention to the case-sensitive problem.

5.4.6 Timeout Failure Displayed during Upgrade

The timeout failure may be displayed during the upgrade.

```
*Feb 10 15:47:12: %UPGRADE-4-PROTO_TIMEOUT: Server is busy and ack timeout.
```

By this time, the following solutions can be used:

1. Ensure whether the boardcards to be upgraded are plugged or reset.
2. Ensure whether the boardcards to be upgraded are busy (with high CPU utilization rate)
3. Ensure whether the boardcards to be upgraded are using large file system space, if so, remove some useless files, and retry the upgrade after freeing the file system space.

6 Network Communication Detection Tools

6.1 Ping Connectivity Test

To test the connectivity of a network, many network devices support the **Echo** protocol. The protocol sends a special packet to a specified network address and waits for a response. This allows you to evaluate the connectivity, delay and reliability of a network. The ping tool provided by DES-7200 can effectively help users diagnose and locate the connectivity problems in a network.

The **Ping** command runs in the user EXEC mode and privileged EXEC mode. In the user EXEC mode, only basic ping functions are available. However, in the privileged EXEC mode, extended ping functions are available.

Command	Function
DES-7200# **ping [vrf** *vrf-name***]** [**ip**] [*address* [**length** *length*] [**ntimes** *times*] [**data** *data*][**source** *source*] [**timeout** *seconds*] [**df-bit**] [**validate**]]	Test the network connectivity.

The basic ping function can be performed in either the user EXEC mode or the privileged EXEC mode. By default, this command sends five 100-byte packets to the specified IP address. If the system receives a response within the specified time (2 seconds by default), it shows "!" . Otherwise, it shows ".". Finally, the system shows statistics. This is a normal ping example:

```
DES-7200# ping 192.168.5.1
Sending 5, 100-byte ICMP Echoes to 192.168.5.1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The extended ping function can be performed in the privileged EXEC mode only. This function allows you specify the number of packets, packet length, and timeout. As with the basic ping function, the extended ping also shows statistics. The following is an example of the extended ping:

```
DES-7200 ping 192.168.5.197 length 1500 ntimes 100 data ffff source
192.168.4.190 timeout 3
Sending 100, 1000-byte ICMP Echoes to 192.168.5.197, timeout is 3 seconds:
  < press Ctrl+C to break >
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
DES-7200#
```

6.2 Ping IPv6 Connectivity Test

To test the connectivity of a network, many network devices support the **Echo** protocol. The protocol sends a special packet to a specified network address and waits for a response. This allows you to evaluate the connectivity, delay and reliability of a network. The ping tool provided by DES-7200 can effectively help users diagnose and locate the connectivity problems in a network.

The **Ping ipv6** command runs in the user EXEC mode and privileged EXEC mode. In the user EXEC mode, only basic ping IPv6 functions are available. However, in the privileged EXEC mode, extended ping IPv6 functions are available.

Command	Function
DES-7200# **ping ipv6** [*address* [**length** *length*] [**ntimes** *times*] [**data** *data*][**source** *source*] [**timeout** *seconds*]]	Test the network connectivity.

The basic ping function can be performed in either the user EXEC mode or the privileged EXEC mode. By default, this command sends five 100-byte packets to the specified IP address. If the system receives a response within the specified time (2 seconds by default), it shows "!" . Otherwise, it shows ".". If the response does not match the request, the system shows “C” and outputs statistics. This is a normal ping example:

```
DES-7200# ping ipv6 2000::1
Sending 5, 100-byte ICMP Echoes to 2000::1, timeout is 2 seconds:
< press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The extended ping function can be performed in the privileged EXEC mode only. This function allows you specify the number of packets, packet length, and timeout. As with the basic ping function, the extended ping also shows statistics. The following is an example of the extended ping:

```
DES-7200# ping ipv6 2000::1  length 1500 ntimes 100 data ffff source 2000::2
timeout 3
Sending 100, 1000-byte ICMP Echoes to 2000::1, timeout is 3 seconds:
  < press Ctrl+C to break >
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 2/2/3 ms
```

6.3 Traceroute Connectivity Test

The **Traceroute** command is mainly used to check the network connectivity. It shows all the gateways that a packet passes through from the source to the destination and exactly locates the fault when the network fails.

One of the network transmission rules is that the number in the TTL field in the packet will decrease by 1 every time when a packet passes through a gateway. When the number in the TTL field is 0, the gateway will discard this packet and send an address unreachable error message back to the source. According to this rule, the execution of the traceroute command is as follows: At first, the source sends a packet whose TTL is 1 to the destination address. The first gateway sends an ICMP error message back, indicating that this packet cannot be forwarded for TTL timeout. Then, the first gateway re-sends the packet after the TTL domain adds 1. Likewise, the second gateway returns a TTL timeout error and the process lasts until the packet reaches the destination address. By recording every address returning the ICMP TTL timeout message, you can draw the entire path passed by the IP packet from the source address to the destination address.

The **traceroute** command can run in the user EXEC mode and the privileged EXEC mode. The command format is as follows:

Command	Function
DES-7200# **traceroute** [*protocol*] [*address*] [**probe** *probe*] [**ttl** *minimum maximum*] [**source** *source*] [**timeout** *seconds*]]	Trace the path that a packet passes through.

The following are two examples that apply **traceroute**. In one example, network connectivity is good. In another example, some gateways in a network are not connected.

1. **traceroute** example where network connectivity is good:

```
DES-7200# traceroute 61.154.22.36
  < press Ctrl+C to break >
Tracing the route to 61.154.22.36
1     192.168.12.1        0 msec   0 msec   0 msec
2     192.168.9.2         4 msec   4 msec   4 msec
3     192.168.9.1         8 msec   8 msec   4 msec
4     192.168.0.10        4 msec   28 msec  12 msec
5     202.101.143.130     4 msec   16 msec  8 msec
6     202.101.143.154     12 msec  8 msec   24 msec
7     61.154.22.36        12 msec  8 msec   22 msec
```

As you can see, to access the host with an IP address of 61.154.22.36, the network packet passes throuth gateways 1 to 6 from the source address.

Meanwhile, you can know the time that the network packet spennds to reach a gateway. This is very useful for network analysis.

2. traceroute example where some gateways in a network are not connected:

```
DES-7200# traceroute 202.108.37.42
< press Ctrl+C to break >
Tracing the route to 202.108.37.42
1     192.168.12.1        0 msec   0 msec   0 msec
2     192.168.9.2         0 msec   4 msec   4 msec
3     192.168.110.1       16 msec  12 msec  16 msec
4     *  *  *
5     61.154.8.129        12 msec  28 msec  12 msec
6     61.154.8.17         8 msec   12 msec  16 msec
7     61.154.8.250        12 msec  12 msec  12 msec
8     218.85.157.222      12 msec  12 msec  12 msec
9     218.85.157.130      16 msec  16 msec  16 msec
10    218.85.157.77       16 msec  48 msec  16 msec
11    202.97.40.65        76 msec  24 msec  24 msec
12    202.97.37.65        32 msec  24 msec  24 msec
13    202.97.38.162       52 msec  52 msec  224 msec
14    202.96.12.38        84 msec  52 msec  52 msec
15    202.106.192.226     88 msec  52 msec  52 msec
16    202.106.192.174     52 msec  52 msec  88 msec
17    210.74.176.158      100 msec 52 msec  84 msec
18    202.108.37.42       48 msec  48 msec  52 msec
```

As you can see, to access the host with an IP address of 202.108.37.42, the network packet passes through gateways 1 to 17 from the source address and there is failure in gateway 4.

6.4 Traceroute IPv6 Connectivity Test

The **Traceroute ipv6** command is mainly used to check the network connectivity. It shows all the gateways that a packet passes through from the source to the destination and exactly locates the fault when the network fails.

For network transmission, refer to the previous section.

The **traceroute ipv6** command can run in the user EXEC mode and the privileged EXEC mode. The command format is as follows:

Command	Function
DES-7200# **traceroute ipv6** [*address* [**probe** *probe*] [**ttl** *minimum maximum*] [**timeout** *seconds*]]	Trace the path that a packet passes through.

The following are two examples that apply **traceroute ipv6**. In one example, network connectivity is good. In another example, some gateways in a network are not connected.

1. **traceroute ipv6** example where network connectivity is good:

```
DES-7200# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1        0 msec  0 msec  0 msec
2     3001::1        4 msec  4 msec 4 msec
3     3002::1        8 msec  8 msec  4 msec
4     3004::1        4 msec  28 msec  12 msec
```

As you can see, to access the host with an IP address of 3004::1, the network packet passes throuth gateways 1 to 4 from the source address. Meanwhile, you can know the time that the network packet spennds to reach a gateway. This is very useful for network analysis.

2. **traceroute ipv6** example where some gateways in a network are not connected:

```
DES-7200# traceroute ipv6 3004::1
  < press Ctrl+C to break >
Tracing the route to 3004::1
1     3000::1        0 msec  0 msec  0 msec
2     3001::1        4 msec  4 msec 4 msec
3     3002::1        8 msec  8 msec  4 msec
4     * * *
5     3004::1        4 msec  28 msec  12 msec
```

As you can see, to access the host with an IP address of 3004::1, the network packet passes through gateways 1 to 5 from the source address and there is failure in gateway 4.

DES-7200

Ethernet Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

Note

Descript, prompt, tip or any other necessary supplement or explanation for the operation.

Note

The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products.

The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 Interface Configuration

1.1 Overview of Interface Types

This chapter classifies the interfaces used on DES-7200 devices and defines interface types. Interfaces on DES-7200 devices are divided into two types:

- L2 Interfaces
- L3 Interfaces (supported on layer 3 devices)

1.1.1 L2 Interfaces

This section presents the types of L2 interfaces and their definitions. L2 interfaces fall into the following types

- Switch Port
- L2 Aggregate Ports

1.1.1.1 Switch Port

Switch port refers to a single physical port of only layer 2 switching function on the device. This port can either be an Access Port or a Trunk Port. You can configure a port to be an Access Port or a Trunk Port by using the **Switch Port** command in the interface configuration mode. Switch port is used to manage a physical interface and relevant layer 2 protocols rather than handling routing or bridging.

1.1.1.2 Access Port

An access port belongs to only one VLAN that transports only the frames belonging to the same VLAN.Typically, it is used to connect computers.

Default VLAN

An access port belongs to only one VLAN. Therefore, its default VLAN is the VLAN where it locates. You do not need to configure it.

Receiving and sending frames

An access port sends untagged frames and receives frames in the following three formats only:

Untagged frame

- Untagged frames
- Tagged frames whose VID is the VLAN where the access port locates
- Tagged frames whose VID is 0

Untagged frame

An access port receives untagged frames and then adds the tag of the default VLAN to them. The added tag will be removed before the access port sends them out.

Tagged frame

An access port handles tagged frames in the following ways:

- When the VID (VLAN ID) of the tag is the same as the default VLAN ID, the access port receives the frame and removes the tag before sending it out.
- When the VID (VLAN ID) of the tag is 0, the access port receives the frame. In the tag, VID=0 is used to prioritize the frame.
- When the VID (VLAN ID) of the tag is different from the default VLAN ID and is not 0, this frame is discarded.

1.1.1.1.2 Trunk Port

A trunk port can belong to multiple VLANs that receives and sends frames belonging to multiple VLANs. Generally, it is used to connect devices or computers.

Default VLAN

Because a trunk port can belong to multiple VLANs, you need to set a native VLAN as the default VLAN. By default, the trunk port transmits the frames of all VLANs. In order to reduce device load and minimize waste of bandwidth, you can set a VLAN allowance list to specify the frames of which VLANs the trunk port can transmit.

Caution

It is recommended to set the native VLAN of the trunk port on the local device to be consistent with that of the trunk port on the remote device. Otherwise, the trunk port cannot forward packets properly.

Receiving and sending frames

The trunk port can receive untagged frames and the tagged frames of the VLANs permitted by the port. All the frames of non-native VLANs sent by the trunk port are tagged, and the frames of native VLAN are untagged.

Untagged frame

If a trunk port receives a frame without IEEE802.1Q TAG, this frame will be transmitted in the native VLAN of the port.

Tagged frame

If a trunk port receives a tagged frame, it handles the frame in the following ways:

- When the trunk port receives a tagged frame whose VID is the same as that of its native VLAN, this frame is accepted. The tag will be removed before it sends the frame.
- When the trunk port receives a tagged frame whose VID is different from that of its native VLAN but is permitted by the port, the frame is accepted. The tag is kept unchanged when it sends the frame.
- When the trunk port receives a tagged frame whose VID is different from that of its native VLAN and is not permitted by the port, the frame is discarded.

Note

Untagged packets are ordinary Ethernet packets that can be recognized by the network cards in PCs for communication. Tagging refers to append four bytes of VLAN information, namely the VLAN tag header, at the end of the source MAC address and the destination MAC address.

1.1.1.1.3 Hybrid port

A hybrid port can belong to multiple VLANs that receives and sends packets of multiple VLANs. It can be used to connect devices or computers. The difference between the hybrid port and the trunk port is that the hybrid port sends the untagged frames of multiple VLANs, but the trunk port sends only the untagged frames of the default VLAN. Note that the VLAN that a hybrid port is going to join must already exist.

1.1.1.3 L2 Aggregate Port

An aggregate port consists of several physical ports. Multiple physical connections can be bound into a simple logical connection, which is called an aggregate port (hereinafter referred to as AP).

For layer 2 switching, an AP works like a switch port of high brandwidth. It increases link bandwidth by using the bandwidth of multiple ports together. In addition, the frames that pass through the L2 aggregate port will undergo traffic balancing on the member ports of the L2 aggregate port. If one member link of AP fails, the L2 aggregate port automatically transfers the traffic on this link to other working member links, making the connection more reliable.

Caution

The member port of the L2 aggregate port can be either access port or trunk port. However, the member ports in one AP must be of the same type, namely, all the ports are either access ports or trunk ports.

1.1.2 L3 Interfaces

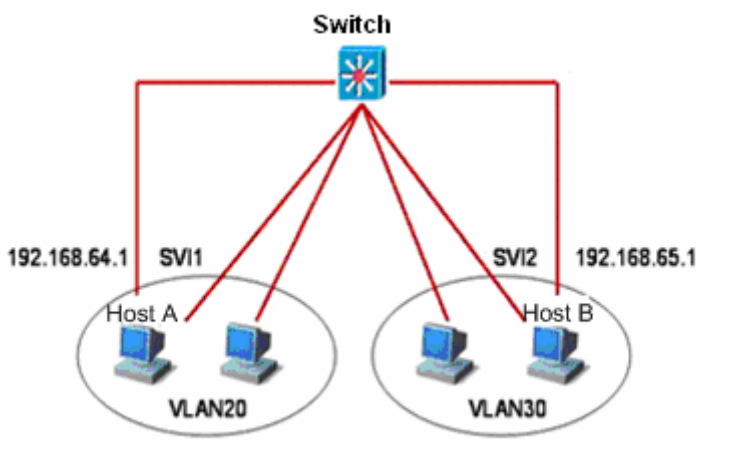
This section discusses the types and definitions of L3 interfaces. L3 interfaces fall into the following categories.

- SVI (Switch virtual interface)
- Routed Port
- L3 Aggregate Ports

1.1.2.1 SVI (Switch virtual interface)

SVI, short for Switch Virtual Interface, is used to implement the logical interface for layer 3 switching. SVI can work as the local management interface through which administrator can manage devices. You can also create SVI as a gateway interface that serves as the virtual sub-interface of each VLAN. It can be used for inter-VLAN routing on layer 3 device. A SVI can be created simply by using the **interface vlan** command in the interface configuration mode. Then an IP address is assigned to the SVI to establish a route between VLANs.

As the following figure depicts, the hosts of VLAN20 can communicate to each other directly without routing through an L3 device. If host A in VLAN20 wants to communicate with host B in VLAN30, it must route through SVI1 corresponding to VLAN20 and SVI2 corresponding to VLAN30.



1.1.2.2 Routed Port

A routed port is a physical port, for example, a port on the layer 3 device. It can be configured by using a layer 3 routing protocol. On the layer 3 device, a single physical port can be set as a routed port that serves as the gateway interface for layer 3 switching. A routed port serves as an access port that is not related to a specific VLAN. A routed port provides no L2 switching function. You may change an L2 switch port into a routed port by using the **no switchport** command and then assign an IP address to it for routing purposes. Note that using the **no switchport** command in the interface configuration mode will close and restart this port and delete all the layer 2 features of this port.

Caution

However, when a port is a member port of an L2 aggregate port or an unauthenticated DOT1x authentication port, the **switchport /no switchport** command will not work.

1.1.2.3 L3 Aggregate Port

Just like a L2 aggregate port, a L3 aggregate port is a logically aggregated port group that consists of multiple physical ports. The aggregated ports must be layer 3 ports of the same type. For layer 3 switching, an AP that serves as the gateway interface for layer 3 switching considers multiple physical links in the same aggregate group as one logical link. This is an important method for expanding link bandwidth. In addition, the frames that pass through the L3 aggregate port will undergo traffic balancing on the member ports of the L3 aggregate port. If one member link of AP fails, the L3 aggregate port automatically assigns the traffic on this link to other working member links, making the connection more reliable.

An L3 aggregate port offers no L2 switching functions. You may establish routes by first changing an L2 aggregate port without members into an L3 aggregate port using the **no switchport** command and then adding multiple routed ports and assigning an IP address to it.

1.2 Configuring Interfaces

This section provides the default setting, guidelines, steps, and examples of configuration.

1.2.1 Interface Numbering Rule

The number of a switch port consists of a slot number and the port number on the slot. For example, the port number is 3 and the slot number is 2, the number of the corresponding interface is 2/3. The slot number ranges from 0 to the total

number of slots. The rule of numbering slots is that for panels facing the device, slots are numbered from front to back, from left to right, and from top down starting from 1 and increased in turn. Ports in a slot are numbered from left to right starting from 1 to the number of ports in the slot. For the devices which have a choice of optical or electrical interfaces, in either case, they use the same port number. You can view information on a slot and ports on it by using the **show** command in CLI.

Aggregate ports are numbered from 1 to the number of aggregate ports supported on the device.

A SVI is numbered by the VID of its corresponding VLAN.

Caution

The number of the static slot on a device is always 0. However, dynamic slots (pluggable modules or line cards) are numbered starting from 1.

1.2.2 Using Interface Configuration Commands

Execute the **interface** command to enter interface configuration mode in the global configuration mode.

Command	Function
DES-7200(config)# **interface** *interface ID*	Input **interface** to enter the interface configuration mode in the global configuration mode. You can also configure an interface range by using the **interface range** or **interface range macro** command. However, the interfaces in the same range must be of the same type and features.

This example shows how to access Gigabitethernet2/1:

```
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)#
```

You can configure the related attributes of the interface in the interface configuration mode.

1.2.3 Using the interface range Command

1.2.3.1 Setting an Interface Range

You can configure multiple interfaces at once by using the **interface range** command in the global configuration mode. As a result, the configured parameters apply to all the interfaces within the range.

Command	Function
DES-7200(config)# **interface range** {*port-range* | **macro** *macro_name*}	Enter an interface range. You can use the **interface range** command to specify multiple ranges separated by a comma. The **macro** parameter can use the macro of a range. See the section of *Configuring and Using Macro Definition for Interface Range*. Be sure that the interfaces of all the ranges specified by a command must be of the same type.

When using the **interface range** command, you should pay attention to the format of **range**.

A valid range format

vlan *vlan-ID* - *vlan-ID*, with VLAN ID in the range of 1–4094;

Fastethernet *slot*/{*the first port*} - { the last *port*};

Gigabitethernet *slot*/{*the first port*} - { the last *port*};

TenGigabitethernet *slot*/{*the first port*} - { the last *port*};

Aggregate Port Aggregate *port number*, with *Aggregate port number* in the range of 1 to MAX.

The interfaces in an **interface range** must be of the same type, for example fastethernet, gigabitethernet, aggregate port or SVI.

This example shows how to use the **interface range** command in the global configuration mode:

```
DES-7200# configure terminal
DES-7200(config)# interface range fastethernet 1/1 - 10
DES-7200(config-if-range)# no shutdown
DES-7200(config-if-range)#
```

This example shows how to separate multiple ranges by a comma “,”:

```
DES-7200# configure terminal
DES-7200(config)# interface range fastethernet 1/1-5, 1/7-8
DES-7200(config-if-range)# no shutdown
DES-7200(config-if-range)#
```

1.2.3.2 Configuring and Using Macro Definition for Interface Range

You can define a macro instead of inputting port ranges. However, you have to define macros using the **define interface-range** command in the global configuration mode before using the **macro** keyword of the **interface range** command.

Command	Function
DES-7200(config)**# define interface-range** *macro_name interface-range*	Define a macro for interface range. Name of the macro, up to 32 characters. A macro can define multiple interface ranges. The interfaces in all ranges in the same macro must be of the same type.
DES-7200(config)**# interface range macro** *macro_name*	The string defined by the macro will be saved in the memory. When you use the **interface range** command, you can use the macro name to replace the interface-range string.

To delete a macro, use the **no define interface-range macro_name** command in the global configuration mode.

When defining an interface range using the **define interface-range** command, you should pay attention to the range format.

A valid range format is:

– **vlan** *vlan-ID - vlan-ID*, with VLAN ID in the range of 1 to 4094;

– **fastethernet** *slot*/{*the first port*} - { the last *port*};

– **gigabitethernet** *slot*/{*the first port*} - { the last *port*};

– **Aggregate Port Aggregate** *port number*, with *Aggregate port number* in the range of 1 to MAX.

Interfaces contained in an i**nterface range** must be of the same type, that is, they should be all switch ports, aggregate ports or SVIs.

This example defines a macro for fastethernet1/1-4 by using the **define interface-range** command:

```
DES-7200# configure terminal
```

```
DES-7200(config)# define interface-range resource
fastethernet 1/1-4
DES-7200(config)# end
```

This example defines a macro for multiple ranges:

```
DES-7200# configure terminal
DES-7200(config)# define interface-range ports1to2N5to7
fastethernet 1/1-2, 1/5-7
DES-7200(config)# end
```

This example uses the macro ports1to2N5to7 to set the specified range of interfaces:

```
DES-7200# configure terminal
DES-7200(config)# interface range macro ports1to2N5to7
DES-7200(config-if-range)#
```

This example deletes the macro ports1to2N5to7:

```
DES-7200# configure terminal
DES-7200(config)# no define interface-range ports1to2N5to7
DES-7200# end
```

1.2.4 Selecting Interface Media Type

Some interfaces come with multiple media types for your choice.Once you have selected a media, interface attributes like connection status, speed, duplex, and flow control will be determined. When you change the media, interface attributes will use their default values. Change the default values when necessary.

The interfaces with multiple media types support the interface media auto-select. If the interface media auto-select has been configured, and only one media is connected to the interface, the device will use the media connected currently; if the two media types are connected to the interface, the device will use the media configured first. The auto-select prefere media is electrical interface by default, use the command **medium-type auto-select prefer fiber** to set the prefer media as optical interface. In the auto-select mode, the interface attributes like speed, duplex, and flow control will use the default values.

This configuration takes effect for only physical ports. Aggregate port and SVI port do not support setting media types.

This configuration command takes effect for only the ports that supports media selection.

The ports configured to be the members of an aggregate port must have the same media type. Otherwise, they cannot be added to the AP. The port type of

the members of the aggregate port cannot be changed. The ports configured to be the media auto-select cannot be added to the AP.

Command	Function
DES-7200(config-if)# **medium-type** { **fiber** | **copper** }	Set the media type of a port.

This example sets the media type of gigabitethernet 1/1:

```
DES-7200# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# medium-type fiber
DES-7200(config-if)# end
```

1.2.5 Setting Interface Description and Management Status

You may give an interface a particular name (description) to help you remember its functions. You may name the interface what you want to do with it, for example, if you want to reserve Gigabitethernet 1/1 for the exclusive use of user A, you may set its description to “Port for User A”.

Command	Function
DES-7200(config-if)# **description** *string*	Set the interface description in no more than 32 characters.

This example sets the description of Gigabitethernet 1/1:

```
DES-7200# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# description PortForUser A
DES-7200(config-if)# end
```

In some circumstances, you may need to disable some interface. You can do this by setting the management status of the interface. Once disabled, no frames can be received and sent through the interface, and all its functions are disabled. You can also restart an disabled interface by setting its management status. The management status of an interface can be **up** or **down**. When a port is disabled, its management status is **down**; otherwise, it is in the status **up**.

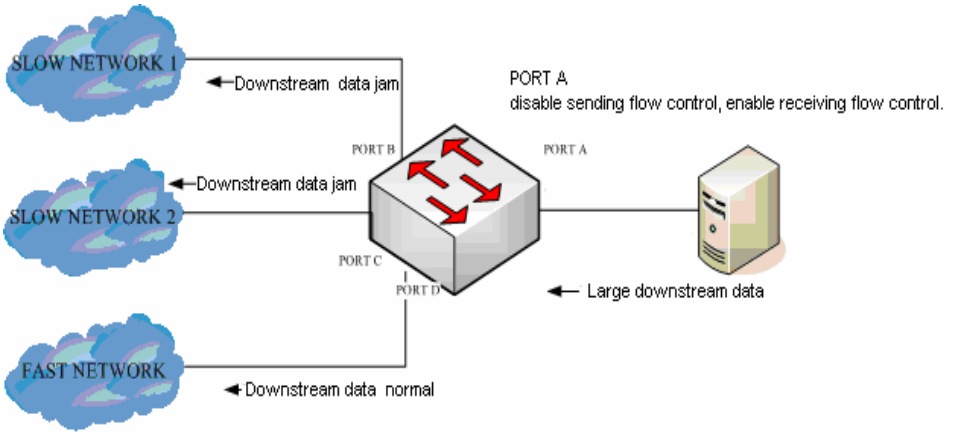
Command	Function
DES-7200(config-if)# **shutdown**	Disable an interface.

The following example illustrates how to disable Gigabitethernet 1/2.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/2
DES-7200(config-if)# shutdown
DES-7200(config-if)# end
```

1.2.6 Setting Speed, Duplexing, and Flow Control for an Interface

The section deals with the setting of speed, duplexing, and flow control for interfaces. The flow control falls into the non-symmetric and symmetric flow control modes. Generally, after enabling the flow control on the interface, the flow control frames received on the interface will be handled, and be sent when the interface jam occurs. The symmetric flow control mode refers to the same handling for the receiving and sending the flow control frames. However, in some conditions, on one hand, the device expects handling the received flow control frame on the interface to avoid the packets being discarded due to the jam; on the other hand, the sending the flow control frame will make the speed of overall network decreased. In this case, the non-symmetric flow control shall be configured to separate the handling pacings of receiving and sending the flow control frames. As shown in Figure 2: the port A is the uplink port, and the ports B-D are the downlink ports, wherin the ports B, C correspond to the slow network. Suppose that the receiving and sending flow control functions are enabled on the port A, the over-large dataflow on the sending port B makes the the ports B,C jammed due to the slow network connected, which leads to the ingress jam on the port A, and the flow control frame sent on the port A, if the uplink device reponds to this frame,the dateflow sending to the port A will be decreased and network speed on the port D is slowed down indirectly. Then you can disable the sending flow control on the port A to ensure the bandwidth utilization rate in overall network.



The following command takes effect only for switch port and routed port.

Command	Function
DES-7200(config-if)# **speed** {**10** | **100** | **1000** | **auto** }	Select a speed or set it to **auto**. Caution: 1000M applies only to gigabit interfaces.
DES-7200(config-if)# **duplex** {**auto** | **full** | **half** }	Set duplex mode. Note that the optical interface for the devices support the half-duplex.
DES-7200(config-if)# **flowcontrol** {**auto** | **on** | **off** }	Set flow control mode. Note: When **speed**, **duplex**, and **flowcontrol** are all set to non-auto, the system will disable auto-negotiation on the interface.
DES-7200(config-if)# **flowcontrol** {**receive** | **send**} {**auto | on | off**}	Support the setting of non-symmetric flow control mode on the device. Note: if the settings of the receive and send modes are the same, the corresponding **flowcontrol** command is displayed consistent with it.

In the interface configuration mode, you can restore the settings of speed, duplexing, and flow control to the default values (auto-negotiation) by using the **no speed**, **no duplex**, and **no flowcontrol** commands. The following example shows how to set the speed of Gigabitethernet 1/1 to 1000M, its duplex mode to **full**, and its flow control to **off**.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# speed 1000
DES-7200(config-if)# duplex full
DES-7200(config-if)# flowcontrol off
DES-7200(config-if)# end
```

Caution According to the related IEEE standards, the Master or Slave status of the 1000M copper port must be confirmed by negotiation.

1.2.7 Configuring Interface MTU

When a heavy throughput of data interchange occurs on a port, there may be a frame beyond the Ethernet standard frame length. This type of frame is called jumbo frame. A user can control the maximum frame length that the port is allowed to receive and send by setting the MTU.

MTU refers to the length of a valid data segment in a frame, excluding the overhead of Ethernet encapsulation.

The MTU of a port is checked during input, not output. If the frame received by the port is longer than the set MTU, it will be discarded.

The MTU is in the range from 64 to 9216 bytes with the granularity of 4 bytes. Its default value is 1500 bytes.

This configuration command takes effect only for physical ports. The SVI interface currently does not support the MTU setting.

Command	Function
DES-7200(config-if)# **Mtu** *num*	Set the MTU for a port. *num*: <64 to 9216>

This example shows how to set the MTU for Gigabitethernet 1/1:

```
DES-7200# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mtu 64
DES-7200(config-if)# end
```

1.2.8 Configuring L2 Interfaces

The following table shows the default settings of L2 interfaces. For the configurations of VLAN and ports, please refer to *Configuring VLAN* and *Configuring Port-based Flow Control*.

Attribute	Default Configuration
Working mode	L2 switch mode
Switch port mode	access port
Allowed VLAN range	1 to 4094
Default VLAN (for access port)	VLAN 1
Native VLAN (for trunk port)	VLAN 1
Media Type	copper

Attribute	Default Configuration
Interface management status	Up
Interface Description	Null
Speed	Auto-negotiation
Duplex mode	Auto-negotiation
Flow control	Auto-negotiation
Aggregate port	None
Storm suppression	Off
Port protection	Off
Port Security	Off

1.2.8.1 Configuring Switch Ports

1.2.8.1.1 Configuring Access/Trunk Port

This section is devoted to the setting of working modes (access/trunk port) of switch port and the setting in each mode.

To set the related attributes of a switch port, use the **switchport** command or other commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **switchport mode** {**access** | **trunk** }	Set the operation mode.

The following example shows how to set the operation mode of Gigabitethernet 1/2 to access port.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/2
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# end
```

Command	Function
DES-7200(config-if)# **switchport access vlan** *vlan-id*	Set the VLAN to which the access port belongs.

The following example shows how to configure the VLAN to which the access port gigabitethernet 2/1 to be 100

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# switchport access vlan 100
DES-7200(config-if)# end
```

Set the native VLAN of the trunk port.

Command	Function
DES-7200(config-if)**# switchport trunk native vlan** *vlan-id*	Set the Native VLAN of the trunk port.

The following example shows how to set the native VLAN of the trunk port Gigabitethernet 2/1 to be 10.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# switchport trunk native vlan 10
DES-7200(config-if)# end
```

Set port security. For more information about port security, refer to *Port-based Flow Control*:

Command	Function
DES-7200(config-if)**# switchport port-security**	Set port security.

The following example shows how to enable port security on Gigabitethernet 2/1.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# end
```

For more information on configuring the speed, duplexing, and flow control of an interface, see the section of *Setting Speed, Duplexing, and Flow Control foran Interface.*

The following example shows how to set Gigabitethernet 2/1 to access port, its VLAN to 100, its speed, duplexing, and flow control to self-negotiation and enable port security.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200 (config)# interface gigabitethernet 2/1
DES-7200 (config-if)# switchport access vlan 100
DES-7200 (config-if)# speed auto
DES-7200 (config-if)# duplex auto
DES-7200 (config-if)# flowcontrol auto
DES-7200 (config-if)# switchport port-security
DES-7200 (config-if)# end
```

1.2.8.1.2 Configuring Hybrid Port

You can configure the hybrid port by performing the following steps:

Command	Description

Command	Description
configure terminal	Enter configuration mode
interface <*interface***>**	Enter the interface configuration mode. Megabit, Gigabit, 10 Gigabit
switchport mode hybrid	Configure the port as a hybrid port.
no switchport mode	Delete the port mode.
switchport hybrid native *vlan* **id**	Set the default VLAN for the hybrid port.
switchport hybrid allowed vlan [[**add**] [**tagged | untaged**]] **|remove**] *vlist*	Set the output rule for the port.

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/1
DES-7200(config-if)# switchport mode hybrid
DES-7200(config-if)# switchport hybrid native vlan 3
DES-7200(config-if)# switchport hybrid allowed vlan untagged 20-30
DES-7200(config-if)# end
DES-7200# show running interface g 0/1
```

1.2.8.2 Configuring L2 Aggregate Ports

This section describes how to create an L2 aggregate port and some related settings.

You may create an L2 aggregate port by using the **aggregateport** command in the interface configuration mode. For details, see *Configuring Aggregate Port.*

1.2.8.3 Clearing Statistics and Resetting an Interface

In the privileged EXEC mode, you may clear the statistics of an interface and then reset it by using the **clear** command. This command is only applicable for switch port, port members of an L2 aggregate port, routed port, and port members of an L3 aggregate port. The **clear** command is shown as follows.

Command	Function
DES-7200# **clear counters** [*interface-id*]	Clear interface statistics.
DES-7200# **clear interface** *interface-id*	Reset the interface.

In the privileged EXEC mode, use the **show interfaces** command to display interface statistics, or use the **clear counters** command to clear the counters. If no interface is specified, the counters of all layer 2 interfaces will be cleared.

The following example shows how to clear the counter of gigabitethernet 1/1.

```
DES-7200# clear counters gigabitethernet 1/1
```

1.2.9 Configuring L3 Interfaces

To configure a layer 3 interface, execute the following steps:

Command	Function
DES-7200(config-if)# **no switchport**	Shut down the interface and change it to L3 mode. This command applies to switch port and L2 aggregate port only.
DES-7200(config-if)# **ip address** *ip_address* *subnet_mask* {[**secondary** | **tertiary** | **quartus**][**broadcast**]}	Configure the IP address and subnet mask of the interface.

To delete the IP address of an L3 interface, use the **no ip address** command in the interface configuration mode.

The **no switchport** operation cannot be performed on one member of an L2 aggregate port.

The following example shows how to set an L2 interface to a routed port and assign an IP address to it.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.20.135.21 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
```

1.2.9.1 Configuring SVI

This section describes how to create a SVI and some related configuration.

You may create a SVI or modify an existing one by using the **interface vlan** *vlan-id* command.

To configure a SVI, execute the following command:

Command	Function
DES-7200(config)# **interface vlan** *vlan-id*	Enter the SVI interface configuration mode.

Then, you can configure the attributes related to the SVI. For detailed information, refer to *Configuring Single IP Address Route*.

The following example shows how to enter the interface configuration mode and assign an IP address to SVI 100.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface vlan 100
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# end
```

1.2.9.2 Configuring Routed Ports

This section deals with how to create and configure a routed port.

You may create a routed port by using the **no switchport** command in the interface configuration command.

To create one routed port and assign an IP address to it, execute the following commands:

Command	Function
DES-7200(config-if)**# no switchport**	Shut down the interface and then change it to L3 mode.
DES-7200(config-if)**# ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

Caution No layer switching can be performed by using **switchport/ no switchport** when an interface is a member of an L2 Aggregate Port.

The following example shows how to set an L2 interface to a routed port and then assign an IP address to it.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface fastethernet 1/6
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
```

1.2.9.3 Configuring L3 Aggregate Ports

This section deals with how to create an L3 aggregate port and some related configuration.

In the interface configuratiion mode, you can use the **no switchport** command to convert a L2 aggregate port to a L3 aggregate port:

Command	Function
DES-7200(config-if)# **no switchport**	Shut down the interface and change it to L3 mode.
DES-7200(config-if)# **ip address** *ip_address subnet_mask*	Configure the IP address and subnet mask.

The following example shows how to create an L3 aggregate port and assign an IP address to it.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface aggregateport 2
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
```

1.3 Showing Interface Configuration and Status

This section covers interface status display and gives examples. You may view interface status by using the **show** command in the privileged EXEC mode. To show interface status, use the following commands.

Command	Function
DES-7200# **show interfaces** [*interface-id*]	Show the status and configuration of the specified interface.
DES-7200# **show interfaces** *interface-id* **status**	Show the status of the specified interface.
DES-7200# **show interfaces** [*interface-id*] **switchport**	Show the administrative and operational status of an switch interface (non-routing interface).
DES-7200# **show interfaces** [*interface-id*] **description**	Show the description and status of the specified interface.
DES-7200# **show interfaces** [*interface-id*] **counters**	Show the statistics of the specified port. Where, the rate displayed may have an error of less than 0.5%.

The following example shows how to display the status of Gigabitethernet 0/1.

```
SwitchA#show interfaces gigabitEthernet 0/1
```

```
Index(dec):1 (hex):1
GigabitEthernet 0/1 is DOWN  , line protocol is DOWN
Hardware is Broadcom 5464 GigabitEthernet
Interface address is: no ip address
  MTU 1500 bytes, BW 1000000 Kbit
  Encapsulation protocol is Bridge, loopback not set
  Keepalive interval is 10 sec , set
  Carrier delay is 2 sec
  RXload is 1 ,Txload is 1
  Queueing strategy: FIFO
    Output queue 0/0, 0 drops;
    Input queue 0/75, 0 drops
  Switchport attributes:
    interface's description:""
    medium-type is copper
    lastchange time:0 Day: 0 Hour: 0 Minute:13 Second
    Priority is 0
    admin duplex mode is AUTO, oper duplex is Unknown
    admin speed is AUTO, oper speed is Unknown
    flow receive control admin status is OFF,flow send control admin status
is OFF,flow receive control oper status is Unknown,flow send control oper
status is Unknown
broadcast Storm Control is OFF,multicast Storm Control is OFF,unicast Storm
Control is OFF
 Port-type: trunk
   Native vlan:1
Allowed vlan lists:1-4094
Active vlan lists:1, 3-4
  5 minutes input rate 0 bits/sec, 0 packets/sec
  5 minutes output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer, 0 dropped
    Received 0 broadcasts, 0 runts, 0 giants
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 abort
    0 packets output, 0 bytes, 0 underruns , 0 dropped
0 output errors, 0 collisions, 0 interface resets
```

The following example shows the status of aggregate port 3.

```
DES-7200# show interfaces aggregateport 3:

Interface                   : AggreatePort 3
Description                 :
AdminStatus                 : up
OperStatus                  : down
Hardware                    : -
Mtu                         : 1500
LastChange                  : 0d:0h:0m:0s
AdminDuplex                 : Auto
OperDuplex                  : Unknown
AdminSpeed                  : Auto
OperSpeed                   : Unknown
FlowControlAdminStatus      : Autonego
FlowControlOperStatus       : Disabled
```

```
Priority                    : 0
```

This example shows the configuration of GigabitEthernet 1/1:

```
DES-7200# show interfaces gigabitEthernet 1/1 switchport
Interface  Switchport Mode     Access    Native    Protected VLAN lists
---------- ---------- --------- --------- --------- --------- ------------
gigabitethernet 1/1     Enabled  Access     1        1        Enabled   All
```

This example shows the description of Gigabitethernet 2/1:

```
DES-7200# show interfaces gigabitethernet 1/2 description
Interface               Status    Administrative    Description
--------------------  ---------  ---------------    ----------------
gigabitethernet 2/1     down        down            Gi 2/1
```

This example shows statistics of the interfaces.

```
DES-7200# show interfaces gigabitethernet 1/2 counters
Interface : gigabitethernet 1/2
5 minute input rate          : 9144 bits/sec, 9 packets/sec
5 minute output rate         : 1280 bits/sec, 1 packets/sec
InOctets                     : 17310045
InUcastPkts                  : 37488
InMulticastPkts              : 28139
InBroadcastPkts              : 32472
OutOctets                    : 1282535
OutUcastPkts                 : 17284
OutMulticastPkts             : 249
OutBroadcastPkts             : 336
Undersize packets            : 0
Oversize packets             : 0
collisions                   : 0
Fragments                    : 0
Jabbers                      : 0
CRC alignment errors         : 0
AlignmentErrors              : 0
FCSErrors                    : 0
dropped packet events (due to lack of resources): 0
packets received of length (in octets):
  64:46264, 65-127: 47427, 128-255: 3478,
  256-511: 658, 512-1023: 18016, 1024-1518: 125
```

1.4 Showing the Optical Module Information

Use the following commands to show the optical module information in the privileged EXEC mode:

Command	Function

DES-7200# **show interfaces** [*interface-id*] **transceiver**	Show the basic information for the optical module on the specified interface.
DES-7200# **show interfaces** [*interface-id*] **transceiver alarm**	Show the current alarm information for the optical module on the specified interface. If there is no alarm information, it shows "none".
DES-7200# **show interfaces** [*interface-id*] **transceiver diagnosis**	Show the optical module transceiver diagnosis parameter on the specified interface.

The following example shows the optical module information on the interface GigabitEthernet 5/4:

```
DES-7200#show interfaces gigabitEthernet 5/4 transceiver
Transceiver Type : 1000BASE_SX_SFP
Connector Type : LC
Wavelength(nm) : 1310
Transfer Distance:
       SMF fiber
       -- 10km
       EBW 50/125 um fiber
       -- 300m
       50/125 um fiber
       -- 100m
       62.5/125 um fiber
       -- 33m
Digital Diagnostic Monitoring : YES
```

The following example shows the alarm information for the optical module on the interface GigabitEthernet 5/4:

```
DES-7200#show interfaces gigabitEthernet 5/4 transceiver alarm
gigabitEthernet 5/4 transceiver current alarm information:
RX  loss of signal
```

The following table shows the alarm information for the SFP optical module:

Field	Description
SFP	
RX loss of signal	Loss of the receiving signal.
RX power high	Alarm of the high receiving power of the optical module.

RX power low	Alarm of the low receiving power of the optical module.
TX fault	Sending fault.
TX bias high	Alarm of the bias high current.
TX bias low	Alarm of the bias low current.
TX power high	Alarm of the high sending power of the optical module.
TX power low	Alarm of the low sending power of the optical module.
Temp high	Alarm of the high temperature.
Temp low	Alarm of the low temperature.
Voltage high	Alarm of the high voltage.
Voltage low	Alarm of the low voltage.
Transceiver info checksum error	Transceiver information checksum error.
Transceiver info I/O error	Transceiver information read&write error
XFP	
RX loss of signal	Loss of the receiving signal.
RX not ready	The receiving state is not ready.
RX CDR loss of lock	RX CDR loss of lock.
RX power high	Alarm of the high receiving power of the optical module.
RX power low	Alarm of the low receiving power of the optical module.
TX fault	Sending fault.
TX CDR loss of lock	TX CDR loss of lock.
TX bias high	Alarm of the bias high current.
TX bias low	Alarm of the bias low current.
TX power high	Alarm of the high sending power of the optical module.
TX power low	Alarm of the low sending power of the optical module.
Module not ready	The module is not ready.
Temp high	Alarm of the high temperature.

Temp low	Alarm of the low temperature.
Voltage high	Alarm of the high voltage.
Voltage low	Alarm of the low voltage.
Transceiver info checksum error	Transceiver information checksum error.
Transceiver info I/O error	Transceiver information read&write error

The following example shows the optical module transceiver diagnosis parameter on the interface GigabitEthernet 5/4:

```
DES-7200#show interfaces gigabitEthernet 5/4 transceiver diagnosis
Current diagnostic parameters:
Temp(°C)    Voltage(V)        Bias(mA) RX power(dBM)     TX power(dBM)
36(OK)      3.31(OK)      6.13(OK) -35.64(warning)   -5.19(alarm)
```

The following table shows the optical module transceiver diagnosis parameter:

Field	Description
diagnostic information	The diagnostic information for the optical module on the interface.
Current diagnostic parameters	Current diagnostic parameters
Temp.(°C)	The diagnostic parameter—temperature, in °C.
Voltage(V)	The diagnostic parameter—voltage, in V.
Bias(mA)	The diagnostic parameter—bias current, in mA.
RX power(dBM)	The diagnostic parameter—RX power, in dBM.
TX power(dBM)	The diagnostic parameter—TX power, in dBM.
OK	The current state is normal.
warning	The current state is warning.
alarm	The current state is alarm.

Caution

The alarm and diagnostic parameter can be shown for the optical module supporting the Digital Diagnostic Monitoring function.

1.5 Line Detection

The administrator can use command **line-detect** to detect the work status of lines. Line detection can help the administrator judge the work status of lines correctly when the lines are in abnormal status.

In the interface configuration mode, execute command **line-detect**:

Command	Function
DES-7200(config)**#interface** *interface*	Enter the Interface configuration mode.
DES-7200(config-if)**# line-detect**	Detect lines.

Caution

Only L2 exchange ports can support line detection. Optical and AP port can not support line detection.

The following gives an example to execute the command to detect line:

```
DES-7200(config)#inteface gigabitEthernet 0/1
DES-7200(config-if-gigabitEthernet 0/1)#line-detect
start cable-diagnoses,please wait...
cable-daignoses end!this is result:
4 pairs
pair state     length(meters)
---- ---------- --------------
A    Ok         2
B    Ok         1
C    Short      1
D    Short      1
```

Command description:

Command	Description
pairs	The number of the line pairs. For example, the twisted pair is composed of four line pairs.
State	1.OK; 2.Short; 3.Open. In normal state, two pairs(A,B) of 100M twisted pair are OK, while other two pairs(C,D) are Short. Four pairs

	(A,B,C,D) of 1000M twisted pair are OK.
Length	The line length, in meter, takes effect only for the pairs in Ok state. In addition, some inaccuracy is possible because the line length is calculated according to the signal transferring time. The length of lines in Short or Open states refers to the length from the port to the defective line point.

1.6 LinkTrap Policy Configuration

You can determine whether to send the LinkTrap of an interface according to the interface configuration on a device. With this funciton enabled, when the interface's link status changes, the SNMP protocol will send a LinkTrap message. Otherwise, it will not send a LinkTrap message. By default, this funciton is enabled.

1.6.1 Configuration Command

Command	Function
DES-7200(config-if)**# [no] snmp trap link-status**	Enable or disable the function of sending the LinkTrap function of this interface.

1.6.2 Configuration Example

The following configuration shows how to configure the interface not to send LinkTrap:

```
DES-7200(config)# interface gigabitEthernet 1/1
DES-7200(config-if)# no snmp trap link-status
```

2 MAC Address Configuration

Using the information in the MAC address table, the Ethernet switch rapidly searches for the address to which the messages in the data link layer are forwarded. This chapter describes the MAC address configuration, including the following sections:

- Understanding the MAC Address Table
- Default Configuration
- Configuring the Dynamic Address
- Configuring the Dynamic Address Aging Time
- Configuring the Management Learning mode of Dynamic Address
- Configuring the Limit of Dynamic Addresses for a VLAN
- Configuring the Static Address
- Configuring the Filtering Address
- Configuring the MAC Addres Change Notification Function
- Configuring IP address and MAC address binding
- Configuration Examples

2.1 Understanding the MAC Address Table

2.1.1 Overview

Layer-2 forwarding, a major function of the Ethernet Switch, is to forward the messages by identifying the data link layer information. The switch forwards the messages to the corresponding interface through the destination MAC addresses carried by the messages, and stores the information about the relationship between the destination MAC address and the interface in the MAC address table.

All the MAC addresses in the MAC address table are associated with the VLAN. Different MAC addresses are allowed to be in the same VLAN. Each VLAN maintains a MAC address table logically. It is possible that a MAC address learned by a VLAN is unknown to other VLANs and shall be learned again.

The MAC address contains the following information:

State	VLAN	MAC address	Interface

Figure-1 MAC Address Entry

- State: Dynamic,static or filtering address.
- VLAN: VLAN to which the MAC address belongs;
- MAC address: the MAC address information in the entry;
- Interface: the information of the interface with which the MAC address is correspondent.

The MAC address entries are updated and maintained by the following two ways:

- Learning the Dynamic Address
- Configuring the Dynamic Address Manually

The switch searches for the corresponding outgoing forward interface according to the destination MAC address and the VLAN ID for the message in the MAC address table, and then forwards the messages in unicast, multicast and broadcast way.

- Unicast forwarding: if the switch searches for the corresponding entry of the packet destination MAC address and VLAN ID in the MAC address table and the outgoing forward interface is sole, the packets are forwarded through this interface.
- Multicast forwarding: if the switch searches for the corresponding entry of the packet destination MAC address and VLAN ID in the MAC address table and this entry is correspondent with a group of outgoing forward interfaces, the packets are forwarded through the interfaces directly.
- Broadcast forwarding: if the switch receives the packets destined to ffff.ffff.ffff, or it can not search for the corresponding entry in the MAC address table, the packets are sent to the VLAN to which belongs and forwarded through the outgoing interfaces except for the incoming interface.

Note

This chapter describes management of dynamic, static and filtering addresses. For the management of multicast address, please refer to *IGMP Snooping Configurations*.

2.1.2 Learning the Dynamic Address

2.1.2.1 Dynamic Address

A dynamic address is the MAC address learnt automatically from the packets received by the switch. Only the dynamic address be removed by the aging mechanism of the address table.

2.1.2.2 Address Learning Process

In general, it maintains the MAC address table by learning the dynamic address. The operation principle is:

The MAC address table in the switch is null and User A shall communicate with User B. User A sends the packet to interface GigabitEthernet 0/2 and the MAC address for User A is learnt in the MAC address table.

There is no source MAC address for User B in MAC address table. Therefore, the switch sends the packets to all ports except for the ports of User A in broadcast form. User C can receive the packets sent from User A and don't belong to User A.

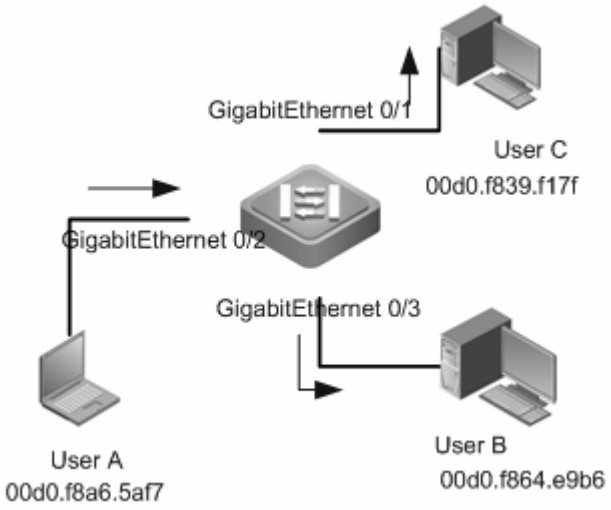


Figure2 Dynamic Address Learn (Step 1)

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2

Figure3 MAC Address Table1

Upon receiving the packets, UserB will send them to UserA through interface GigabitEthernet 0/3. The MAC address for UserA exits in the MAC address

table. Therefore, the packets are forwarded to interface GigabitEthernet 0/2 in the unicast form and the switch learns the MAC address for UserB at the same time. The difference from the step one is that UserC can not receive the packets sent from UserB to UserA.

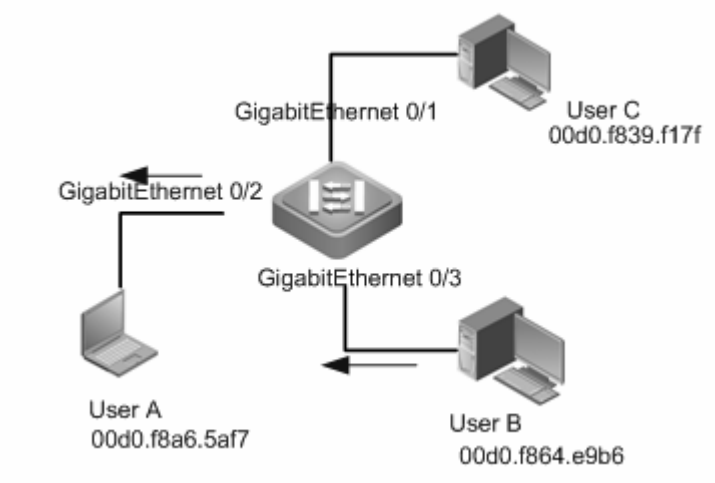


Figure4 Dynamic Address Learn (Step 2)

Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 0/2
Dynamic	1	00d0.f8a4.e9b6	GigabitEthernet 0/3

Figure5 MAC Address Table 2

After the communication between UserA and UserB, the switch learns the source MAC addresses for UserA and UserB. The mutual packets between UserA and UserB are forwarded in the unicast form and UserC can not receive them again.

Caution	In the stack system, the address tables of each member device are asynchronous. For example: Suppose the device A and device B stack and the device A is the host, send the broadcast packets to the device A, the port receiving the frames on the device A will learn the MAC1 address, which will be recorded in the address table. Since the packets are broadcasted to the device B through the stack port, the stack port on the device B will also learn this MAC1 address but not record it in the address table. Removing the MAC address learned from the frame-receiving port on the device A, the MAC1 address in the address table will also be removed. However, the stack port of the device B still learn this

	MAC address, the inconsistency of the hardware address table of the master and slave devices occurs. Send the packets destined to MAC1 address to other ports of the device A, those packets can not be broadcasted to the device B for the reason that the MAC1 address has already been learned by the stack port of the device B. After this MAC address ages out, the packets are broadcasted to the port of the device B.

2.1.2.3 Address Aging

The capacity of MAC address is restricted. The switch updates the MAC address list by learning new addresses and aging out unused addresses.

For an address in the MAC address table, if the switch has not received any packet from the MAC address for a long time (depending on the aging time), the address will be aged out and removed from the MAC address table.

2.1.3 Management Learning mode of the Dynamic Address

DES-7200 high-density modular Ethernet switches support the management learning mode of the dynamic address, including:

- Uniform MAC address learning mode
- Dispersive MAC address learning mode

2.1.3.1 Uniform MAC address learning mode

A. Operation Mechanism

In this mode, multiple line cards in the switch learn the MAC addresses, with each line card learning the MAC address independently. The MAC address learn process is described as follows:

The UserA under the Line Card1 sends the packets to the UserB. For the MAC address for the UserB does not exist on the switch, the packets will be sent to all line cards on the switch in broadcast form.

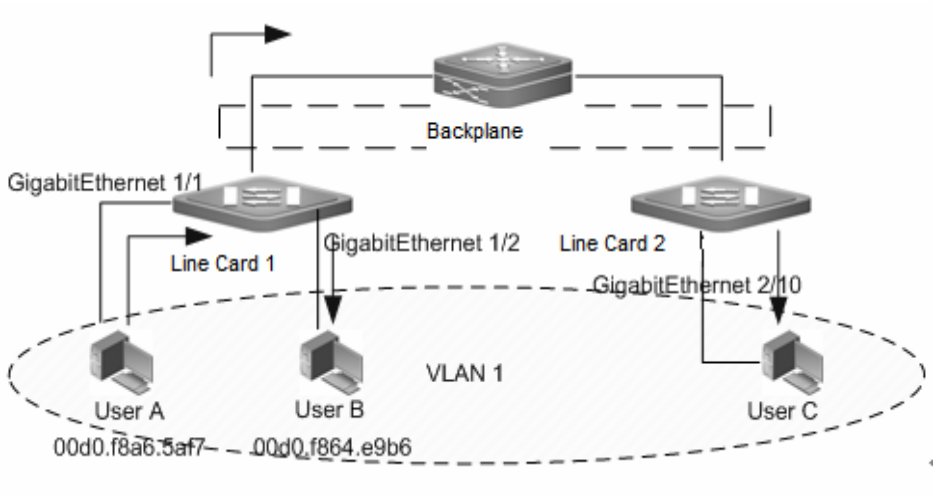


Figure-6 Uniform MAC Address Forward Process 1

The UserA under the Line Card1 sends the packets to the UserB. For the MAC address for the UserB does not exist on the switch, the packets will be sent to all line cards on the switch in broadcast form. The switch learns the address after receiving the packets from the UserA. At this time, Line Card 1 and Line Card 2 both receive the packets from the UserA, so they learn the MAC address for the UserA simultaneously.

MAC address table(Line card 1)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1

MAC address table(Line card 2)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1

Figure-7 Uniform MAC address Learning: MAC address table

After receiving the packets from the UserA, the UserB sends the reply packets to the Line Card1. Since the Line Card 1 has learned the MAC address for the UserA, the packets will be sent to the port of UserA in the unicast form and will not be sent to the Line Card 2.

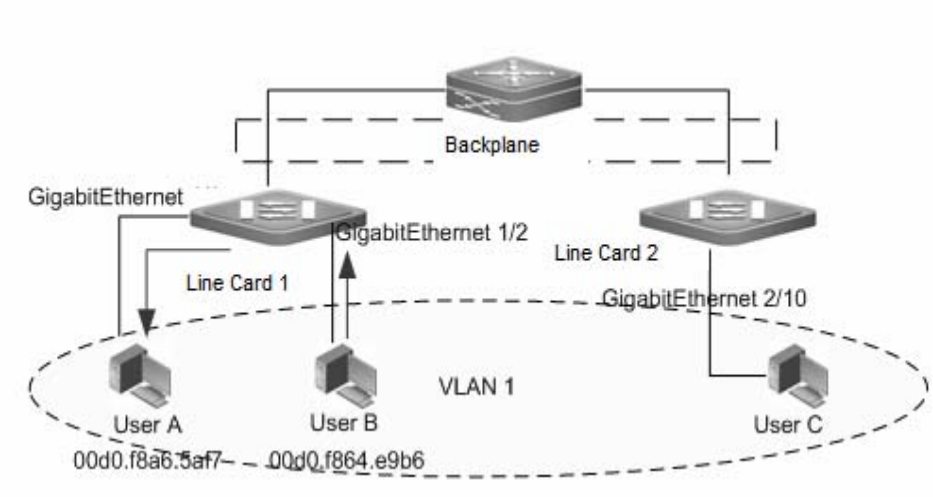


Figure-8 Uniform MAC Address Forward Process 2

For the reply packets sent by the UserB are forwarded to the port of UserA through the Line Card 1, the switch only learn the Mac addresses on the Line Card 1 and the MAC addres for UserB can not be learned on the Line Card 2.

MAC address table(Line card 1)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1
Dynamic	1	00d0.f864.c9b6	GigabitEthernet 1/2

MAC address table(Line card 2)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1

Figure-9 Uniform MAC address Learning: MAC address table 2

The advantages of the uniform MAC address learning:

- ✧ The capacity of the address table for all linecards in the switch is allocated on demand: If two users exchange the packets on the same line card, only the MAC address space of the line card 1 is occupied.
- ✧ High System Performance: Small system expenditure since the internal system adopts the dispersive MAC address learning mode.

The disadvantages of the uniform MAC address learning: since the address tables for all line cards in the switch are asynchronous, the packets are sent in the unicast form for Line Card 1 while in the broadcast form for Line Card 2.

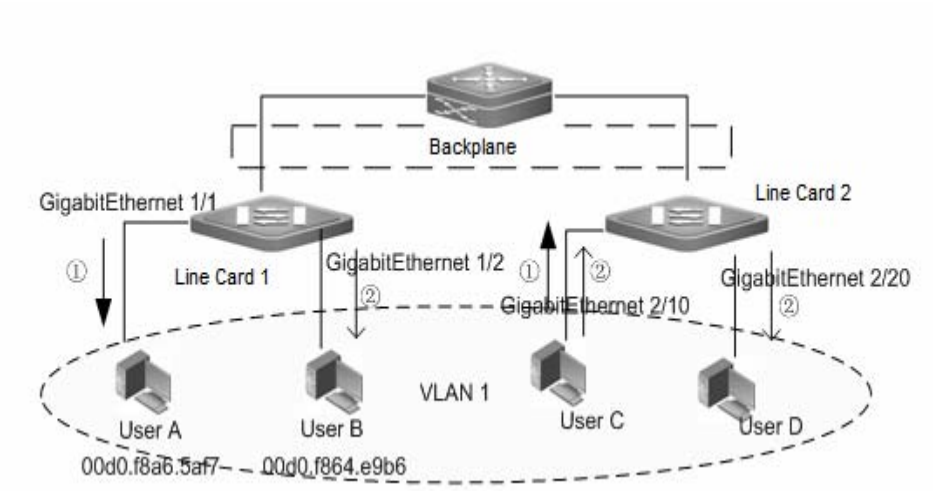


Figure-10 Uniform MAC address Learning: Unicast and Multicast Packets Forward

When the UserC under the Line Card 2 sends a packet to the UserA, since the Line Card 2 has learned the MAC address for the UserA, the packet will be forwarded to the UserA in the unicast form.

When the UserC under the Line Card 2 sends a packet to the UserB, since the Line Card 2 has learned the MAC address for the UserB, the packet will be forwarded in the broadcast form. At this time, the UserD that is in the same VLAN of UserC also receives the packet. The packet will be forwarded in the unicast form to the UserB after being sent to the Line Card 1.

B. MAC Address Synchronization

In the uniform MAC address learning mode, the Ethernet switch supports the MAC address synchronization function. All line cards in the switch no longer learn the MAC address in the dispersive MAC address learning mode and synchronize the new MAC address learned by any line card.

The advantages of the MAC address synchronization: the MAC addresses within the switch are synchronous. It helps prevent the packets in the network from being forwarded in the broadcast form if the number of users connecting to the switch exceeds the MAC address table limit.

The disadvantages of the MAC address synchronization:

- ✧ Occupy the large space of the MAC address table: Even though two users exchange the packets on the same line card, the MAC address space of other line cards will also be occupied.

✧ Decrease the System Performance: The system performance is decreased and it needs the extra synchronous expenditure because the line card adopts the non-dispersive MAC address learning mode.

Caution

With the dynamic MAC address synchronization enabled, every time the address learning or address aging occurs, the corresponding operation is executed by the switch. Frequent address learning or address aging in a short time consumes a lot of CPU resources, which results in the high utilization of CPU. The administrator shall enable this function prudently.

2.1.3.2 Dispersive MAC address learning mode

In the uniform mode, all line cards join the address learning in all VLANs. Even though a port in a specified VLAN is only distributed on one line card, other line cards still learns the address when receiving the packet from this specified VLAN.

In the dispersive mode, the line card is responsible for learning the address only in the VLAN where the port that is on this line card is in, not learning the address in other VLANs.

In the VLAN 1, all ports are on the line card 1. In the VLAN 2, all ports are on the line card 2. In the VLAN 3, all ports are on the line card 3.

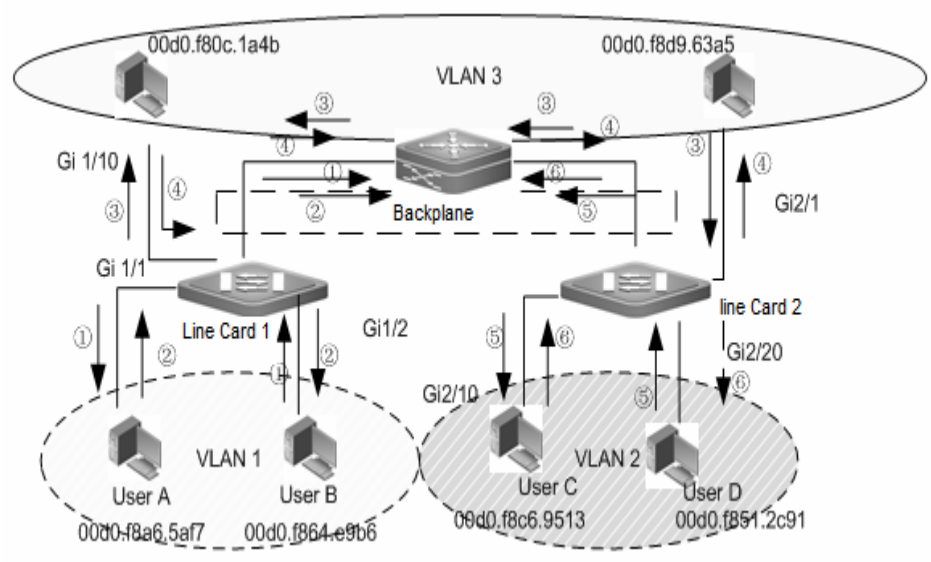


Figure-11 Separated MAC address Learning Forward

If the address tables of the line card 1 and line card 2 are null, the UserA and the UserB exchanges the packets in VLAN1, the UserC and the UserD exchanges the packets in VLAN2, the UserE and the UserF exchanges the packets in VLAN3. The following shows the MAC address table learned by the switch:

MAC address table(Line card 1)			
Status	VLAN	MAC address	Interface
Dynamic	1	00d0.f8a6.5af7	GigabitEthernet 1/1
Dynamic	1	00d0.f864.c9b6	GigabitEthernet 1/2
Dynamic	3	00d0.f8d9.63a5	GigabitEthernet 2/1
Dynamic	3	00d0.f80c.1a4b	GigabitEthernet 1/10

MAC address table(Line card 2)			
Status	VLAN	MAC address	Interface
Dynamic	2	00d0.f8c6.9513	GigabitEthernet 2/10
Dynamic	2	00d0.f851.2c91	GigabitEthernet 2/20
Dynamic	3	00d0.f8d9.63a5	GigabitEthernet 2/1
Dynamic	3	00d0.f80c.1a4b	GigabitEthernet 1/10

Figure-12 Separated MAC address Learning: MAC address table

In the dispersive mode, the line card learns the neccesary address information only. To this end, it maximizes the resources of the MAC address table in the system.

Caution

1. In the dispersive mode, theoretically, when the line cards in different models are mix-inserted, the total capacity of the address table equals to the sum of the capacity of the address table of all line cards. In the uniform mode, when the line cards in different models are mix-inserted, the minimum capacity of the address table of the line card determines the maximum total capacity of the address table.
2. In the dispersive mode, for 7200-4XG, to reach the limited capacity, the port 1 and 2, 3 and 4 on this line card can not be configured in the same VLAN. For 7200-4XG, to reach the limited capacity, the port 1 and 2, 3 and 4, 5 and 6, 7 and 8 on this line card can not be configured in the same VLAN.

2.1.4 Limit of Dynamic Addresses for a VLAN

The capacity of the MAC address table on the Ethernet switch is limited and shared by all VLANs. To prevent large amout of dynamic addresses in a VLAN from occupying the whole MAC address table and disabling other VLANs to learn the dynamic addresses which leads the packets in other VLANs to be forwarded in the broadcast way, the switch provides the limit of dynamic addresses for a VLAN. The user can specify the number of dynamic addresses learned in each VLAN and configure the upper limit of dynamic addresses for each VLAN.

For the VLAN with the limit of dynamic addresses configured, only the specified MAC addresses can be learned. The MAC addresses that exceeds the upper limit are not learned and the packets destined to those MAC addresses are forwarded in the broadcast form.

Caution

If the upper limit of the dynamic addresses for a VLAN is less than the number of the learned dynamic addresses in the current VLAN, the Ethernet switch no longer learns the address in the VLAN and learns again untill the the number of the addresses is less than the upper limit due to the address aging and deletion.

For DES-7200 series, only 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG, 7200-24GE and 7200-24G2XG line cards support this function.

2.1.5 Static Address

A static address is a manually configured MAC address. A static address is the same as a dynamic address in terms of funciton. However, you can only manually add and delete a static address rather than learn and age out a static address. A static address is stored in the configuration file and will not be lost even if the device restarts.

By configuring the static address manually, you can bind the MAC address for the network device with the interface in the MAC address table.

2.1.6 Filtering Address

A filtering address is a manually configured MAC address When the device receives the packets from a filtering address, it will directly discard them. You can only manually add and delete a filtering address rather than age it out. A

filtering address is stored in the configuration file and will not be lost even if the device restarts.

If you want the device to filter some invalid users, you can specify their source MAC addresses as filtering addresses. Consequently, these invalid users cannot communicate with outside through the device.

Caution	A filtering address is invalid for the packets sent to the CPU. For example, the L2 source MAC address for an ARP packet is a filtering address, this ARP packet can still be sent to the CPU, but can not be forwarded.

2.1.7 MAC Address Change Notification

The MAC address notification function is an effective way to let you know user changes for the devices in a network.

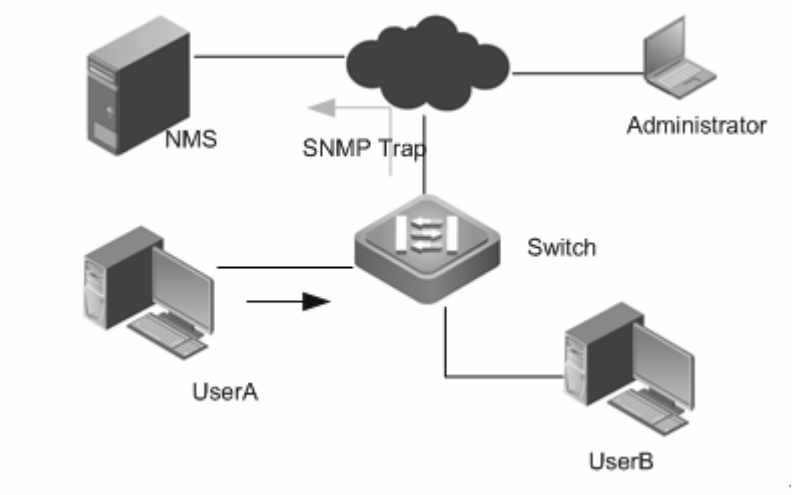


Figure-13 MAC address Change Notification

After the MAC address change notification is enabled, the MAC address change notification infornation is generated and sent in the SNMP Trap message form to the specified NMS when the switch learns a new MAC address or ages out a learned MAC address.

The notification about adding a MAC address lets you know a newcomer (identified by the MAC address) is using the device. The notification about deleting a MAC address (in the case of that the user did not communicate with the device within the aging time) lets you know that a user does not use the device any more.

When many users use the device, lots of MAC address changes may occur in a short period of time (for example, when the device is powered on), incurring additional network traffic. In order to release network burden, you can set the time interval of sending MAC address notifications. All the notification messages within the interval time will be bundled in one SNMP Trap message. So one notification message includes multiple MAC address changes, reducing netowrk traffic significantly.

When a MAC address change notification is generated, it will be recorded in the MAC address notification history list. Then even though the NMS has not been specified to receive the SNMP Trap message, the administrator can view the information about address change by checking the MAC address notification history list.

Caution

MAC address change notification is effective only for dynamic addresses, not for static addresses and filtering addresses.

2.1.8 IP address and MAC address Binding

2.1.8.1 Overview

IP address and MAC address binding lets you filter pakcets. After you bind an IP address and a MAC address, the switch will only receive the IP packets whose source IP address and MAC address match the binding address ;or it will be discarded.

Taking advantages of IP address and MAC address binding, you can check the legality of the input sources. Note that this funciton takes precedence over 802.1X, port-based security and ACL effectiveness.

2.1.8.2 Address Binding Mode

The address binding mode divides into 3 modes: compatible, loose and strict. By default, the address binding mode is strict. The following table lists the corresponding forwarding rules:

Mode	IPv4 packet forward rule	IPv6 packet forward rule
Strict	Packets with IPV4+MAC are forwarded.	No IPV6 packet is forwarded.
Loose	Packets with IPV4+MAC are forwarded.	All IPV6 packets are forwarded.

Compatible	Packets with IPV4+MAC are forwarded.	The IPV6 packets binded with the source MAC addresses are forwarded.

2.1.8.3 Exceptional Ports for the Address Binding

By default, the IP address and MAC address binding function is effective on all ports. You can configure the exceptional ports to make this address binding function ineffective on some ports.

Note

Because the binding relationship on the uplink port is uncertain, generally the uplink port is configured as the exceptional port. It is not necessary to check the IP address and MAC address binding on the uplink port.

Caution

For DES-7200 series, the ARP Check function takes no effect on the IP+MAC binding exceptional port.

2.1.9 Related Protocols

《IEEE Std 802.3™ Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications》

《IEEE Std 802.1Q™ Virtual Bridged Local Area Networks》

2.2 Default MAC Address Table Configuration

Function	Default
Dynamic address aging time	300s
Dynamic address learning mode	dispersive
Dynamic address synchronization	disabled
Limit of VLAN dynamic address	disabled
MAC address change notification	disabled
Address-bind mode	compatible
Bridge Protocol Frame Forwarding Action	BPDU: not forward 802.1x: forward GVRP: not forward

2.3 Setting Dynamic Addresses

2.3.1 Clearing Dynamic Addresses

Command	Function
DES-7200#**clear mac-address-table dynamic**	Clear all dynamic addresses.
DES-7200#**clear mac-address-table dynamic address** *mac-address* **vlan** *vlan-id*	Clear the specified MAC address. *mac-address*：the specified MAC address to be cleared. *vlan-id*：the specified VLAN to which the MAC address to be cleared belongs.
DES-7200#**clear mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	Clear all dynamic addresses on the specified port or Aggregate Port, or clear all dynamic addresses on all interfaces. *Interface-id:* the specified port or Aggregate Port; *vlan-id*：the specified VLAN to which the dynamic address to be cleared belongs.
DES-7200#**clear mac-address-table dynamic vlan** *vlan-id*	Clear all dynamic addresses in the specified VLAN. *vlan-id*：the specified VLAN to which the dynamic address to be cleared belongs.

The following example shows how to clear all dynamic addresses in VLAN 1 on interface GigabitEthernet 0/1:

```
DES-7200#clear mac-address-table dynamic interface GigabitEthernet 0/1 vlan
1
```

2.3.2 Viewing Configurations

Command	Function

DES-7200# **show mac-address-table dynamic**	Show all dynamic addresses.
DES-7200# **show mac-address-table dynamic address** *mac-address* [**vlan** *vlan-id*]	Show the specified dynamic MAC address. *mac-address*：the specified MAC address. *vlan-id*：the specified VLAN to which the MAC address belongs.
DES-7200# **show mac-address-table dynamic interface** *interface-id* [**vlan** *vlan-id*]	Show all dynamic addresses on the specified port or Aggregate Port. *Interface-id:* the specified port or Aggregate Port; *vlan-id*：the specified VLAN to which the dynamic address belongs.
DES-7200# **show mac-address-table dynamic vlan** *vlan-id*	Show all dynamic addresses in the specified VLAN. *vlan-id*：the specified VLAN to which the dynamic address belongs.
DES-7200# **show mac-address-table count**	Show the statistics in the mac address table.

The following example shows all dynamic MAC addresses in VLAN 1 on interface GigabitEthernet 0/1:

```
DES-7200#show mac-address-table dynamic interface gigabitEthernet 0/1 vlan
1
Vlan        MAC Address         Type     Interface
----------  ------------------- -------- ------------------
 1        0000.5e00.010c       DYNAMIC  GigabitEthernet 0/1
 1        00d0.f822.33aa       DYNAMIC  GigabitEthernet 0/1
 1        00d0.f822.a219       DYNAMIC  GigabitEthernet 0/1
 1        00d0.f8a6.5af7       DYNAMIC  GigabitEthernet 0/1
```

The following example shows the statistics in the MAC address table:

```
DES-7200# show mac-address-table count
Dynamic Address Count  : 30
Static  Address Count  : 0
Filtering Address Count: 0
Total Mac Addresses    : 30
Total Mac Address Space Available: 8159
```

2.4 Setting the Address Aging Time

2.4.1 Setting the Aging Time

The following table shows how to set the aging time of address:

Command	Function
DES-7200(config)# **mac-address-table aging-time** [*0 |10-1000000*]	Set the time for an address to be stored in the dynamic MAC address table after it has been learned. It is in the range of 10 to 1000000 seconds, 300 seconds by default. When you set the aging time as 0, the address aging function is disabled and the learned addresses will not be aged.
DES-7200(config)**# no mac-address-table aging-time**	Restore the aging time to the default value.

The following example shows how to set the address aging time to 180s:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mac-address-tabsle aging-time 180
```

2.4.2 Viewing Configurations

Command	Function
DES-7200)**#show mac-address-table aging-time**	Show the aging time of all addresses.

The following example shows how to view the address aging time configurations:

```
DES-7200#show mac-address-table aging-time
Aging time    : 180 seconds
```

Caution

The actual aging time may be different from the setting value for the MAC address table. However, it will not be 2 times than the setting value.

2.5 Setting the Management Learning Mode of Dynamic Addresses

2.5.1 Setting the Dynamic Address Learning Mode

Command	Function
DES-7200(config)# **mac-manage-learning dispersive**	Set the management learning mode of the dynamic address as the dispersive mode.
DES-7200(config)# **mac-manage-learning uniform**	Set the management learning mode of the dynamic address as the uniform mode.

The following example shows how to set the dispersive address learning mode:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mac-manage-learning dispersive
```

2.5.2 Setting the Uniform Address Learning-Sync

Command	Function
DES-7200(config)# **mac-manage-learning uniform learning-synchronization**	In the uniform address learning mode, enable dynamic address synchronization.
DES-7200(config)# **no mac-manage-learning uniform learning-synchronization**	In the uniform address learning mode, disable dynamic address synchronization.
DES-7200(config)# **mac-manage-learning uniform**	Set the management learning mode of the dynamic address as the uniform mode.

The following example shows how to enable dynamic address synchronization:

```
DES-7200#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mac-manage-learning uniform learning-synchronization
```

2.5.3 Viewing Configurations

```
DES-7200 #show mac-address-table mac-manage-learning
MAC manage-learning
running mode: dispersive.
configuration mode: dispersive.
dynamic address learning-synchronization: off.
```

2.6 Setting the Limit of Dynamic Addresses for a VLAN

2.6.1 Setting the Limit of Dynamic Addresses for a VLAN

You can set the limit of dynamic MAC addresses that a VLAN can learn.

The table below sets the limit of the dynamic addresses for a VLAN.

Command	Function
DES-7200**# configure terminal**	Enter the global configuration mode.
DES-7200(config)**# vlan** [*1-4094*]	Enter the VLAN configuration mode.
DES-7200(config-vlan)**# max-dynamic-mac-count** [*1-32768*]	Set the maximum number of dynamic MAC addresses that the VLAN can learn.

To disable the limit of the dynamic addresses for a VLAN, use the **no max-dynamic-mac-count** command.

The following example shows how to set the maximum dynamic address number to 160:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan 1
DES-7200(config-vlan)#max-dynamic-mac-count 160
```

Caution Above listed commands can only be supported by the 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG, 7200-24GE and 7200-24G2XG line cards of DES-7200 series.

2.6.2 Viewing Configurations

Show the maximum number of dynamic addresses for a specified VLAN:

```
DES-7200#show mac-address-table max-dynamic-mac-count vlan 1
vlan limit   mac count learning
---- ------- --------- --------
 1   160       6        YES
```

Show the maximum number of dynamic addresses for all VLANs:

```
DES-7200#show mac-address-table max-dynamic-mac-count
vlan limit   mac count learning
---- ------- --------- --------
 1   160     6        YES

 3   500     124      YES
```

Caution Above listed commands can only be supported by the 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG, 7200-24GE and 7200-24G2XG line cards of DES-7200 series.

2.7 Setting the Static MAC Addresses

2.7.1.1 Adding and Removing the Static MAC Addresses

You can add a static address to the MAC address table by specifying the destination MAC address, the VLAN (the static address will be added to the address table of this VLAN), and the interface (the packets to the destination MAC address are forwarded to this interface).

To add a static address, execute the following commands:

Command	Function

Command	Function
DES-7200(config)# **mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	*mac-addr*: Specify the destination MAC address to which the entry corresponds. *vlan-id*: Specify the VLAN to which this address belongs. *interface-id:* specify the interface (physical port or aggregate port) to which the packet is forwarded. Upon receiving the packets to the destination MAC address in the VLAN, the switch will forward them to the interface.
DES-7200(config)# **no mac-address-table static** *mac-address* **vlan** *vlan-id* **interface** *interface-id*	Remove the static MAC address entries.

The following example shows how to configure the static address 00d0.f800.073c. When a packet to this address is received in VLAN 4, it is forwarded to Gigabitethernet 0/3.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# mac-address-table static 00d0.f800.073c vlan 4 interface
gigabitethernet 0/3
```

The following example shows how to remove the static address 00d0.f800.073c.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#no mac-address-table static 00d0.f800.073c vlan 4 interface
gigabitethernet 0/3
```

2.7.1.2 Viewing Configurations

Command	Function
DES-7200# **show mac-address-table static**	Show the information of all the static MAC addresses.

The following example shows how to view the information of all the static MAC addresses:

```
Vlan        MAC Address         Type      Interface
----------  ------------------- -------- ------------------
          4       00d0.f800.073c       STATIC    GigabitEthernet 0/3
```

2.8 Setting the Filtering MAC Addresses

2.8.1.1 Adding and Removing the Filtering Addresses

To add a filtering address, specify the MAC address to be filtered and the VLAN that the MAC address belongs to. The device will directly discard the packets from the MAC address in the VLAN.

To add a filtering address, execute the following command:

Command	Function
DES-7200(config)# **mac-address-table filtering** *mac-addr* **vlan** *vlan-id*	mac-addr: Specify the MAC address to be filtered by the device. vlan-id: Specify the VLAN to which this address belongs.
DES-7200(config)# **no mac-address-table filtering** *mac-addr* **vlan** *vlan-id*	Remove the filtering MAC address entries.

The following example shows how to configure the filtering address 00d0.f800.073c. When a packet to or from this address is received in VLAN 4, it will be discarded.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# mac-address-table filtering 00d0.f800.073c vlan 4
```

The following example shows how to remove the filtering address 00d0.f800.073c.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#no mac-address-table filtering 00d0.f800.073c vlan 4
```

2.8.1.2 Viewing Configurations

Command	Function
DES-7200# **show mac-address-table filtering**	Show the information of all the filtering MAC addresses.

The following example shows how to view the information of all the filtering MAC addresses:

```
Vlan         MAC Address          Type      Interface
----------  -------------------- -------- ------------------
          4       00d0.f800.073c       FILTER    GigabitEthernet 0/3
```

2.9 Setting MAC Address Change Notification

2.9.1 Setting MAC Address Change Notification

By default, the global switch of MAC addresses is turned off, so the MAC address change notification function is disabled on all interfaces.

To configure the MAC address change notification function, execute the following command:

Command	Function
DES-7200(config)# **snmp-server host** *host-addr* **traps** [**version** {**1 | 2c |3 [auth | noauth | priv**]}] *community-string*	Configure the NMS to receive the MAC address change notification. *host-add*: IP address of the receiver. *version:* Specify the version of the SNMP Trap message to be sent. *community-string*: Specify the authentication name carried with the SNMP Trap message.
DES-7200 (config)**#snmp-server enable traps**	Allow the switch to send the SNMP Trap message.
DES-7200(config)# **mac-address-table notification**	Turn on the global switch of the MAC address change notification function.
DES-7200(config)# **mac-address-table notification** {**interval** *value* | **history-size** *value*}	*interval value* :Interval of generating the MAC address change notification (optional), in the range of 1 to 3600 seconds, 1 second by default. *history-size value*: Maximum number of the records in the MAC notification history list, in the range of 1 to 200, 50 by default.

Command	Function
DES-7200(config-if)# **snmp trap mac-notification** {**added	removed**}	Enable the MAC address change notification on the interface. added: Send a MAC address change notification when a MAC address is **added** on this interface. Removed: Send a MAC address change notification when a address is deleted.

To disable the MAC address change notification function, use the **no snmp-server enable traps** command in the global configuration mode. To turn off the global switch of the MAC address change notification function, use the **no mac-address-table notification** command. To disable the MAC address change notification funciton on a specified interface, use the **no snmp trap mac-notification** {**added** | **removed**} command in the interface configuration mode.

This example shows how to enable the MAC address change notification funciton, use public as the authentication name to send a MAC address change notification to the NMS whose IP address is 192.168.12.54 at the interval of 40 seconds, set the size of the MAC address change history list to 100, and enable the MAC address change notification funciton on gigabitethernet 0/1 when a MAC address is added or removed.

```
DES-7200(config)# snmp-server host 192.168.12.54 traps public
DES-7200(config)# snmp-server enable traps
DES-7200(config)# mac-address-table notification
DES-7200(config)# mac-address-table notification interval 40
DES-7200(config)# mac-address-table notification  history-size 100
DES-7200(config)# interface gigabitethernet 0/1
DES-7200(config-if)# snmp trap mac-notification added
DES-7200(config-if)# snmp trap mac-notification removed
```

2.9.2 Viewing the MAC Address change Notification Information

In the privileged mode, you can view the information on the MAC address table of the device by using the commands listed in the following table:

Command	Function

Command	Function
DES-7200# **show mac-address-table notification**	Show the global configuration of the MAC address change notification function.
DES-7200# **show mac-address-table notification interface**	Show the configuration of the MAC address change notification on the interface.
DES-7200# **show mac-address-table notification history**	Show the history list of the MAC address change notification.

The following examples show how to view the MAC address change notification.

View the global configuration of the MAC address change notification:

```
DES-7200# show mac-address-table notification
MAC Notification Feature : Enabled
Interval(Sec): 2
Maximum History Size : 154
Current History Size : 2
DES-7200# show mac-address-table notification interface
Interface          MAC Added Trap MAC Removed Trap
---------------- -------------- ----------------
Gi0/1              Disabled      Enabled
Gi0/2              Disabled      Disabled
Gi0/3              Enabled       Enabled
Gi0/4              Disabled      Disabled
Gi0/5              Disabled      Disabled
Gi0/6              Disabled      Disabled
DES-7200# show mac-address-table notification history
History Index:1
Entry Timestamp: 15091
MAC Changed Message :
Operation   VLAN MAC Address    Interface
---------- ---- -------------- --------------------
Added       1    00d0.f808.3cc9 Gi0/1
Removed     1    00d0.f808.0c0c Gi0/1
History Index:2
Entry Timestamp: 21891
MAC Changed Message :
Operation   VLAN  MAC Address    Interface
----------- ---- ------------- --------------------
Added       1    00d0.f80d.1083 Gi0/1
```

2.10 Setting IP Address and MAC Address Binding

2.10.1 Setting IP Address and MAC address Binding

In the global mode, to configure IP address and MAC address binding, execute the following commands.

Command	Function
DES-7200(config)**# address-bind** *ip-address mac-address*	Configure IP address and MAC address binding.
DES-7200(config)**# address-bind install**	Enable the address binding function.

To cancel the IP address and MAC address binding, use the **no address-bind** *ip-address mac-address* command in the global configuration mode.

To disable the address binding function, execute the **no address-bind install** command.

The following example shows how to bind the IP address and MAC address:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#address-bind 192.168.5.1 00d0.f800.0001
DES-7200(config)#address-bind install
```

Problem: In the stack environment, if one switch learns the MAC address when receiving the IP packets not correspond to the address binding, this MAC address can only be learned by the chip of that switch and cannot be learned by the chips of other switches in the stack environment.

Caution

Phenomenon: In the stack environment, if one switch learns the MAC address when receiving the IP packets not correspond to the address binding, this address entry is displayed using the **show mac** command and the IP packets can still be broadcasted to other stack switches. The MAC address learning is normal when receiving the non-IP packets or the IP packets correspond to the address binding.

Workaround: N/A.

After executing the **address-bind install** command but the IP+MAC binding is not configured, then allow all packets to be transmitted on the interface.

Note

For DES-7200 series, when the global IP+MAC binding, port security and DOT1X are co-used and no matter whether the security channel is enabled or not, all secure users can communicate with each other.

2.10.2 Setting the Address Binding Mode

In the global mode, to configure the address binding mode, execute the following commands.

Command	Function
DES-7200(config)# **address-bind ipv6-mode** { **compatible**| **loose** | **strict** }	Configure the address binding mode.
DES-7200(config)# **no adress-bind ipv6-mode**	Restore to the default address binding mode.

The following example shows how to set the address binding mode to strict:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#address-bind ipv6-mode strict
```

In the IPV6 mode, DHCP Snooping address binding, port security MAC+IP address binding functions are enabled at the same time.

Mode	IPv4 packet forward rule	IPv6 packet forward rule
Strict	Only packets with IPV4+MAC are forwarded.	Only IPV6 packets with IPv6 security address configured are allowed to be forwarded.
Loose	Only packets with IPV4+MAC are forwarded.	All IPV6 packets are allowed to be forwarded.
Compatible	Only packets with IPV4+MAC are forwarded.	Only IPV6 packets binded with the source MAC address or the security address configured are allowed to be forwarded. For DES-7200 series, when the IPv6 compatible mode, port security and DOT1X authentication are co-used, all IPv6 packets with the secure address can be transmitted on the interface.

Caution

2.10.3 Setting the Exceptional Ports for the IP Address and MAC Address Binding

To make the IP address and MAC address binding not to take effect on some ports, you can set these ports as exceptional ports. To configure an exceptional port, execute the following command in the global configuration mode.

Command	Function
DES-7200(config)#address-bind uplink *interface-id*	Configure the exceptional port for the IP address and MAC address binding. *Interface-id:* port or Aggregate port

Use the **no address-bind uplink** *interface-id* command to cancel the configuration of the specified exceptional port.

The following example shows how to set the interface GigabitEthenet 0/1 to the exceptional port:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# address-bind uplink GigabitEthernet 0/1
```

2.10.4 Viewing the IP Address and MAC Address Binding Table

To show the IP address and MAC address binding table, use the **show address-bind** command in the privileged mode:

Command	Function
DES-7200(config)#show address-bind	View the IP address and MAC address binding table.

The following example shows how to view the IP address and MAC address binding table :

```
DES-7200#show address-bind
Total Bind Addresses in System : 1

IP Address        Binding MAC Addr
---------------    ----------------
   192.168.5.1    00d0.f800.0001
```

2.11 Configuration Examples

2.11.1 Network Topology

As Figure-14 shows, the database server connects to the switch through the interface GigabitEthernet 0/1, the web server connects to the switch through the

interface GigabitEthernet 0/2, and the server administrator connects to the switch through the interface GigabitEthernet 0/3. Other users access the web server through the interface GigabitEthernet 0/10. All data are forwarded in VLAN 1.

The static MAC address configuration enables the data exchanged between the web server and the database server, the administrator and the server to be forwarded in the unicast form, preventing these data from being forwarded in the broadcast form in the user network and ensuring the security of the information exchanged between the web server and the database server, the administrator and the server .

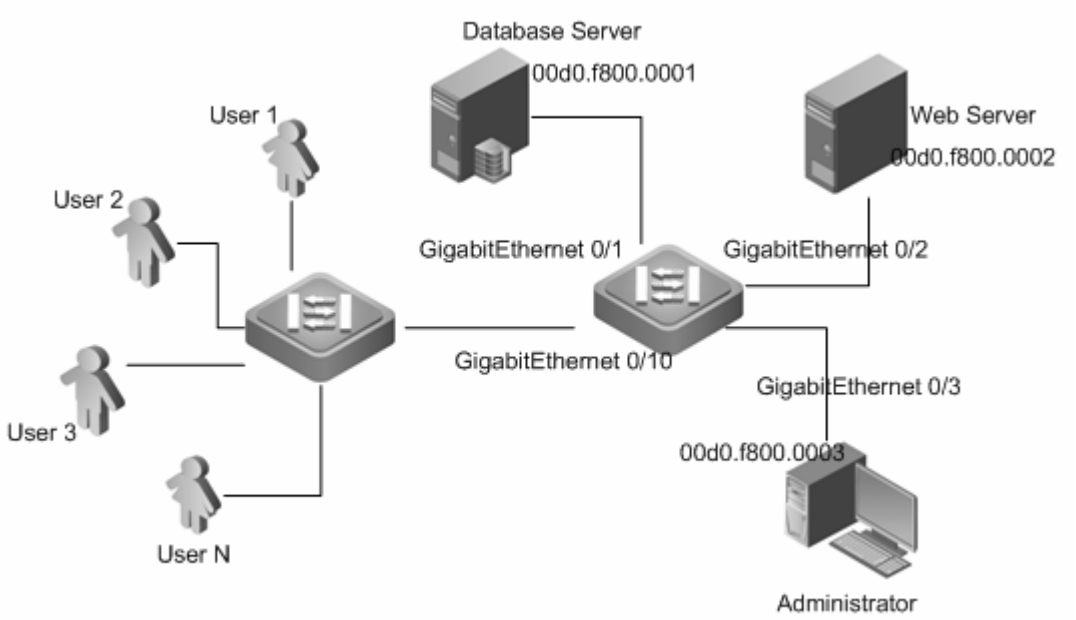


Figure 1 Typical Configuration Topology

2.11.2 Configurations

The following example shows how to configure the switch:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mac-address-table static 00d0.f800.0001 vlan 1 interface
GigabitEthernet 0/1
DES-7200(config)#mac-address-table static 00d0.f800.0002 vlan 1 interface
GigabitEthernet 0/2
DES-7200(config)#mac-address-table static 00d0.f800.0003 vlan 1 interface
GigabitEthernet 0/3
```

The following example shows the switch configurations:

```
DES-7200#show mac-address-table static
Vlan       MAC Address        Type    Interface
----------  ------------------- -------- ------------------
```

```
1       00d0.f800.0001      STATIC   GigabitEthernet 0/1
1       00d0.f800.0002      STATIC   GigabitEthernet 0/2
1       00d0.f800.0003      STATIC   GigabitEthernet 0/3
```

3 Aggregate Port Configuration

This chapter explains how to configure an aggregate port on DES-7200 devices.

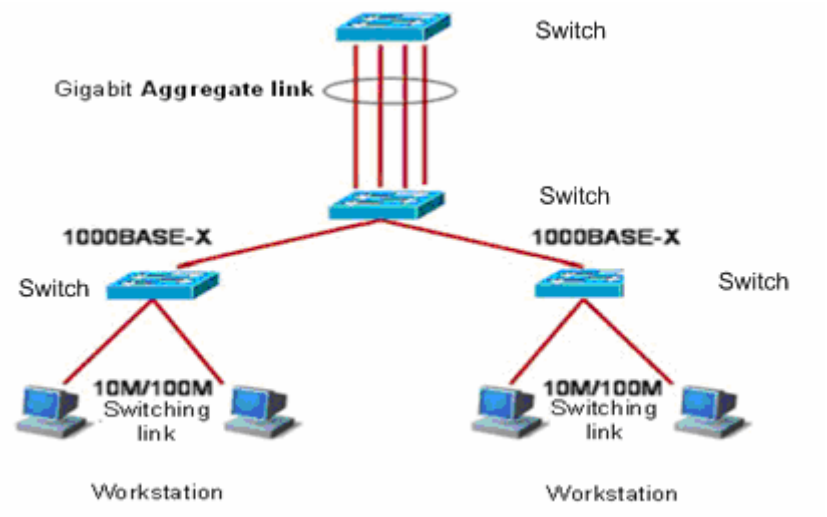
3.1 Overview

3.1.1 Understanding Aggregate Port

Multiple physical links can be bound into a logical link, called an aggregate port (hereinafter referred to as AP). DES-7200 devices provide the AP function that complies with the IEEE802.3ad standard. This function can be used to expand link bandwidth and improve reliability.

AP function supports traffic balancing that evenly allocating the traffic to every member link. AP function also supports link backup. When a link member in an AP is disconnected, the system will automatically allocate the traffic of the member link to other active member links in the AP, except for the broadcast or multicast packets it received.

Typical AP configurations



Each AP includes up to 8 member ports.

Product Model	Supported max AP number
DES-7200	128

3.1.2 Understanding Traffic Balancing

Traffic can be evenly distributed on the member links of an AP according to the features such as source MAC address, destination MAC address, combination of source MAC address and destination MAC address, source IP address, destination IP address, and combination of source IP address and destination IP address. The **aggregateport load-balance** command can be used to set the method to distribute traffic.

Source MAC address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the source MAC addresses of packets. Those packets with different source MAC addresses are evenly distributed on the member links of an AP according to different source MAC addresses. Those packets with the same source MAC address are forwarded through the same member link.

Destination MAC address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the destination MAC addresses of packets. Those packets with different destination MAC addresses are evenly distributed on the member links of an AP according to different destination MAC addresses. Those packets with the same destination MAC address are forwarded through the same member link.

The traffic balancing based on the combination of source MAC address and destination MAC address refers to distribute the traffic on the member links of an AP according to the combination of source MAC address and destiantion MAC address of packets. Those packets with different source and destination MAC addresses are evenly distributed on the member links of an AP according to different source and destination MAC addresses. Those packets with the same source and destination MAC address are distributed on the same member link.

Source IP address- or destination IP address-based traffic balancing refers to distribute the traffic on the member links of an AP according to the source IP addresses or destination IP addresses of packets. Those packets with different source IP addresses or destination IP addresses are evenly distributed on the member links of an AP according to different source or destination IP addresses. Those packets with the same source IP address or destination IP address are forwarded through the same member link. This mode is specific for Layer 3

packets. If layer2 packets are received under this mode, traffic balancing is performed automatically according to the default device setting.

The traffic balancing based on the combination of source IP address and destination IP address refers to distribute the traffic on the member links of an AP according to the combination of source IP address and destiantion IP address of packets. Those packets with different source and destination IP addresses are evenly distributed on the member links of an AP according to different source and destination IP addresses. Those packets with the same source IP address and destination IP address are forwarded through the same member link. This mode is specific for Layer 3 packets. If layer2 packets are received under this mode, traffic balancing is performed automatically according to the default device setting.

All the abovementioned balancing modes are applicable to AP on Layer 2 and Layer 3.

Table-1 lists the traffic balancing modes supported on different switch models, wherein " √ " indicates support, "×" indicates no support.

Traffic Balancing Mode	Source MAC-based	Destination MAC-based	Source+Destination MAC-based	Source IP-based	Destination IP-based	Source+Destination IP-based
DES-7200	√	√	√	√	√	√

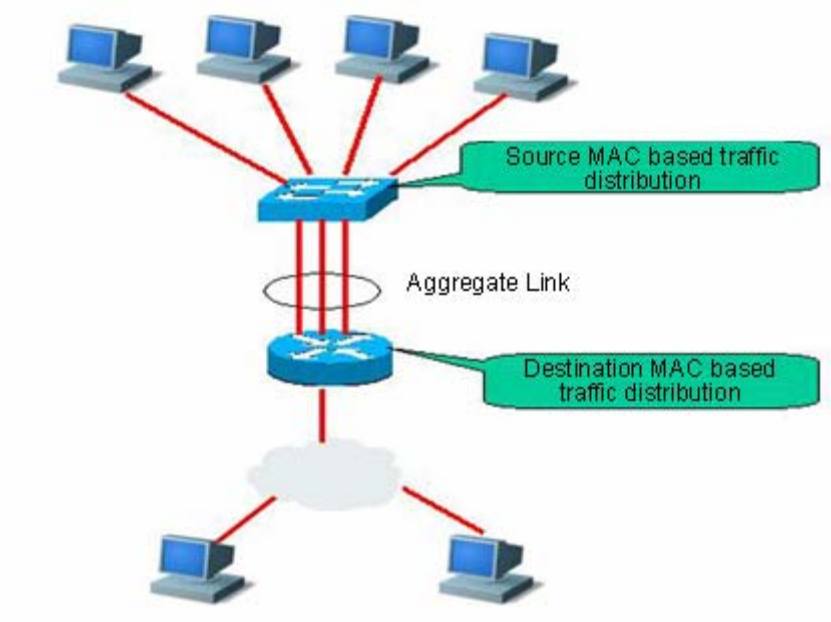
An appropriate traffic distribution method should be set according to the actual network environments, so that the traffic can be evenly distributed on the the links for the maximum utilization of network bandwidth.

In the following diagram, a switch communicates with a router through an AP, and the router serves as the gateway for all the devices inside the network (such as 4 PCs on the top of the diagram). The source MAC addresses of all the packets that the devices outside the network (such as 2 PCs at the bottom of the diagram) send through the router are the MAC address of the gateway. In order to distribute traffic between the router and other hosts on other links, traffic balancing should be performed based on the destination MAC address. However, traffic balancing should be performed based on the source MAC address on the switch.

Note

When the traffic balancing mode is source IP address-based, destination IP address-based, or source IP address and destination IP address-based traffic balancing mode, Layer 2 packets are distributed under the default device mode. You can execute **show aggregateport load-balance** command to get the default device mode before setting the parameter *aggregateport load-balance.*

AP traffic balancing



3.2 Configuring Aggregate Port

3.2.1 Default Aggregate Port Configuration

The default AP configuration is shown in the table below.

Attribute	Default value
Layer-2 AP interface	None
Layer-2 AP interface	None
Traffic balancing	Traffic is distributed according to the source MAC addresses of the incoming packets.

Caution By default, the DES-7200 series perform traffic balancing based on the combination of the source MAC addresses and destination MAC addresses of the incoming packets.

3.2.2 Aggregate Port Configuration Guide

- The rates of the member ports of an AP must be the same.
- L2 ports can only be join a L2 AP, and L3 ports can only join a L3 AP. L2/L3

attributes of AP including member ports must not be modified.

- An AP does not support port security.
- Once a port is added to an AP, its attributes will be replaced by those of the AP.
- Once a port is removed from an AP, its attributes will be restored to original attributes.

Caution

When a port is added to an AP, you cannot perform any configuration on the port before removing the port from the AP.

3.2.3 Configuring a Layer2 Aggregate Port

In the interface configuration mode, add the interface to an AP by performing the following steps.

Command	Function
DES-7200(config-if-range)# **port-group** *port-group-number*	Add the interface to an AP (the system will create the AP if it does not exist).

In the interface configuration mode, use the **no port-group** command to remove a physical port from the AP.

The example below shows how to configure the layer2 Ethernet interface 1/0 to a member of layer2 AP 5.

```
DES-7200# configure terminal
DES-7200(config)# interface range gigabitEthernet 0/1
DES-7200(config-if-range)# port-group 5
DES-7200(config-if-range)# end
```

The command **interface aggregateport** *n* (n is the AP number) in the global configuration mode can be used to directly create an AP (if AP n does not exist).

3.2.4 Configuring a Layer3 Aggregate Port

By default, an aggregate port is on layer 2. To configure a layer-3 AP, perform the following operations.

The example below shows how to configure a layer-3 AP (AP 3) and configure its IP address (192.168.1.1):

```
DES-7200# configure terminal
DES-7200(config)# interface aggretegateport 3
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
```

```
DES-7200(config-if)# end
```

Caution

Only L3 switch support L3 AP.

You shall create a L3 AP before adding the interface to the L3 AP by executing **port-group** command.

The example below shows how to add the interface gigabitEthernet 0/1-3 to L3 AP:

```
DES-7200# configure terminal
DES-7200(config)# interface range gigabitEthernet 0/1-3
DES-7200(config-if)# no switchport

DES-7200(config-if)# port-group 2
```

3.2.5 Configuring Traffic Balancing on an Aggregate Port

In the configuration mode, configure traffic balancing on the AP by performing the following steps:

Command	Function
DES-7200(config)# **aggregateport load-balance** {**dst-mac** | **src-mac | src-dst-mac | dst-ip | src-ip | src-dst-ip** }	Set the AP traffic balancing and select the algorithm: **dst-mac:** Distribute traffic according to the destination MAC addresses of the incoming packets. **src-mac:** Distribute traffic according to the source MAC addresses of the incoming packets. **src-dst-mac:** Distribute traffic according to the combination of the source MAC addresses and destination MAC addresses of the incoming packets. **src-ip**: Distribute traffic according to the source IP addresses of the incoming packets. **dst-ip**: Distribute traffic according to the destination IP addresses of the incoming packets. **src-dst-ip:** Distribute traffic according to the combination of the source IP addresses and destination IP addresses of the incoming packets.

To restore the traffic balancing configuration of an AP to the default value, execute the **no aggregateport loag-balance** command in the global configuration mode:

3.3 Showing an Aggregate Port

In the privileged mode, show the AP configuration by performing the following steps.

Command	Function
DES-7200# **show aggregateport** [*port-number*]{**load-balance | summary**}	Show the AP settings.

```
DES-7200# show aggregateport load-balance
Load-balance : Source MAC address
DES-7200# show aggregateport 1 summary
AggregatePort MaxPorts SwitchPort Mode   Ports
------------- -------- ---------- ------
Ag1             8        Enabled          ACCESS
```

4 LACP Configuration

4.1 Overview

LACP(Link Aggregation Control Protocol) is a protocol based on IEEE802.3ad and aims to implement the dynamic link aggregation and deaggregation. This protocol interacts with its peer by using the LACPDU(Link Aggregation Control Protocol Data Unit).

With LACP enabled on the port, LACP notifies the following information of the port by sending LACPDUs: priority and MAC address of the system, port priority, number and operation key. Upon receiving the information, the peer determines the port that can be aggregated by comparing the reveived information with the information of other ports on the peer device. In this way, the two parties can reach an aggreement in adding/removing the port to/from a dynamic aggregation group.

4.2 Dynamic Link Aggregation Mode

A LACP port can be in one of the three aggregation modes: Active, Passive and Static.

The port in the active state will transceive the LACP packets and negotiate with the peer end, the port in the passive state will only respond to the received LACP pacekts, and the port in the static mode will not transceive the LACP packets or negotiate with the peer end, see the static AP configuration guide *AP-SCG.doc* for detailed configuration.

Port mode	Neighbor port mode
Active mode	Active or passive mode.
Passive mode	Active mode
Static mode	Static mode.

4.3 LACP Port State

The port member in the aggregation group can be in the following 3 states:

When the link state of the port is Down, no packet is forwarded on the port. The port state is **down**.

When the link state of the port is Up, after the LACP negotiation, the port joins in the packet forwarding as a port member in the aggregation group. The port state is **bndl**.

When the link state of the port is Up, the port fails to join in the packet forwarding because the LACP is not enabled on the port, or the attribute of the port and the master port is inconsistent. The port state is **susp**.

Note

- Only the port with full-duplex attribute can be aggregated.
- The port rate, flow-control, media-type and Layer2&3 port attribute must be consistent.
- After the port aggregation, changing the above port attributes will lead to the aggregation failure of other ports in the same aggregation group.

Caution

- The LACP cannot be enabled on the ports with the function of forbidding the member ports to add to or leave the AP enabled; and the function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP member ports. The AP with the function of forbidding the member ports to add to or leave cannot configured as the LACP AP, and function of forbidding the member ports to add to or leave the AP cannot be enabled on the LACP AP.
- The SYSLOG will be displayed when the LACP fails to leave the AP due to external function limitations, such as: %LACP-5-UNBUNDLE_FAIL: Interface FastEthernet 0/1 failed to leave the AggregatePort 1. In this case, please modify the configuration to cancel the related configuration of forbidding the member ports to leave the AP, otherwise the normal packets transmission on the AP will be influenced.

4.4 Dynamic Link Aggregation Priority Relations

4.4.1 LACP System ID

Only one LACP aggregation system can be configured on each device. Each LACP aggregation system has sole system priority. The system ID consists of LACP system priority and the device MAC address. First compare the two system priorities: the lower the system priority is, the higher the system ID will be. Then compare the two device MAC addresses if the system priorities are equal: the smaller the MAC

address is , the higher the system ID will be. The system with the higher system ID determines the port state.

4.4.2 LACP Port ID

Each port owns an independent LACP port priority, which is configurable. The port ID consists of LACP port priority and port number. First compare the two port priorities: the lower the port priority value is, the higher the port ID is. Then compare the two port numbers if the two port priorities are equal: the smaller the port number is, the higher the port ID is.

4.4.3 LACP Master Port

When the dynamic member port is up, LACP selects a port with the highest priority in the aggregation group based on the port rate, duplex rate, ect. Only can the ports with the same attributes with the master port be aggregated and join in the packet forwarding in the aggregation group. When the port attributes change, LACP re-selects the master port without deaggregation. But when the new master port is not aggregated, LACP deaggregates the member ports in the aggregation group and re-aggregates.

4.4.4 LACP Negotiation Procedure

Upon receiving the LACP packets from the peer port, the system ID with higher priority is selected. On the end of higher system ID, set the ports in the aggregation group are to be aggregated in the descending order of port priority(when the number of ports in the aggregation group exceeds the maximum port number, the state of the ports exceeding the aggregation capacity is **sups**.) Upon receiving the updated LACP packets on the peer port, the corresponding port is to be aggregated.

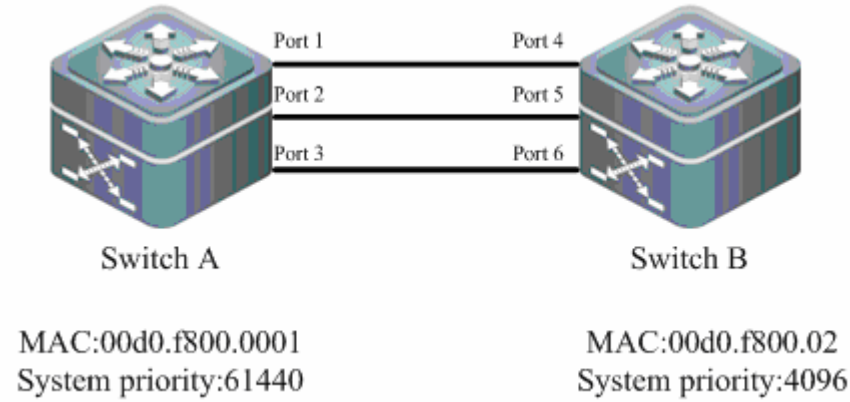


Figure-1 LACP Negotiation

As shown in Figure-1, switch A and switch B are interconnected through the 6 ports. Set the system priority for the switchA and the switchB to be 61440 and 4096

respectively. Enable the LACP function on the 6 ports directly-connected between the switches. Set the aggregation mode for the 3 ports is active, and set the default port priority for the other 3 ports as 32768.

Upon receiving the LACP packets from the switchA, switchB finds its system priority is higher than the switchA, the port4-6 on the switchB are to be aggregated according to the sequence of the port priority. After receiving the updated LACP packets from the switchB, the switchA finds its system priority is lower than the switchB and the port1-3 on the switchA are also aggregated.

4.5 LACP Requirements

LACP is a protocol that automatically add/remove the port to/from the aggregation group. The requirements of the auto-aggreagation of those two ports are:

Only can the ports with the same operation key be aggregated;

Only can the ports that are with the same attributes such as port rate and duplex as the master port be dynamically aggregated.

The port link state is UP, the peer port running LACP and the port or the peer port must be in the Active mode.

4.6 LACP Configuration

4.6.1 Configuring LACP

You can configure the LACP system priority, port priority and administrative key in the aggregation group. All dynamic link groups on one switch share one LACP system priority. Changing the system priority will affect all aggregation groups.

Run the following commands to configure the LACP:

Command	Function
DES-7200# **configure**	Enter the global configuration mode.
DES-7200(config)# **lacp system-priority** *system-priority*	(Optional) Set the LACP system priority, in the range of 0-65535. The default system priority is 32768.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **lacp port-priority** *port-priority*	(Optional) Set the LACP port priority, in the range of 0-65535. The default system priority is 32768.

Command	Function
DES-7200(config-if)# **port-group** *key* **mode active | passive**	Add the port to the aggregation group and specify the LACP port mode. If the aggregation group does not exist, an aggregation group will be created. *key:* the administrative key of the aggregation group. **active:** the port is added to the dynamic aggregation group in the active mode. **passive:** the port is added to the aggregation group in the passive mode.
DES-7200(config-if)# **end**	Return to the privileged mode.

4.6.2 Viewing the LACP Configuration

To view the LACP state, run the following command in the privileged mode:

Command	Function
DES-7200# **show lacp summary**	Show the LACP state information.

4.7 LACP Configuration Example

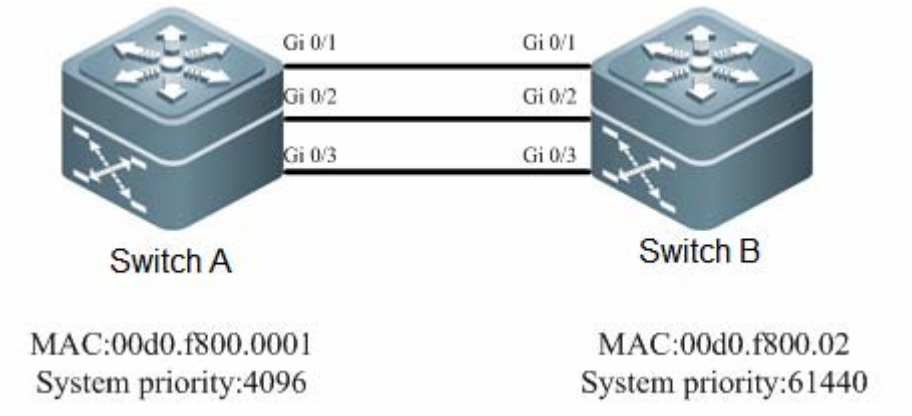


Figure-2 LACP Link Aggregation

As shown in the figure-2, on the SwitchA, set the LACP system priority as 4096, enable the LACP on the interface Gi 0/1、Gi 0/2、 Gi 0/3, and set the LACP port priority as 4096:

```
SwitchA#configure terminal
SwitchA(config)# lacp system-priority 4096
SwitchA(config)# interface range GigabitEthernet 0/1-3
SwitchA(config-if-range)# lacp port-priority 4096
SwitchA(config-if-range)# port-group 3 mode active
SwitchA(config-if-range)# end
```

On the SwitchB, set the LACP system priority as 61440, enable the LACP on the interface Gi 0/1、Gi 0/2、 Gi 0/3, and set the LACP port priority as 61440:

```
SwitchB# configure terminal
SwitchB(config)# lacp system-priority 61440
SwitchB(config)# interface range GigabitEthernet 0/1-3
SwitchB(config-if-range)# lacp port-priority 61440
SwitchB(config-if-range)# port-group 3 mode active
SwitchB(config-if-range)# end
```

After the configuration, if the LACP negotiation succeeds, it prompts the following log:

```
*Feb 25 17:11:31: %LACP-5-BUNDLE: Interface Gi0/1 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/2 joined AggregatePort 3.
*Feb 25 17:11:32: %LACP-5-BUNDLE: Interface Gi0/3 joined AggregatePort 3.
*Feb 25 17:11:32: %LINEPROTO-5-UPDOWN: Line protocol on Interface AggregatePort
3, changed state to up
```

Then show the member port state in the aggregation group on the SwitchA:

```
DES-7200(config)#show LACP summary
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs.
A - Device is in active mode.       P - Device is in passive mode.

Aggregate port 3:

Local information:
                          LACP port      Oper    Port    Port
Port    Flags    State    Priority       Key    Number  State
-------------------------------------------------------------
Gi0/1    SA       bndl       4096          0x3    0x1     0x3d
Gi0/2    SA       bndl       4096          0x3    0x2     0x3d
Gi0/3    SA       bndl       4096          0x3    0x3     0x3d
```

```
Partner information:
                  LACP port                Oper    Port    Port
Port    Flags     Priority     Dev ID      Key     Number  State
------------------------------------------------------------------
Gi0/1    SA       61440    00d0.f800.0002   0x3     0x1     0x3d
Gi0/2    SA       61440    00d0.f800.0002   0x3     0x2     0x3d
Gi0/3    SA       61440    00d0.f800.0002   0x3     0x3     0x3d
```

The following table describes the fileds:

Field	Description
Local information	Show the local LACP information.
Port	Show the system port ID.
Flags	Show the port state flag: “S” indicates that the LACP is stable and in the state of periodically sending the LACPPDU; “A” indicates that the port is in the active mode.
S	Show the device is requesting slow LACPDUs, that is sending a packet per 30 seconds.
F	Show the device is requesting fast LACPDUs, that is sending a packet every second.
A	Show the port is in the active mode.
P	Show the port is in the passive mode.
State	Show the port aggregation information: “bndl” indicates that the port is aggregated; “Down” represents the disconnection port state; “susp” indicates that the port is not aggregated.
LACP Port Priority	Show the LACP port priority.
Oper Key	Show the port operation key.
Port Number	Show the port number.
Port State	Show the flag bit for the LACP port state.
Partner infomation	Partly show the LACP information of the peer port.
Dev ID	Partly show the system MAC information of the peer device.

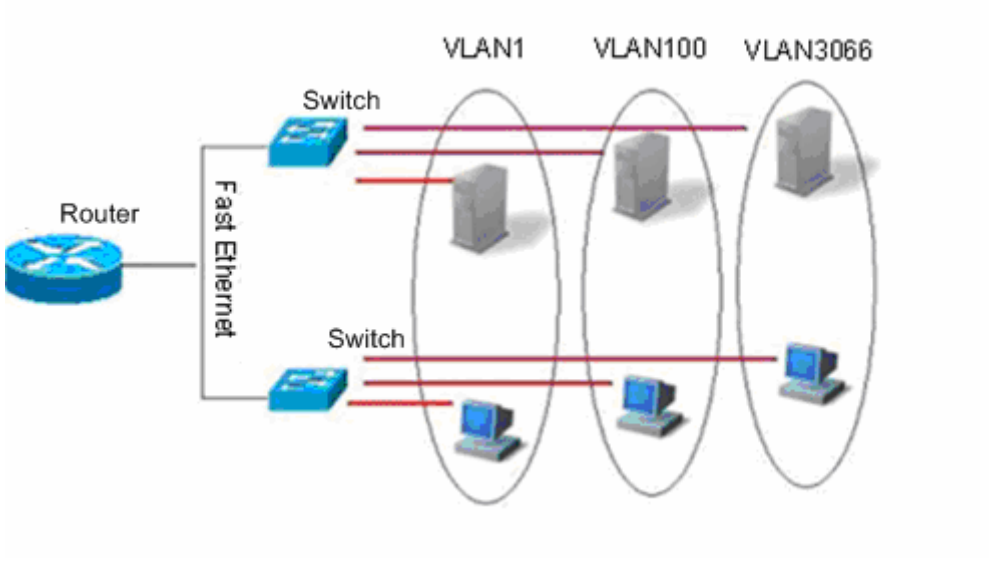
5 VLAN Configuration

This chapter describes how to configure IEEE802.1q VLAN.

5.1 Overview

Virtual Local Area Network (VLAN) is a logical network divided on a physical network. VLAN corresponds to the L2 network in the ISO model. The division of VLAN is not restricted by the physical locations of network ports. A VLAN has the same attributes as a common physical network. Except for no restriction on physical location, unicast, broadcast and multicast frames on layer 2 are forwarded and distributed within a VLAN, not being allowed to directly go to other VLANs.Therefore, when a host in a VLAN wants to communicate with another host in another VLAN, a layer 3 device must be used, as shown in the following diagram.

You can define a port as the member of a VLAN. All the terminals connected to the specified port are part of the VLAN. A network can support multiple VLANs. In this case, when you add, delete, and modify users in the VLANs, you do not need to modify the network configuration physically.



Like a physical network, a VLAN is usually connected to an IP subnet. A typical example is that all the hosts in the same IP subnet belong to the same VLAN. A layer 3 device must be used for communication between VLANs. DES-7200 L3 devices can perform IP routing between VLANs through SVI (Switch Virtual Interfaces). For the configuration about SVI, refer to *Interface Management Configuration* and *IP Unicast Routing Configuration*.

5.1.1 Supported VLAN

Complying with IEEE802.1Q Standard, our products support up to 4094 VLANs(VLAN ID 1-4094), in which VLAN 1 is the default VLAN that cannot be deleted.

Caution

DES-7200 series support 4094 VLANs.

5.1.2 VLAN Member Type

You can determine the frames that can pass a port and the number of VLANs that the port can belong to by configuring the VLAN member type of the port. For the detailed description about VLAN member type , see the following table:

Member Type	Port Feature
Access	One access port can belong to only one VLAN, which must be specified manually.
Trunk (802.1Q)	By default, one Trunk port belongs to all the VLANs of the device itself, and it can forward the frames of all the VLANs. However, you can impose restriction by setting a list of allowed VLANs.

5.2 Configuring a VLAN

A VLAN is identified by its VLAN ID. You can add, remove, and modify the VLANs in the range of 2 to 4094 on a device. VLAN 1 is created by a device automatically and cannot be removed.

You can configure the member type of a port in a VLAN, add a port to a VLAN, and remove a port from a VLAN in the interface configuration mode.

5.2.1 Saving the VLAN Configuration

To save the VLAN configuration in the configuration file, execute the **copy running-config startup-config** command in the privileged mode. To view VLAN configuration, execute the **show vlan** command.

5.2.2 Default VLAN Configuration

The following table shows the default configuration of a VLAN.

Parameter	Default value	Range
VLAN ID	1	1 to 4094
VLAN Name	VLAN xxxx, where xxxx is the VLAN ID	None
VLAN State	Active	Two status: active or inactive

5.2.3 Creating/Modifying a VLAN

In the privileged mode, you can create or modify a VLAN by executing the following commands.

Command	Function
DES-7200(config)**# vlan** *vlan-id*	Enter a VLAN ID. If you enter a new VLAN ID, the device will create it. If you enter an existing VLAN ID, the device modifies the corresponding VLAN.
DES-7200(config)**# name** *vlan-name*	(Optional) Name the VLAN. If you skip this step, the device automatically assigns the VLAN a name of VLAN xxxx, where xxxx is a 4-digit VLAN ID starting with 0. For example, VLAN 0004 is the default name of VLAN 4.

To restore the name of a VLAN to its default, simply enter the **no name** command.

The following example creates VLAN 888, names it test888, and saves its configuration into the configuration file:

```
DES-7200# configure terminal
DES-7200(config)# vlan 888
DES-7200(config-vlan)# name test888
DES-7200(config-vlan)# end
```

5.2.4 Deleting a VLAN

You cannot delete the default VLAN (VLAN 1).

In the privileged mode, you can delete a VLAN by executing the following command.

Command	Function
DES-7200(config)**# no vlan** *vlan-id*	Enter the VLAN ID that you want to delete.

5.2.5 Adding Existing Access Ports to Specified VLAN

If you assign a port to an inexistent VLAN, the switch will automatically create that VLAN.

In the privileged mode, you can assign a port to a VLAN by executing the following command.

Command	Function
DES-7200(config-if)**# switchport mode access**	Define the member type of the port in a VLAN (L2 ACCESS port).
DES-7200(config-if)**# switchport access vlan** *vlan-id*	Assign the port to the VLAN.

The following example adds Ethernet 1/10 to VLAN20 as an access port:

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 1/10
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport access vlan 20
DES-7200(config-if)# end
```

The following example shows how to verify the configuration:

```
DES-7200(config)#show interfaces gigabitEthernet 3/1
 switchport
Switchport is enabled
Mode is access port
Acsess vlan is 1,Native vlan is 1
Protected is disabled
Vlan lists is ALL
```

5.2.6 Adding Access Ports to the Existing VLAN

In VLAN configuration mode, add the specified Access port to this VLAN. The effect of this command is the same as the command to specify the VLAN to which the interface belongs in interface configuration mode (namely **switchport access vlan** *vlan-id*).

Command	Function
DES-7200(config)# **vlan** *vlan-id*	Type in a VLAN ID. If a new VLAN ID is typed in, the device will create a VLAN. If an existing VLAN ID is typed in, the corresponding VLAN will be modified.
DES-7200(config-vlan)# **add interface** { *interface-id* | **range** *interface-range* }	Add one or a group of Access ports to the existing VLAN. By default, all layer-2 Ethernet ports belong to VLAN1.
DES-7200(config-vlan)# [**no**]**add interface** { *interface-id* | **range** *interface-range* }	Delete one or a group of Access ports form the existing VLAN.
DES-7200(config-vlan)#**show interface** *interface-id* **switchport**	Display the information about layer-2 interface.

Caution

- This command only applies to Access port.
- In terms of these two commands to add interface to the VLAN, the later configured command will override the previously configured command.

The following example adds Access port (GigabitEthernet 0/10) to VLAN20:

```
DES-7200# configure terminal
SwitchA(config)#vlan 20
SwitchA(config-vlan)#add interface GigabitEthernet 0/10
```

The following example how to verify the configurations:

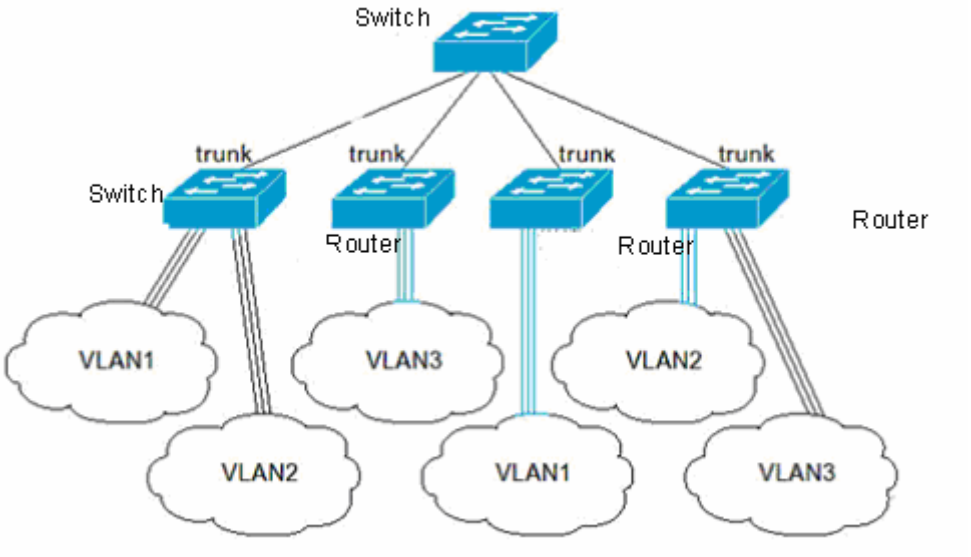
```
DES-7200# show interface GigabitEthernet 0/10 switchport
Interface        Switchport   Mode  Access Native Protected  VLAN lists
----------       --------     -----  ----- ------ ---------- -------
GigabitEthernet 0/10 enabled  ACCESS  20     1   Disabled   ALL
```

5.3 Configuring VLAN Trunks

5.3.1 Overview

A trunk is a point-to-point link that connects one or multiple Ethernet switching interfaces to other network devices (for instance, router or switch). A trunk can transmit the traffics of multiple VLANs.

The Trunk encapsulation of DES-7200 device is 802.1Q-complied. The following diagram shows a network connected with trunks.



You can set a common Ethernet port or aggregate port to be a trunk port. For the details of aggregate port, refer to *Configuring Aggregate Port*.

In order to switch an interface between the access mode and the trunk mode, use the **switchport mode** command:

Command	Function
DES-7200(config-if)# **switchport mode access**	Set an interface to the access mode
DES-7200(config-if)# **switchport mode trunk**	Set an interface to the Trunk mode

A native VLAN must be defined for a trunk port. The untagged packets received and sent through the port are deemed as the packets of the native VLAN. Obviously, the default VLAN ID of the port (that is, the PVID in the IEEE 802.1Q) is the VLAN ID of the native VLAN. Moreover, you must untag them before

sending the packets of the native VLAN through the trunk port. The default native VLAN of a trunk port is VLAN 1.

When you configure a trunk link, be sure that the ports on both ends of the trunk belong to the same native VLAN.

5.3.2 Configuring a Trunk Port

5.3.2.1 Basic Trunk Port Configuration

In the privileged mode, you can configure a trunk port by executing the following command.

Command	Function
DES-7200(config-if)# **switchport mode trunk**	Configure the port as a L2 trunk port.
DES-7200(config-if)# **switchport trunk native vlan** *vlan-id*	Specify a native VLAN for the port.

To restore all the trunk-related settings of a trunk port to their defaults, use the **no switchport mode** command in the interface configuration mode.

5.3.3 Defining the Allowed VLAN List of a Trunk Port

By default, the traffic of all VLANs in the range of 1 to 4094 can be transmitted over a trunk port. However, you can restrict the traffic of some VLANs from passing the trunk port by setting its allowed VLAN list.

In the priviledged mode, you can modify the allowed VLAN list of a trunk port by executing the following command.

Command	Function

Command	Function
DES-7200(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	(Optional) Configure the allowed VLAN list of the trunk port. The *vlan-list* parameter may be a VLAN or a series of VLANs. It starts with a small VLAN ID and ends with a large VLAN ID. Both IDs are connected with "-", such as 10–20. **All:** Add all the allowed VLANs to the allowed VLAN list; **add**: Add the specified VLAN list to the allowed VLAN list; **remove:** Remove the specified VLAN list from the allowed VLAN list; **except**: Add all the VLANs other than the specified VLAN list to the allowed VLAN list.

To restore the allowed VLAN list of the trunk port to its default, execute the **no switchport trunk allowed vlan** command in the interface configuration mode.

The following example removes VLAN 2 from the allowed VLAN list of port 1/15:

```
DES-7200(config)# interface fastethernet 1/15
DES-7200(config-if)# switchport trunk allowed vlan remove 2
DES-7200(config-if)# end
DES-7200# show interfaces fastethernet 1/15 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
--------- ---------- ----  ------ ------ -------- ----------
Gi0/15    enabled    TRUNK  1     1      Disabled   1,3—4094
```

5.3.4 Configuring a Native VLAN.

Tagged or untagged 802.1Q frames can be received or sent on a trunk port. Untagged frames are used to transmit the traffic of the native VLAN. By default, the native VLAN is VLAN 1.

In the privileged mode, you can configure a native VLAN for a trunk port by executing the following command.

Command	Function
DES-7200(config-if)# **switchport trunk native vlan** *vlan-id*	Configure a native VLAN.

To restore the native VLAN of a trunk port to its default, execute the **no switchport trunk native vlan** command in the interface configuration command.

If a frame carries the VLAN ID of the native VLAN, it will be automatically untagged when being forwarded through the trunk port.

When you set the native VLAN of a trunk port to an inexistent VLAN, the switch will not automatically create the VLAN. In addition, the native VLAN of a trunk port may be out the allowed VLAN list. In this case, the traffic of the native VLAN cannot pass the trunk port.

5.4 Showing VLAN Information

Only in the privileged mode can you view the VLAN information, including VLAN VID, VLAN status, member ports of the VLAN, and VLAN configuration. The related commands are listed as below:

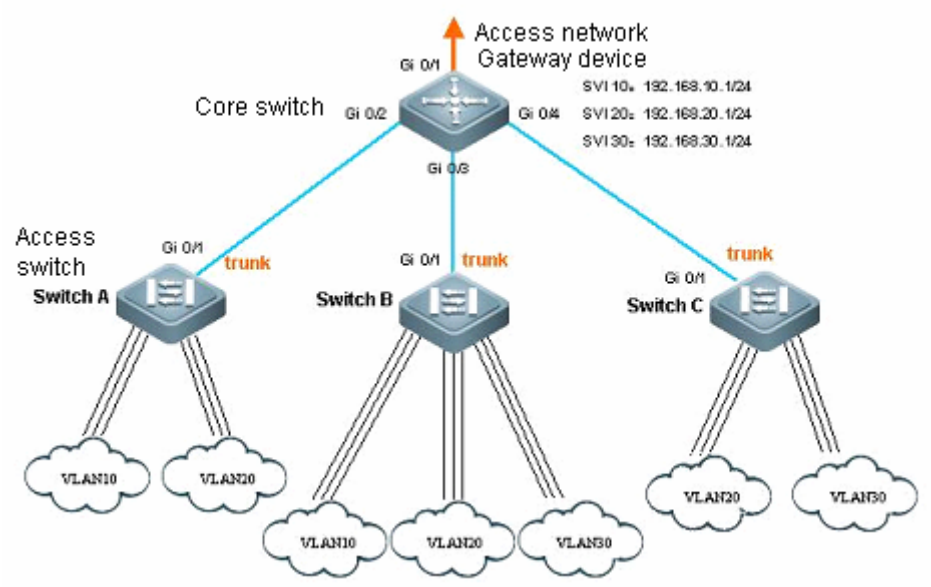
Command	Function
show vlan [**id** *vlan-id*]	Show the information about all or the specified VLAN.

The following example shows the information about a VLAN:

```
DES-7200# show vlan
VLAN  Name      Status             Ports
---- --------  --------   -------------------------------
   1 VLAN0001   STATIC    Gi0/1, Gi0/5, Gi0/6, Gi0/7
                          Gi0/8, Gi0/9, Gi0/10, Gi0/11
                          Gi0/12, Gi0/13, Gi0/14, Gi0/15
                          Gi0/16, Gi0/17, Gi0/18, Gi0/19
                          Gi0/20, Gi0/21, Gi0/22, Gi0/23
                          Gi0/24
  10 VLAN0010  STATIC    Gi0/2, Gi0/3
  20 VLAN0020  STATIC    Gi0/2, Gi0/3, Gi0/4
30 VLAN0030  STATIC    Gi0/3, Gi0/4

DES-7200#show vlan id 20
VLAN  Name              Status    Ports
----  --------          ------    -----------------------
20  VLAN0020          STATIC    Gi0/2, Gi0/3, Gi0/4
```

5.5 Configuration Examples

5.5.1 Network Topology



5.5.2 Networking Requirements

As shown above, an Intranet is divided into VLAN 10, VLAN 20 and VLAN 30 in order to realize laye-2 isolation. The IP subnets corresponding to three VLANs are 192.168.10.0/24, 192.168.20.0/24 and 192.168.30.0/24. The three VLANs are interconnected through the IP forwarding capacity of layer-3 core switch.

5.5.3 Configuration Tips

This example shows to how to configure the core switch and one of the access switches:

- Configure three VLANs on the core switch; configure the port connecting access switch to trunk port and specify the allowed vlan list to realize layer-2 isolation;
- Configure three SVI interfaces on the core switch to serve as the gateway interfaces for IP subnets corresponding to the three VLANs; configure the corresponding IP addresses;
- Create VLANs on three access switches and assign Access port for each VLAN; specify the trunk port for connecting core switch. This example shows the configuration steps on the access switch of Switch A.

5.5.4 Configuration Steps

5.5.4.1 Configurations on Core Switch

- **Create VLAN**

Enter the global configuration mode

```
DES-7200#configure terminal
```

Create VLAN 10

```
DES-7200(config)#vlan 10
```

Create VLAN 20

```
DES-7200(config-vlan)#vlan 20
```

Create VLAN 30

```
DES-7200(config-vlan)#vlan 30
```

Return to the global configuration mode

```
DES-7200(config-vlan)#exit
```

- **Configure respective trunk ports and specify the allowed vlan list**

Enter the interface range of Gi 0/2-4

```
DES-7200(config)#interface range GigabitEthernet 0/2-4
```

Configure Gi 0/2-4 as trunk ports

```
DES-7200(config-if-range)#switchport mode trunk
```

Return to the global configuration mode

```
DES-7200(config-if-range)#exit
```

Enter port Gi 0/2

```
DES-7200(config)#interface GigabitEthernet 0/2
```

Delete all vlans from the allowed vlan list of this port

```
DES-7200(config-if)#switchport trunk allowed vlan remove 1-4094
```

Add vlan 10 and vlan 20 into the allowed vlan list of this port

```
DES-7200(config-if)#switchport trunk allowed vlan add 10,20
```

Enter port Gi 0/3

```
DES-7200(config-if)#interface GigabitEthernet 0/3
```

Delete all vlans from the allowed vlan list of this port

```
DES-7200(config-if)#switchport trunk allowed vlan remove 1-4094
```

Add vlan 10, vlan 20 and vlan 30 into the allowed vlan list of this port

```
DES-7200(config-if)#switchport trunk allowed vlan add 10,20,30
```

Enter port Gi 0/4

```
DES-7200(config-if)#interface GigabitEthernet 0/4
```

Delete all vlans from the allowed vlan list of this port

```
DES-7200(config-if)#switchport trunk allowed vlan remove 1-4094
```

Add vlan 20 and vlan 30 into the allowed vlan list of this port

```
DES-7200(config-if)#switchport trunk allowed vlan add 20,30
```

Return to the global configuration mode

```
DES-7200(config-if)#exit
```

- **Display vlan configurations on core switch**

Display vlan information, including vlan id, name, state and member ports

```
DES-7200#show vlan
VLAN  Name      Status              Ports
---- --------  --------   -------------------------------
   1 VLAN0001   STATIC    Gi0/1, Gi0/5, Gi0/6, Gi0/7
                          Gi0/8, Gi0/9, Gi0/10, Gi0/11
                          Gi0/12, Gi0/13, Gi0/14, Gi0/15
                          Gi0/16, Gi0/17, Gi0/18, Gi0/19
                          Gi0/20, Gi0/21, Gi0/22, Gi0/23
                          Gi0/24
  10 VLAN0010  STATIC     Gi0/2, Gi0/3
  20 VLAN0020  STATIC     Gi0/2, Gi0/3, Gi0/4
  30 VLAN0030  STATIC     Gi0/3, Gi0/4
```

Display the vlan state of port Gi 0/2

```
DES-7200#show interface GigabitEthernet 0/2 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
-------- ---------- -----  ------ ------ --------- ---------
Gi0/2     enabled   TRUNK    1      1     Disabled  10,20
```

Display the vlan state of port Gi 0/3

```
DES-7200#show interface GigabitEthernet 0/3 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
-------- ---------- -----  ------ ------ --------- ----------
Gi0/3     enabled   TRUNK    1      1     Disabled  10,20,30
```

Display the vlan state of port Gi 0/4

```
DES-7200#show interface GigabitEthernet 0/4 switchport
Interface Switchport Mode  Access Native Protected VLAN lists
-------- ---------- -----  ------ ------ --------- ----------
Gi0/4     enabled   TRUNK    1      1     Disabled  20,30
```

- **Create SVI port and specify the IP address**

Enter the global configuration mode

```
DES-7200#configure terminal
```

Create SVI 10

```
DES-7200(config)#interface vlan 10
```

Configure the IP address of SVI 10

```
DES-7200(config-if)#ip address 192.168.10.1 255.255.255.0
```

Create SVI 20

```
DES-7200(config-if)#interface vlan 20
```

Configure the IP address of SVI 20

```
DES-7200(config-if)#ip address 192.168.20.1 255.255.255.0
```

Create SVI 30

```
DES-7200(config-if)#interface vlan 30
```

Configure the IP address of SVI 30

```
DES-7200(config-if)#ip address 192.168.30.1 255.255.255.0
```

Return to the global configuration mode

```
DES-7200(config-if)#exit
```

5.5.4.2 Configurations on the Access Switch of Switch A

- **Create VLAN**

Enter the global configuration mode

```
DES-7200#configure terminal
```

Create VLAN 10

```
DES-7200(config)#vlan 10
```

Create VLAN 20

```
DES-7200(config-vlan)#vlan 20
```

Return to the global configuration mode

```
DES-7200(config-vlan)#exit
```

- **Assign Access port for each VLAN**

Enter the interface range of Gi 0/2-12

```
DES-7200(config)#interface range GigabitEthernet 0/2-12
```

Configure Gi 0/2-12 as Access ports

```
DES-7200(config-if)#switchport mode access
```

Add Gi 0/2-12 to VLAN 10

```
DES-7200(config-if)#switchport access vlan 10
```

Enter the interface range of Gi 0/13-24

```
DES-7200(config-if)#interface range GigabitEthernet 0/13-24
```

Configure Gi 0/13-24 as Access ports

```
DES-7200(config-if)#switchport mode access
```

Add Gi 0/13-24 to VLAN 20

```
DES-7200(config-if)#switchport access vlan 20
```

Return to the global configuration mode

```
DES-7200(config-if)#exit
```

- **Specify the trunk port for connecting core switch**

Enter port Gi 0/1

```
DES-7200(config)#interface GigabitEthernet 0/1
```

Configure Gi 0/1 as trunk port

```
DES-7200(config-if)#switchport mode trunk
```

Return to global configuration mode

```
DES-7200(config-if)#exit
```

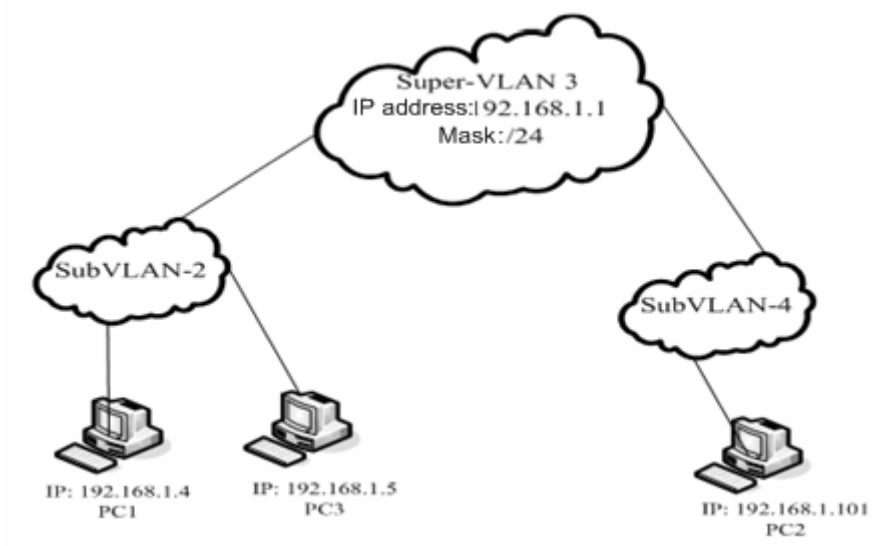
6 Super VLAN Configuration

This chapter describes the Super VLAN configuration of DES-7200 devices.

6.1 Overview

Super VLAN is a method for VLAN division. Super VLAN, also called VLAN aggregation, is a management technology for optimizing IP addresses. Its principle is to assign the IP address of a network segment to different sub VLANs that belong to the same super VLAN. Each sub VLAN is an independent broadcast domain and isolated on the layer 2. Users in a sub VLAN use the IP address of a virtual interface of the super VLAN as the gateway for communication on the layer 3, which allows multiple VLANs to share one IP address and saves IP address resources. At the same time, the ARP proxy function is required to realize layer 3 interoperation between sub VLANs, as well as interoperation between sub VLANs and other networks. The ARP proxy can forward and handle the ARP request and response packets to realize layer 3 interoperation between the isolated layer 2 ports of sub VLANs. By default, the ARP proxy function is enabled for super VLAN and sub VLAN.

Super VLAN not only save lots of IP addresses,but also is convenient for the network management. You only need to assign an IP address to a super VLAN including multiple sub VLANs.



The following presents the communication procedure between two aggregated sub VLANs.

As shown in the above diagram, Sub VLAN2 and Sub VLAN4 are aggregated to form Super VLAN3. An IP address is assigned to Super VLAN3, and both Sub VLAN2 and Sub VLAN4 are located in this subnet. Supposing PC1 in Sub VLAN2 wants to communicate with PC2 in the subnet, after knowing that the peer is located in the same network segment, PC1 directly sends an ARP request packet with a destination IP address. Upon receiving this ARP request packet, the layer 3 device directly broadcasts this packet through layer 2 within Sub VLAN2, and sends a copy to the ARP module of the device. This module first checks whether the destination IP address in the ARP request packet is in Sub-VLAN2. If so, it will discard this packet because it and PC1 are located in the same broadcast domain, and the destination host will directly respond to PC1. If not, it will respond PC1 with the MAC address of SuperVLAN3, acting as an ARP agent. For example, PC1 and PC2 have to communicate through the ARP agent which forwards packets from PC1 to PC2. However, PC1 and PC3 can communicate directly without a forwarding device.

Restrictions:

- A super VLAN can only contain sub VLANs. The sub VLAN contains actual physical ports.
- A super VLAN cannot serve as a sub VLAN of other Super VLANs.
- A super VLAN cannot be used as the normal 1Q VLAN.
- VLAN 1 cannot be used as a super VLAN.
- A sub VLAN cannot be configured as a network interface, and cannot be assigned with an IP address.
- Super VLAN does not support VRRP, IGMP Snooping and PIM Snooping.

- Super VLAN interface-based ACL and QOS configurations take no effect for sub VLANs.

6.2 Configuring a Super VLAN

To configure a super VLAN, execute the following commands.

Command	Function
DES-7200# **configure**	Enter the global configuration mode.
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode
DES-7200(config-vlan)# **supervlan**	Enable the Super VLAN function
DES-7200(config-vlan)# **end**	Return to the privileged mode.

The super VLAN function is disabled by default. The enabled super VLAN function can be disabled by using the **no supervlan** command.

6.3 Configuring the Sub VLANs of a Super VLAN

A super VLAN is meaningful only when subVLANs are configured.

To configure a VLAN as the sub VLAN of a super VLAN, execute the following command.

Caution

The SubVLAN configuration may fail due to a lack of resources.

Command	Function
DES-7200# **configure**	Enter the global configuration mode
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode
DES-7200(config-vlan)# **supervlan**	Set this VLAN as a super VLAN
DES-7200(config-vlan)# **subvlan** *vlan-id-list*	Specify several sub VLANs and add them to the super VLAN.
DES-7200(config-vlan)# **exit**	Return to the global mode.

To delete a sub VLAN from the super VLAN, execute the **no subvlan** [*vlan-id-list*] command.

Caution

If you want to delete SubVLAN, you must switch it to ordinary VLAN and then use command **no vlan.**

6.4 Setting an Address Range for a Sub VLAN

You can configure an address range for each sub VLAN so that the device can idetnify which sub VLAN that a given IP address belongs to. The address ranges configured for sub VLANs of the super VLAN should not be overlapped or covered each other.

To set an address range for a sub VLAN, execute the following command in the global configuration mode:

Command	Function
DES-7200# **configure**	Enter the global configuration mode
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode
DES-7200(config-vlan)# **subvlan-address-range** *start-ip end-ip*	Set an address range for the sub VLAN. start-ip is the start IP address of this sub VLAN, and end-ip is the end IP address of this sub VLAN.
DES-7200(config-vlan)# **end**	Return to the privileged mode.
DES-7200# **show run**	Verify the configuration.

Note

You can delete previous configurations by using command **no subvlan-address-range**.

6.5 Setting a Virtual Interface for a Super VLAN

When a user in a sub VLAN needs to perform layer 3 communication, a virtual layer 3 interface of the super VLAN should be created first.

The SVI of the super VLAN itself is used as the virtual interface.

To set a virtual interface for a supre VLAN, execute the following commands in the global configuration mode.

Command	Function
DES-7200# **configure**	Enter the global configuration mode.
DES-7200(config)# **interface vlan** *vlan-id*	Enter the SVI mode.
DES-7200(config-vlan)# **ip address** *ip mask*	Set an IP address for the virtual interface.
DES-7200(config-vlan)# **end**	Return to the privileged mode.
DES-7200# **show run**	Verify the configuration.

6.6 Setting ARP Proxy for a VLAN

You can set ARP Proxy for a VLAN so that sub VLANs can communciate with each other.

ARP Proxy is enabled for a VLAN by default.

To set ARP Proxy for a VLAN, execute the following command in the global configuration mode:

Command	Function
DES-7200# **configure**	Enter the global configuration mode.
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN mode.
DES-7200(config-vlan)# **proxy-arp**	Enable ARP Proxy function for the VLAN.
DES-7200(config-vlan)# **end**	Return to the privileged mode.
DES-7200# **show run**	Verify the configuration.

To disable ARP Proxy for a VLAN, execute the **no proxy-arp** command.

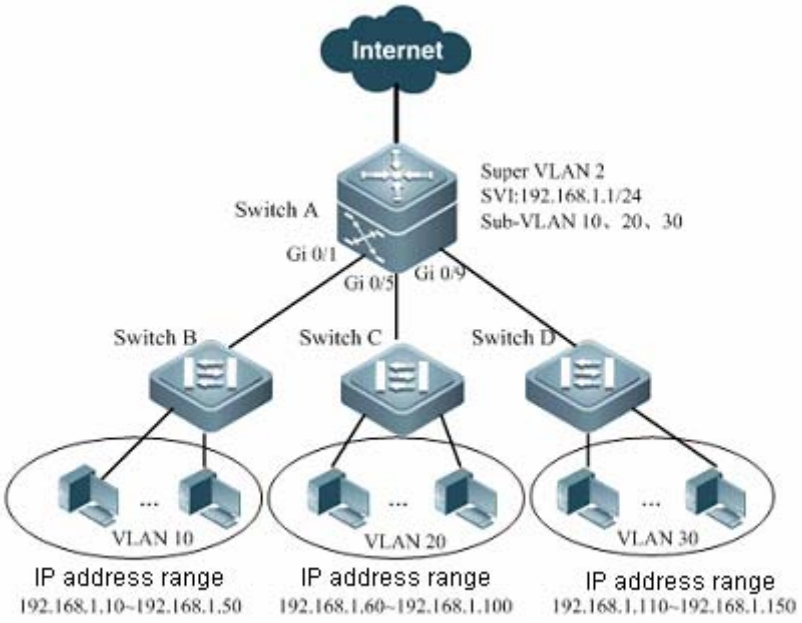
6.7 Showing Super VLAN Setting

To show the super VLAN setting, execute the following command.

Command	Function
DES-7200# **show supervlan**	Show the super VLAN setting.

6.8 Typical Super Configuration Example

6.8.1 Network Topology



Super VLAN application topology

6.8.2 Application Requirements

As shown above, Switch A is the convergence device connecting with access devices of Switch B, Switch C and Switch D on the Trunk ports.

Application requirements include:

- Layer-2 isolation of access users can be achieved through VLAN division.
- Users belonging to different VLANs share a same IP gateway, allowing layer-3 communication and communication with Internet.

6.8.3 Configuration tips

1. Achieve layer-2 isolation on access switches (Switch B, Switch C and Switch D) through VLAN division (VLAN 10, VLAN 20 and VLAN 30).
2. Configure Super VLAN (VLAN 2) on the convergence device (Switch A), and configure the VLANs (VLAN 10, VLAN 20 and VLAN 30) to Sub-VLANs on the access device.
3. Configure SVI (192.168.1.1/24) for Super VLAN, and assign IP address ranges for respective Sub-VLANs (as shown above).

6.8.4 Configuration Steps

The following configurations are performed on Switch A; VLAN divisions on Switch B, Switch C and Switch D won't be further described.

- **Configure Switch A**

Step 1: Enter the global configuration mode and create VLAN 2, VLAN 10, VLAN 20 and VLAN 30.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan 2
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 10
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 20
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 30
DES-7200(config-vlan)#exit
```

Step 2: Configure VLAN 2 as the Super VLAN; the corresponding Sub-VLANs are VLAN 10, VLAN 20 and VLAN 30.

```
DES-7200(config)#vlan 2
DES-7200(config-vlan)#supervlan
DES-7200(config-vlan)#subvlan 10,20,30
DES-7200(config-vlan)#exit
```

Step 3: Configure the corresponding layer-3 virtual interface for Super VLAN 2, and users belonging to Sub-VLANs associated to Super VLAN 2 will achieve layer-3 communication through this interface.

```
DES-7200(config)#interface vlan 2
DES-7200(config-if-VLAN 2)#ip address 192.168.196.1 255.255.255.0
```

Step 4: Configure the IP address range of 192.168.196.10-192.168.196.50 for Sub-VLAN 10, 192.168.196.60-192.168.196.100 for Sub-VLAN 20, and 192.168.196.110-192.168.196.150 for Sub-VLAN 30.

```
DES-7200(config)#vlan 10
DES-7200(config-vlan)#subvlan-address-range 192.168.196.10 192.168.196.50
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 20
DES-7200(config-vlan)#subvlan-address-range 192.168.196.60 192.168.196.100
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 30
DES-7200(config-vlan)#subvlan-address-range 192.168.196.110
192.168.196.150
```

Step 5: Configure Gi 0/1, Gi 0/5 and Gi 0/9 as Trunk ports for connecting Switch B, Switch C and Switch D.

```
DES-7200(config)#interface range gigabitEthernet 0/1,0/5,0/9
DES-7200(config-if-range)#switchport mode trunk
```

6.8.5 Verification

Step 1: Display configurations of Switch A. Key points: mapping relation between Super VLAN and Sub-VLAN, IP address range of Sub-VLAN, and the gateway address of Super VLAN.

```
DES-7200#show running-config
!
vlan 1
!
vlan 2
 supervlan
 subvlan 10,20,30
!
vlan 10
 subvlan-address-range 192.168.196.10 192.168.196.50
!
vlan 20
 subvlan-address-range 192.168.196.60 192.168.196.100
!
vlan 30
 subvlan-address-range 192.168.196.110 192.168.196.150
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/5
 switchport mode trunk
!
interface GigabitEthernet 0/9
 switchport mode trunk
```

```
!
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.196.1 255.255.255.0
!
```

Step 2: Display configurations of Super VLAN, as shown below: By default, ARP proxy is enabled in Super VLAN and Sub-VLANs.

```
DES-7200(config-if-range)# show supervlan
supervlan id  supervlan arp-proxy  subvlan id  subvlan arp-proxy  subvlan ip
range
------------  ------------------  -------------------------
2      ON       10      ON     192.168.196.10 - 192.168.196.50
                20      ON     192.168.196.60 - 192.168.196.100
                30      ON    192.168.196.110 - 192.168.196.150
```

7 Protocol VLAN Configuration

7.1 Protocol VLAN Technology

Every packet received on a port of the device should be classified and added to an unique VLAN. There are three possibilities:

1. If the packet has no VLAN ID (for instance, UNTAG or Priority packet), and the device only supports port-based VLAN classification, the VLAN ID in the tag added to the packet is the PVID of the inbound port.

2. If the packet has no VLAN ID (for instance, UNTAG or Priority packet), and the device supports protocol type-based VLAN classification, one of the VLAN IDs corresponding to the protocol suite configured on the inboud port will be selected as the VLAN ID in the tag added to the packet. However, if the protocol type of the packet matches none of the protocol suite configured on the inbound port, the VLAN ID will be assigned by port-based VLAN classification.

3. If the packet is tagged, its VLAN is determined by the VLAN ID in the tag.

As a protocol type-based VLAN classification technology, the protocol VLAN classifies the packets that have no VLAN ID and be of the same protocol type to the same VLAN.

The protocol VLAN configuration takes effect for Trunk port and Hybrid port, not for the Access port.

DES-7200 products support both global IP address-based VLAN classification, and packet type and Ethernet type-based VLAN classification on a port.

Because IP address-based VLAN classification is a global configuration, once configured, it will apply to all trunk ports and Hybrid ports.

1. If the incoming packet has no VLAN ID, and its IP address matches the configured IP address, this packet will be classify into the configured VLAN.

2. If the incoming packet has no VLAN ID, and its packet type and Ethernet type match those you configured on the inbound port respectively, this packet will be classified into the configured VLAN.

IP address-based VLAN classification takes precedence over packet type and Ethernet type-based VLAN classification. Hence, if you have configured both IP address-based VLAN classification and packet type and Ethernet type-based VLAN classification, and the incoming packet matches them both, IP address-based VLAN classification takes effect.

You should configure a VLAN, trunk port, hybrid port, access port and AP attributes before configuring the protocol VLAN. If you have configured protocol VLAN on a trunk port or a hybrid port, the allowed VLAN list for the trunk port and hybrid port must include all the VLANs related to the protocol VLAN.

7.2 Configuring a Protocol VLAN

7.2.1 Default Protocol VLAN

No Protocol VLAN is configured by default.

7.2.2 Configuring IP Address-based VLAN Classification

To configure IP address-based VLAN classification, execute the following commands:

Command	Description
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **protocol-vlan ipv4** *address* **mask** *address* **vlan** *vid*	Configure IP address, subnet mask and VLAN classification.
DES-7200(config)# **no protocol-vlan ipv4** *address* **mask** *address*	Remove the IP address configuration.
DES-7200(config)# **no protocol-vlan ipv4**	Remove all IP address configuration.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)#**protocol vlan ipv 4**	Enable the IP address-based VLAN classification on the interface.
DES-7200(config-if)#**no protocol vlan ipv4**	Disable the IP address-based VLAN classification on the interface.

Command	Description
DES-7200(config-vlan)**# show protocol-vlan ipv4**	Show the configured IP address

Note

Specify the IP address and subnet mask in the x.x.x.x format. Available VLAN IDs may vary with different products.

The following command configures the IP address of 192.168.100.3, and the mask of 255.255.255.0 VLAN 100.

```
DES-7200# configure terminal
DES-7200(config)# protocol-vlan ipv4 192.168.100.3 mask 255. 255.255.0 vlan
100
DES-7200(config-vlan)# end
DES-7200# show protocol-vlan ipv4
ip              mask            vlan
-------------  -------------   -----

192.168.100.3   255.255.255.0   100
```

7.2.3 Configuring Packet Type and Ethernet Type Profile

To configure the packet type and Ethernet type profile, execute the following commands:

Command	Description
DES-7200**# configure terminal**	Enter the global configuration mode.
DES-7200(config)**# protocol-vlan profile** *id* **frame-type** [*type*] **ether-type** [*type*]	Configure packet type and Ethernet type profile.
DES-7200(config)**# no protocol-vlan profile** *id*	Delete an profile.
DES-7200(config)**# no protocol-vlan profile**	Clear all profiles.
DES-7200(config-vlan)**# show protocol-vlan profile** [*id*]	Exit the VLAN mode
DES-7200**# configure terminal**	Show all profiles.
DES-7200(config)**# protocol-vlan profile** *id* **frame-type** [*type*] **ether-type** [*type*]	Show a profile.

For example:

```
DES-7200# configure terminal
DES-7200(config)# protocol-vlan  profile 1 frame-type  ETHERII ether-type
EHTER_AARP
DES-7200(config)# protocol-vlan  profile 2 frame-type  SNAP ether-type
0x809b
DES-7200(config-vlan)# end
DES-7200# show protocol-vlan profile
profile    frame-type    ether-type      Interfaces|vid
-------     ---------   ----------        -----------
1           ETHERII     EHTER_AARP       NULL|NULL
2           SNAP         ETHER_APPLETALK  NULL|NULL
```

Note

1) The configuration will not become effective until the profile is applied to a port.
2) Before updating a profile, you must delete the profile and then reconfigure it.

7.2.4 Applying a Profile

To apply a profile, execute the following commands:

Command	Description
DES-7200**# configure terminal**	Enter the global configuration mode.
DES-7200(config)**# interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)**# protocol-vlan profile** *id* **vlan** *vid*	Apply a profile to this port.
DES-7200(config-if)**# no protocol-vlan profile** *id*	Clear all profiles on this port .
DES-7200(config-if)**# no protocol-vlan profile**	Clear a profile on this port
DES-7200(config-if)**# show protocol-vlan profile**	Show the profile configuration.

The following example applies profile 1 and profile 2 to the GE interface 1 of Slot 3. The VLAN categories are VLAN 101 and 102:

```
DES-7200# configure terminal
DES-7200(config)# interface gi 3/1
DES-7200(config-if)# protocol-vlan profile 1 vlan 101
DES-7200(config-if)# protocol-vlan profile 2 vlan 102
```

```
DES-7200(config-if)# end
DES-7200# show protocol-vlan profile
profile     frame-type  ether-type      Interfaces|vid
-------     ---------   ----------       -------------
1           ETHERII     EHTER_AARP       gi3/1|101
2           SNAP         ETHER_APPLETALK  gi3/1|102
```

Note

1. All profiles can be applied to each interface.
2. Different VIDs can be specified for the same profile on different interfaces.
3. DES-7200 series support 4094 VLANs.

7.3 Showing a Protocol VLAN

To show a protocol VLAN, execute the following command:

Command	Description
DES-7200# **show protocol-vlan**	Show a protocol VLAN.

```
DES-7200# show protocol-vlan
ip              mask            vlan
-------------   -------------   ----
192.168.100.3   255.255.255.0   100
profile     frame-type   ether-type      Interfaces|vid
-------     ---------    ----------      -------------
1           ETHERII     EHTER_AARP       gi3/1|101
2           SNAP         ETHER_APPLETALK  gi3/1|1
```

7.4 Typical Protocol VLAN Configuration Examples

7.4.1 Example of protocol-based VLAN configuration

7.4.1.1 Network Topology

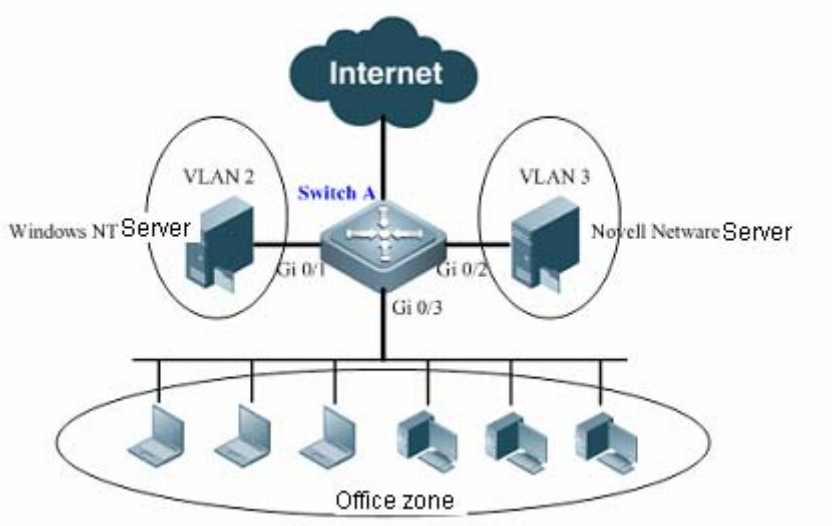


Diagram for protocol-based VLAN configuration

7.4.1.2 Application Requirements

The above figure shows the structure of a Windows NT and Novell Netware interconnected network. The office zone is connected to the layer-3 device of Switch A through Hub. There are different PC users distributed in the office zone, with certain users using Windows NT operating system and supporting IP protocol and other users using Novell Netware operating system and supporting IPX protocol. The entire office zone is connected to Internet and server via the uplink port of Gi 0/3.

Networking requirement:

- Implement layer-2 isolation between Windows NT users and Novell Netware users in order to lessen network traffic.

7.4.1.3 Configuration Tips

Configuration tips:

1. Configure packet type and Ethernet type profiles (in this example, IP packets correspond to Profile 1, and IPX packets correspond to Profile 2).
2. Apply the profile to the uplink port (Gi 0/3) and associate with the VLAN (in this example, associate Profile 1 with VLAN 2 and Profile 2 with VLAN 3).

Notes:

1. Protocol-based VLAN can only apply to Trunk port and Hybrid port, which can directly connect with Hub or user PCs.
2. PC user can determine its IP network segment according to the protocol-based VLAN (network segment configuration for each VLAN won't be described herein).

7.4.1.4 Configuration Steps

Configure Switch A

Step 1: Enter global configuration mode and create VLAN 2 and VLAN 3.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan range 2,3
DES-7200(config-vlan-range)#exit
```

Step 2: Since Windows NT server and Novell Netware server are directly connected with Gi 0/1 and Gi 0/2, we can configure port-based VLANs.

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-GigabitEthernet 0/1)#switchport access vlan 2
DES-7200(config-GigabitEthernet 0/1)#exit
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-GigabitEthernet 0/2)#switchport access vlan 3
DES-7200(config-GigabitEthernet 0/2)#exit
```

Step 3: Configure uplink port Gi 0/3 as a Trunk port.

```
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-GigabitEthernet 0/3)#switchport mode trunk
```

Step 4: Configure the corresponding Profile 1 and Profile 2 for IP protocol and IPX protocol respectively (assuming that Ethernet II encapsulation is used, the Ethernet types of IP and IPX are 0X0800 and 0X8137 respectively)

```
DES-7200(config)#protocol-vlan profile 1 frame-type eTHERII ether-type
0x0800
DES-7200(config)#protocol-vlan profile 2 frame-type eTHERII ether-type
0x8137
```

Step 5: Apply Profile 1 and Profile 2 to Gi 0/3 in order to classify VLAN 2 and VLAN 3. IP packets received on the port will belong to VLAN 2, and IPX packets received on the port will belong to VLAN 3.

```
DES-7200(config-GigabitEthernet 0/3)#protocol-vlan profile 1 vlan 2
DES-7200(config-GigabitEthernet 0/3)#protocol-vlan profile 2 vlan 3
DES-7200(config-GigabitEthernet 0/3)#exit
```

7.4.1.5 Verification

Step 1: Display configurations of Switch A. Key points: whether profiles have been properly configured for the Protocol VLAN, and whether the port applied with profiles has been properly configured.

```
DES-7200#show running-config
!
vlan 2
!
vlan 3
!
protocol-vlan profile 1 frame-type ETHERII ether-type 0x800
protocol-vlan profile 2 frame-type ETHERII ether-type 0x8137
!
interface GigabitEthernet 0/1
 switchport access vlan 2
!
interface GigabitEthernet 0/2
 switchport access vlan 3
!
interface GigabitEthernet 0/3
 switchport mode trunk
protocol-vlan profile 1 vlan 2
 protocol-vlan profile 2 vlan 3
!
```

Step 2: Display the type of protocol packets matched by profile and the corresponding port number and VLAN ID.

```
DES-7200#show protocol-vlan profile
profile frame-type ether-type/DSAP+SSAP interface   vlan
------- ---------- -------------------- --------------------
1      ETHERII    0x800                  Gi0/3        2
2      ETHERII    0x8137                 Gi0/3        3
```

7.4.2 Example of IP address based VLAN configuration

7.4.2.1 Network Topology

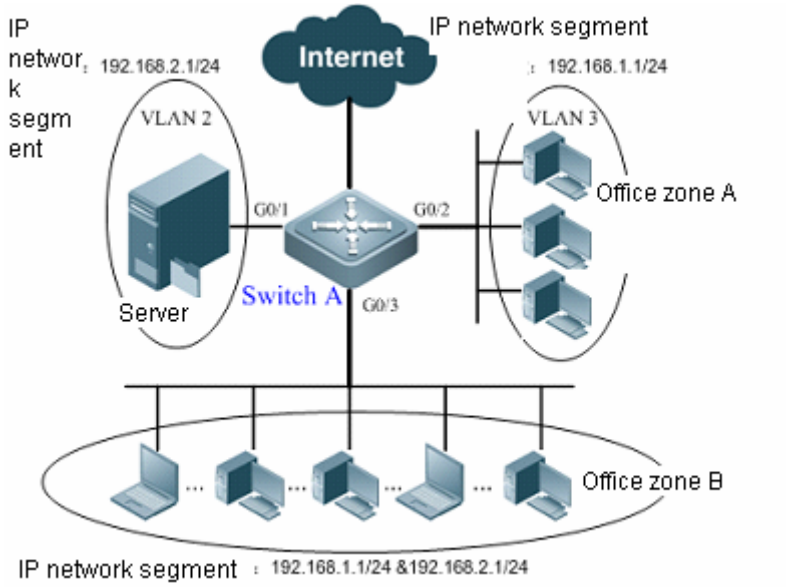


Diagram for IP address based VLAN configuration

7.4.2.2 Application Requirements

Office zone A and office zone B are connected to the elayer-3 device of Switch A through hubs. Office users falling within the fixed network segment are distributed in office zone A and belong to a port-based VLAN. Office zone B is distributed by office users falling within two different network segments, and port-based VLAN cannot be realized in this zone.

Networking requirements

- For PC users from office zone B, Switch A shall be able to determine their VLAN according to the IP network segment of packets.

7.4.2.3 Configuration Tips

Configuration tips:

Globally configure IP address based VLANs (in this example, IP network segment of 192.168.1.1/24 belongs to VLAN 3, and IP network segment of 192.168.2.1/24 belongs to VLAN 2), and enable IP address based VLAN on the uplink port (Gi 0/3).

Notes:

IP address based VLAN can only apply to Trunk port and Hybrid port, which can directly connect with Hub or user PCs.

7.4.2.4 Configuration Steps

Configure Switch A

Step 1: Enter global configuration mode and create VLAN 2 and VLAN 3.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan range 2-3
DES-7200(config-vlan-range)#exit
```

Step 2: Configure G0/3 as a Trunk port.

```
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-GigabitEthernet 0/3)#switchport mode trunk
DES-7200(config-GigabitEthernet 0/3)#exit
```

Step 3: Since the server is directly connected with port Gi 0/1, this port can be configured to belong to VLAN 2.

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-GigabitEthernet 0/1)#switchport access vlan 2
DES-7200(config-GigabitEthernet 0/1)#exit
```

Step 4: Configure port Gi 0/2 to belong to VLAN 3.

```
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-GigabitEthernet 0/2)#switchport access vlan 3
DES-7200(config-GigabitEthernet 0/2)#exit
```

Step 5: Associate IP network segment of 192.168.1.1/24 with VLAN 3 and IP network segment of 192.168.2.1/24 with VLAN 2.

```
DES-7200(config)#protocol-vlan ipv4 192.168.1.1 mask 255.255.255.0 vlan 3
DES-7200(config)#protocol-vlan ipv4 192.168.2.1 mask 255.255.255.0 vlan 2
```

Step 6: On port Gi 0/3, enable IP address based VLAN classification.

```
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-GigabitEthernet 0/3)# protocol-vlan ipv4
```

7.4.2.5 Verification

Step 1: Display configurations of Switch A. Key points: whether IP address based VLAN classification has been properly configured, and whether the uplink port has been configured as a Trunk port.

```
DES-7200#show running-config
!
```

```
vlan 1
!
vlan 2
!
vlan 3
!
protocol-vlan ipv4 192.168.1.1 mask 255.255.255.0 vlan 3
protocol-vlan ipv4 192.168.2.1 mask 255.255.255.0 vlan 2
!
interface GigabitEthernet 0/1
 switchport access vlan 2
!
interface GigabitEthernet 0/2
 switchport access vlan 3
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
```

Step 2: Display the policy configured for matching IP network segment and VLAN ID.

```
DES-7200#show protocol-vlan ipv4
ip               mask          vlan
---------------- --------------- ----
192.168.1.1    255.255.255.0    3
192.168.2.1    255.255.255.0    2
```

8 Private VLAN Configuration

8.1 Private VLAN Technology

If the service provider offers a VLAN to each subscriber, the service provider supports a limited number of subscribers because one device supports 4096 VLANs at most. On the layer 3 device, each VLAN is assigned with a subnet address or a series of addresses, which results in a waste of IP addresses. In this case, private VLAN comes into being.

A private VLAN divides the layer 2 broadcast domain of a VLAN into several sub domains. Each sub domain consists of a private VLAN pair: primary VLAN and secondary VLAN.

A private VLAN domain can have multiple private VLAN pairs, and each VLAN pair represents a sub domain. All the private VLAN pairs in one private VLAN domain share a primary VLAN. Each sub domain has a different secondary VLAN IDs.

There is only one primary VLAN in each private VLAN domain. The secondary VLAN is used for layer 2 separation in the same private VLAN domain. There are two types of secondary VLANs:

- Isolated VLAN: Layer 2 communication is not possible for the ports in the same isolated VLAN. There is only one isolated VLAN in a private VLAN domain.
- Community VLAN: The ports in the same community VLAN can perform layer 2 communication, but not with the ports in other community VLANs. There can be multiple community VLANs in a private VLAN domains.

Promiscuous port, a port in the primary VLAN, can communicate with any port, including the isolated port and community port of the secondary VLAN in the same private VLAN.

Isolated port, a port in the isolated VLAN, can only communicate with the promiscuous port. The packets received on the isolated port are allowed to be forwarded to the Trunk Port, but the packets in the isolated VLAN received on the Trunk Port cannot be forwarded to the isolated port.

Isolated Trunk Port, can be the member port of multiple ordinary VLANs and PVLANs. In the isolated VLAN, the isolated trunk port can only communicate with the promiscuous port; in the community VLAN, it can communicate with the community ports in the same community VLAN and the promiscuous port; in the ordinary VLAN, it follows the 802.1Q rule. The packets in the isolated VLAN received on the isolated trunk port are allowed to be forwarded to the Trunk Port, but the packets in the isolated VLAN received on the Trunk Port cannot be forwarded to the isolated port.

The VID for the tagged packet forwarded from the promiscuous port to the the isolated trunk port, is the VID for the secondary VLAN.

Community port, a port in the community VLAN, can communicate with other community ports in the same community VLAN as well as the promiscuous port in the primary VLAN. However, they cannot communicate with the community ports in other community VLANs and isolated ports in the isolated VLANs.

The following list shows the packet forwarding relationship between various port types:

Output Port / Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port (In the same VLAN)	Trunk Port (In the same VLAN)
Promiscuous port	√	√	√	√	√
Isolated Port	√	X	X	X	√
Community Port	√	X	√	√	√
Isolated Trunk Port (In the same VLAN)	√	X	√	X	√
Trunk Port (In the same VLAN)	√	X	√	X	√

The following list shows the whether the VLAN TAG changes or not after the packet forwarding between various port types:

Output Port / Input Port	Promiscuous Port	Isolated Port	Community Port	Isolated Trunk Port (In the same VLAN)	Trunk Port (In the same VLAN)
Promiscuous port	Unchanged	Unchanged	Unchanged	Add the secondary VLAN ID	Add the primary VLAN ID TAG
Isolated Port	Unchanged	N/A	N/A	N/A	Add the isolated VLAN ID TAG
Community Port	Unchanged	N/A	Unchanged	Add the community VLAN ID TAG	Add the community VLAN ID TAG
Isolated Trunk Port (In the same VLAN)	Remove the VLAN TAG	N/A	Remove the VLAN TAG	Unchanged in the non-isolated VLAN.	Unchanged
Trunk Port (In the same VLAN)	Remove the VLAN TAG	N/A	Remove the VLAN TAG	Change to the secondary VLAN ID in the primary VLAN; Unchanged in other non-isolated VLAN.	Unchanged
Switch CPU	Untag	Untag	Untag	Add the secondary VLAN ID TAG	Add the primary VLAN ID TAG

In a private VLAN, an SVI interface can be created for the primary VLAN rather than the secondary VLANs.

A port in the private VLAN can be a SPAN source port instead of a mirrored destination port.

8.2 Configuring a Private VLAN

8.2.1 Default Private VLAN Configuration

No Private VLAN is configured by default.

8.2.2 Configuring a VLAN as a Private VLAN

To configure a VLAN as a private VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
vlan *vid*	Enter the VLAN configuration mode.
private-vlan{community | isolated| primary}	Configure a private VLAN.
no private-vlan{community | isolated | primary}	Remove the configured private VLAN.
end	Exit the VLAN configuration mode.
show vlan private-vlan [*type*]	Show a private VLAN

Note

The member port in the 802.1Q VLAN cannot be declared as a private VLAN. VLAN 1 cannot be declared as a private VLAN as well. If there is a trunk or uplink port in the 802.1Q VLAN, first delete this VLAN from the allowed VLAN list. The following conditions must be met in order to make a private VLAN become active:

1. The primary VLAN is available.
2. The secondary VLANs are available.
3. The secondary VLANs are associated with the primary VLAN.

The following example configures 802.1Q VLAN as a private VLAN:

```
DES-7200# configure terminal
DES-7200(config)# vlan 303
DES-7200(config-vlan)# private-vlan community
```

```
DES-7200(config-vlan)# end
DES-7200# show vlan private-vlan community
VLAN Type  Status   Routed   Interface   Associated VLANs
--- ----   -------- ------   ---------   ------------------
303 comm   inactive Disabled             no association
DES-7200#configure terminal
DES-7200(config)#vlan 404
DES-7200(config-vlan)# private-vlan isolated
DES-7200(config-vlan)# end
DES-7200# show vlan private-vlan
VLAN Type  Status   Routed   Interface   Associated VLANs
--- ----   -------- ------   ---------   ------------------
303 comm  inactive  Disabled             no association
404 isol  inactive  Disabled             no association
```

8.2.3 Associating the Secondary VLANs with the Primary VLAN

To associate the secondary VLANs with the primary VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
vlan *p_vid*	Enter the primary VLAN configuration mode.
private-vlan association {svlist | add *svlist* **| remove** *svlist***}**	Associate with the secondary VLANs.
no private-vlan association	Remove the association with all the secondary VLANs.
end	Exit the VLAN mode.
show vlan private-vlan [*type***]**	Show the private VLAN

For example:

```
DES-7200# configure terminal
DES-7200(config)# vlan 202
DES-7200(config-vlan)# private-vlan association 303-307,309,440
DES-7200(config-vlan)# end
DES-7200# show vlan private-vlan
VLAN Type  Status   Routed   Interface   Associated VLANs
--- ----   -------- ------   ---------   ------------------
202 prim  inactive  Disabled             303-307,309,440
303 comm  inactive  Disabled             202
304 comm  inactive  Disabled             202
305 comm  inactive  Disabled             202
```

```
306 comm  inactive   Disabled            202
307 comm  inactive   Disabled            202
309 comm  inactive   Disabled            202
440 comm  inactive   Disabled            202
```

Note

This operation is performed in the configuration mode of the VLAN declared as the primary VLAN.

8.2.4 Mapping Secondary VLANs to the Layer 3 Interface of the Primary VLAN

To map the secondary VLANs to the layer 3 interface of the primary VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
interface vlan *p_vid*	Enter the interface configuration mode of the primary VLAN.
private-vlan mapping {svlist | add *svlist* **| remove** *svlist***}**	Map the secondary VLANs to the layer 3 SVI of the primary VLAN.
end	Exit the interface configuration mode.

The following example configures Secondary VLAN routing:

```
DES-7200# configure terminal
DES-7200(config)# interface vlan 202
DES-7200(config-if)# private-vlan mapping add 303-307,309,440
DES-7200(config-if)# end
DES-7200#
```

Note

The primary VLAN and the secondary VLANs in this process are associated.

8.2.5 Configuring a Layer 2 Interface as the Host Port of a Private VLAN

To configure a layer 2 interface as the Host Port of a private VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface***>**	Enter the interface configuration mode. Three kinds of interfaces are available: fastethernet, GE and 10GE.
switchport mode private-vlan host	Configure the interface as the host interface of the private VLAN.
no switchport mode	Remove the configuration.
End	Exit the interface mode.
switchport private-vlan host-association *p_vid s_vid*	Associate the layer 2 interface with the private VLAN.
no switchport private-vlan host-association	Remove the association.

For example:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# switchport mode private-vlan host
DES-7200(config-if)# switchport private-vlan host-association
202 203
DES-7200(config-if)# end
```

Note

The primary VLAN and the secondary VLANs in this process are associated.

8.2.6 Configuring a Layer 2 Interface as the Isolated PVLAN Trunk Port

To configure a layer 2 interface as the isolated trunk port in the PVLAN, execute the following commands:

Command	Description

Command	Description
DES-7200# **configure terminal**	**Enter the global configuration mode.**
DES-7200(config-if)# **interface** <*interface*>	**Enter the interface configuration mode. Three kinds of interfaces are available: Megabit, Gigabit, 10 Gigabit.**
DES-7200(config-if)# **switchport mode trunk**	**Configure the trunk mode.**
DES-7200(config-if)# **switchport private-vlan association trunk** *p_vid s_vid* OR: DES-7200(config-if)# **no switchport private-vlan association trunk** *p_vid s_vid*	**Associate the Layer2 port and the private VLAN.** ***p_vid:*** **primary vlan id;** ***s_vid:*** **secondary vlan id.** **Remove the configuration.**
DES-7200(config-if)# **switchport trunk allowed vlan** {**all** | [**add** | **remove** | **except**] } *vlan-list*	**(Optional) Configure the allowed VLAN list on the Trunk port.** all: **all supported VLANs in the allowed VLAN list;** add: **add the specified VLAN list to the allowed VLAN list;** remove: **remove the specified VLAN from the allowed VLAN list;** except: **add all VLANs beyond the VLAN list to the allowed VLAN list.** ***vlan-list:*****can be a VLAN, or a series of VLAN, for example, 10-20.**
DES-7200(config-if)# **switchport trunk native vlan** *vlan-id*	**Configure the Native VLAN** **Use the** no switchport trunk native **command in the interface configuration mode to restore the Trunk Native VLAN list to the default VLAN1.**

For example:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# switchport private-vlan association trunk 202 203
DES-7200(config-if)# switchport trunk allowed vlan 100
DES-7200(config-if)# switchport trunk native vlan 100
```

```
DES-7200(config-if)# end
DES-7200#
```

Note

The primary VLAN and the secondary VLANs in this process are associated.

8.2.7 Configuring a Layer 2 Interface as the Promiscuous Port of a Private VLAN

To configure a layer 2 interface as the promiscuous port of a private VLAN, execute the following commands:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface***>**	Enter the interface configuration mode. Three kinds of interfaces are available: Megabit, Gigabit, and 10 Gigabit.
switchport mode private-vlan promiscuous	Configure the interface as the promiscuous port of the private VLAN.
no switchport mode	Remove the configuration.
switchport private-vlan mapping p_vid{svlist | add *svlist* **| remove** *svlist***}**	Map the secondary VLANs to the promiscuous port.
no switchport private-vlan mapping	Remove the mapping.

For example:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# switchport mode private-vlan promiscuous
DES-7200(config-if)# switchport private-vlan mapping 202 add 203
DES-7200(config-if)# end
```

Note

The primary VLAN and the secondary VLANs in this process are associated.

8.3 Showing a Private VLAN

8.3.1 Showing a Private VLAN

To show a private VLAN, execute the following command:

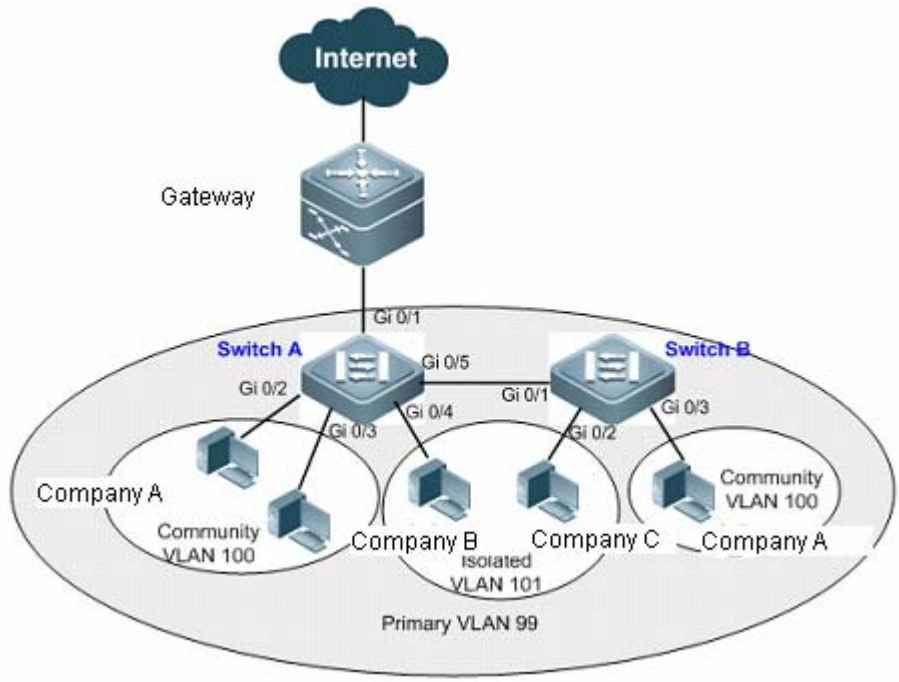
Command	Description
show vlan private-vlan [*type*]	Show the private VLAN.

```
DES-7200# show vlan private-vlan
VLAN Type  Status    Routed   Interface   Associated VLANs
--- ----   --------  ------   ---------   ------------------
202 prim   active   Enabled    Gi0/1      303-307,309,440
303 comm   active   Disabled   Gi0/2      202
304 comm   active   Disabled   Gi0/3      202
305 comm   active   Disabled   Gi0/4      202
306 comm   active   Disabled              202
307 comm   active   Disabled              202
309 comm   active   Disabled              202
440 comm   active   Enabled    Gi0/5      202
```

8.4 Typical PVLAN Configuration Examples

8.4.1 PVLAN Cross-device Layer-2 Application

8.4.1.1 Topological Diagram



Topology for PVLAN cross-device layer-2 application

8.4.1.2 Application Requirements

As shown above, in a hosting service network, company users access the network via Switch A and Switch B. The following requirements must be met:

- Intra-company users shall be able to communicate with each other, while inter-company users shall be isolated from each other.
- All company users share a same gateway address and are able to access Internet.

8.4.1.3 Configuration Tips

- Configuration tips are shown below:

1. All companies shall belong to the same PVLAN (Primary VLAN 99), and users from all companies share a layer-3 interface through this VLAN to communicate with Internet.

2. If there are multiple users in a company, respective companies shall belong to different Community VLANs (company A belonging to Community VLAN 100), so that intra-company users can communicate with each other and inter-company users are isolated from each other.

3. If there is only one user in a company, such companies shall belong to the same Isolated VLAN (company B and company C belonging to Isolated VLAN 101), so that inter-company users are isolated from each other.

- Configuration tips are shown below:

1. To run PVLAN across device, you need to configure the interconnected ports to Trunk Ports.

2. The gateway-connecting port shall be configured as Promiscuous Port; the peer port (interface of gateway device) can be configured as Trunk Port or Hybrid Port, and the Native VLAN shall be the Primary VLAN of PVLAN.

8.4.1.4 Configuration Steps

Step 1: Create Primary VLAN and Secondary VLAN on the device.

! Configure Primary VLAN 99, Community VLAN 100 and Isolated VLAN 101 on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 99
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 100
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 101
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#exit
```

! Configurations of Switch B are the same as above.

Step 2: Associate Secondary VLAN and Primary VLAN on the device.

! Associate Community VLAN 100, Isolated VLAN 101 and Primary VLAN 99 on Switch A.

```
SwitchA(config)#vlan 99
SwitchA(config-vlan)#private-vlan association 100-101
```

```
SwitchA(config-vlan)#exit
```

! Configurations of Switch B are the same as above.

Step 3: Configure the uplink port for connecting gateway device.

! Configure port Gi 0/1 of Switch A as Promiscuous Port

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode private-vlan
promiscuous
SwitchA(config-if-GigabitEthernet 0/1)#switchport private-vlan mapping 99
100-101
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

Step 4: Associate the user access ports of respective companies to the corresponding Secondary VLANs (as shown in the above figure).

! On Switch A, associate port Gi 0/2 and Gi 0/3 to Community VLAN 100 and associate port Gi 0/4 to Isolated VLAN 101.

```
SwitchA(config)#interface range gigabitEthernet 0/2-3
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 99 100
SwitchA(config-if-range)#exit
SwitchA(config)#interface gigabitEthernet 0/4
SwitchA(config-if-GigabitEthernet 0/4)#switchport mode private-vlan host
SwitchA(config-if-GigabitEthernet 0/4)#switchport private-vlan
host-association 99 101
```

! On Switch B, associate port Gi 0/2 to Isolated VLAN 101 and associate port Gi 0/3 to Community VLAN 100.

```
SwitchB(config)#interface gigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/2)# switchport private-vlan
host-association 99 101
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#switchport mode private-vlan host
SwitchB(config-if-GigabitEthernet 0/3)# switchport private-vlan
host-association 99 100
SwitchB(config-if-GigabitEthernet 0/3)#exit
```

Step 5: Configure the connection ports for running PVLAN across device.

! Configure port Gi 0/5 of Switch A as Trunk Port

```
SwitchA(config)#interface gigabitEthernet 0/5
SwitchA(config-if-GigabitEthernet 0/5)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/5)#exit
```

! Configure port Gi 0/1 of Switch B as Trunk Port.

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

8.4.1.5 Verify Configurations

Step 1: Display configurations of respective devices.

! Configurations of Switch A

```
SwitchA#show running-config
!
vlan 99
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
 private-vlan community
!
vlan 101
 private-vlan isolated
!
interface GigabitEthernet 0/1
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 99 add 100-101
!
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
interface GigabitEthernet 0/4
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/5
 switchport mode trunk
!
```

! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 99
```

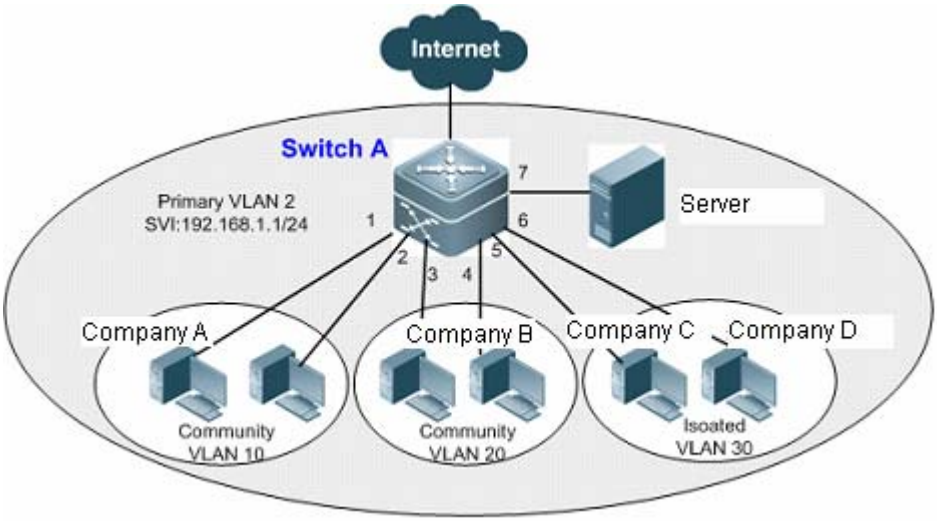
```
 private-vlan primary
 private-vlan association add 100-101
!
vlan 100
 private-vlan community
!
vlan 101
 private-vlan isolated
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 99 101
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 99 100
!
```

Step 2: Display PVLAN-related configurations on respective devices.

```
SwitchA#show vlan private-vlan
VLAN  Type      Status   Routed   Ports          Associated VLANs
------------------------------ ------------------
99    primary   active   Disabled Gi0/1, Gi0/5          100-101
100   community active   Disabled Gi0/2, Gi0/3, Gi0/5       99
101   isolated  active   Disabled Gi0/4, Gi0/5               99
```

8.4.2 Layer-3 Application of PVLAN on a Single Device

8.4.2.1 Topological Diagram



Topology for layer-3 application of PVLAN on a single device

8.4.2.2 Application Requirements

As shown above, in a hosting service network, company users access the network via the layer-3 device of Switch A. The following requirements must be met:

- Intra-company users shall be able to communicate with each other, while inter-company users shall be isolated from each other.
- All company users can access the server.
- All company users share a same gateway address and are able to access Internet.

8.4.2.3 Configuration Tips

1) Configure PVLAN on the device (Switch A). For detailed configurations, please refer to the configurations described in the section of "PVLAN Cross-device Layer-2 Application".
2) Configure the server-connecting port (Gi 0/7) as the Promiscuous Port. All company users can communicate with the server via Promiscuous Port.

3) On the layer-3 device (Switch A), configure the gateway address of PVLAN (configure SVI of VLAN2 as 192.168.1.1/24) and configure the layer-3 port mapping of Primary VLAN (VLAN 2) and Secondary VLAN (VLAN 10, 20 and 30). All company users can access Internet via this gateway address.

8.4.2.4 Configuration Steps

Step 1: Create Primary VLAN and Secondary VLAN on the device.

! Configure Primary VLAN 2, Community VLAN 10, Community VLAN 20 and Isolated VLAN 30 on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan primary
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 10
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#private-vlan community
SwitchA(config-vlan)#exit
SwitchA(config)#vlan 30
SwitchA(config-vlan)#private-vlan isolated
SwitchA(config-vlan)#exit
```

Step 2: Associate Secondary VLAN and Primary VLAN on the device.

! Associate Community VLAN 10, Community VLAN 20, Isolated VLAN 30 and Primary VLAN 2 on Switch A.

```
SwitchA(config)#vlan 2
SwitchA(config-vlan)#private-vlan association 10,20,30
SwitchA(config-vlan)#exit
```

Step 3: Associate the user access ports of respective companies to the corresponding Secondary VLANs (as shown in the above figure).

! On Switch A, associate ports Gi 0/1 and Gi 0/2 to Community VLAN 10, associate ports Gi 0/3 and Gi 0/4 to community VLAN 20, and associate ports Gi 0/5 and Gi 0/6 to Isolated VLAN 30.

```
SwitchA(config)#interface range gigabitEthernet 0/1-2
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 10
SwitchA(config-if-range)#exit
SwitchA(config)#interface range gigabitEthernet 0/3-4
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 20
```

```
SwitchA(config-if-range)#exit
SwitchA(config)#interface range gigabitEthernet 0/5-6
SwitchA(config-if-range)#switchport mode private-vlan host
SwitchA(config-if-range)#switchport private-vlan host-association 2 30
SwitchA(config-if-range)#exit
```

Step 4: Configure the server-connecting port.

! Configure port Gi 0/7 of Switch A as Promiscuous Port

```
SwitchA(config)#interface gigabitEthernet 0/7
SwitchA(config-if-GigabitEthernet 0/7)#switchport mode private-vlan
promiscuous
SwitchA(config-if-GigabitEthernet 0/7)#switchport private-vlan maping 2
10,20,30
SwitchA(config-if-GigabitEthernet 0/7)#exit
```

Step 5: Configure the gateway address of PVLAN on layer-3 device.

! On Switch A, configure the SVI of Primary VLAN 2 as 192.168.1.1/24, and configure Community VLAN 10, Community VLAN 20 and Isolated VLAN 30 mapping.

```
SwitchA(config)#interface vlan 2
SwitchA(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 2)#private-vlan mapping 10,20,30
SwitchA(config-if-VLAN 2)#exit
```

8.4.2.5 Verify Configurations

Step 1: Display the configurations of Switch A.

```
SwitchA#show running-config
!
vlan 2
 private-vlan primary
 private-vlan association add 10,20,30
!
vlan 10
 private-vlan community
!
vlan 20
 private-vlan community
!
vlan 30
 private-vlan isolated
!
interface GigabitEthernet 0/1
 switchport mode private-vlan host
```

```
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/2
 switchport mode private-vlan host
 switchport private-vlan host-association 2 10
!
interface GigabitEthernet 0/3
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/4
 switchport mode private-vlan host
 switchport private-vlan host-association 2 20
!
interface GigabitEthernet 0/5
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/6
 switchport mode private-vlan host
 switchport private-vlan host-association 2 30
!
interface GigabitEthernet 0/7
 switchport mode private-vlan promiscuous
 switchport private-vlan mapping 2 add 10,20,30
!
interface VLAN 2
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
 private-vlan mapping add 10,20,30
!
```

Step 2: Display PVLAN-related configurations.

```
SwitchA#show vlan private-vlan
VLAN  Type   Status   Routed   Ports  Associated VLANs
------------------------------ ------------------
2    primary   active   Enabled  Gi0/7       10,20,30
10   community  active   Enabled  Gi0/1, Gi0/2   2
20   community  active   Enabled  Gi0/3, Gi0/4   2
30   isolated   active   Enabled  Gi0/5, Gi0/6   2
```

9 Share VLAN Configuration

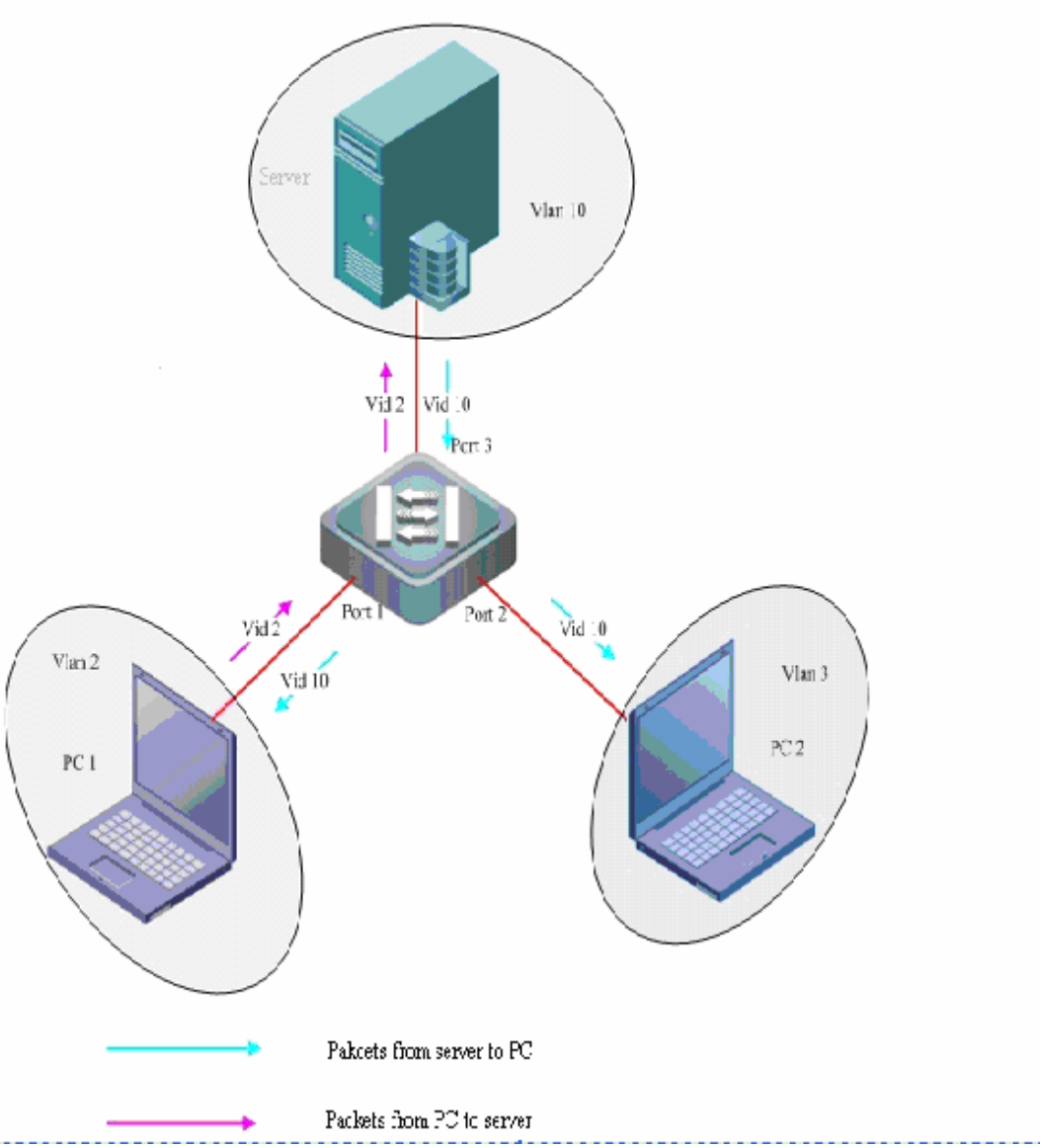
9.1 Overview

As a VLAN sharing addresses, the Share VLAN can solve the problem that the packets to this MAC address will be broadcast in another VLAN while the switch learns a MAC address in a VLAN. When a VLAN is set to be the Share VLAN, however, it will replicate its learned dynamic and static MAC addresses to other VLANs, and other VLANs also replicate their learned dynamic and static MAC addresses to the Share VLAN. The address triggering this address application procedure is called home address and the replicated addresses are called sub addresses. The sub addresses will not trigger replication anymore. When the home address is deleted or aged out, the sub addresses are deleted or aged out at the same time. However, deleting sub addresses will not bring any influence on the home address.

9.2 Application Model

Packets are forwarded by searching the address table. If the address table has not the destination address, the packets will be broadcasted in a VLAN, as shown in Figure 1.

Figure 1



The VID of the packets from PC1 to the server is 2. The switch will learn PC1's address, as shown in Table 1.

Table 1

VLAN	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	Port 1

Assume that all the response packets of the server belong VLAN 10. Since the switch learns PC1's MAC address with VID 2, it will broadcast the response packets whose VID is 10 upon their arrival. Consequently, PC2 will receive the packets that the server sends to PC1, which are unuseful. This wastes bandwidth and PC2's resource. How to avoid this problem? Administrator can set VLAN 10 to be a Share VLAN, so that the switch will replicate the MAC address to VLAN 10 when it learns the MAC address with VID 2.

Table 2

VLAN	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	Port 1
10	PC1-MAC	DYNAMIC	Port 1

In this way, when the response packets from the server arrive in the switch, the switch can find the address with VID 10 and send them out only through port 1.

Note

- A switch supports only one Share VLAN.
- Only replicating dynamic MAC address and static MAC address is allowed.
- The protocol VLAN, private VLAN, remote VLAN or interface address table replication function is mutually exclusive with the Share VLAN, and vice versa.
- The super VLAN cannot be set to be the Share VLAN, and vice versa.
- The sub VLAN cannot be set to be the Share VLAN, and vice versa.
- The MAC addresses in the Share VLAN will not be replicated to the super VLAN, and vice versa.
- Once a sub-address is deleted, it will be replicated only after its home address is aged out or deleted and the sub address is learned again.
- The MAC address replication will fail in case of shortage of the MAC address table. Once replication failed, the home address and replicated sub-address will be deleted if the home address is a dynamic address or the replicated sub-address will be deleted if the home address is a static address.

9.3 Configure Share VLAN

Do the following steps to configure the Share VLAN:

Command	Function
DES-7200(config-vlan)**# Share**	Enable the Share VLAN.
DES-7200(config-vlan)**# no Share**	Disable the Share VLAN.

For instance:

```
DES-7200# configure
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# vlan 10
DES-7200(config-vlan)# Share
DES-7200(config)# end
```

9.4 Showing the Share VLAN

Do the following steps to show the Share VLAN:

Command	Function
DES-7200(config-vlan)**#show mac-address-table Share**	Show the status of MAC address.
DES-7200# **show vlan**	Show the Share VLAN.

For example:

Show the Share VLAN:

```
DES-7200#show vlan
VLAN  Name      Status    Ports
----  --------  -------  --- --------------------------------
   1   VLAN0001  STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                           Gi0/5, Gi0/6, Gi0/7, Gi0/8
                           Gi0/9, Gi0/10, Gi0/11, Gi0/12
                           Gi0/13, Gi0/14, Gi0/15, Gi0/16
                           Gi0/17, Gi0/18, Gi0/19, Gi0/20
                           Gi0/21, Gi0/22, Gi0/23, Gi0/24
   2   VLAN0002  STATIC    Gi0/1
   4   VLAN0004  STATIC    Gi0/2
10   VLAN0010  Share    Gi0/1
```

Show the status of the MAC address:

```
DES-7200# show mac-address-table Share
Vlan  MAC Address    Type    Interface            Status
----  -------------- ------- ------------------ ----------
   2   0040.4650.1e1e DYNAMIC GigabitEthernet 0/1 original
  10   0040.4650.1e1e DYNAMIC GigabitEthernet 0/1 duplicated
```

9.5 Typical SHARE VLAN Configuration Example

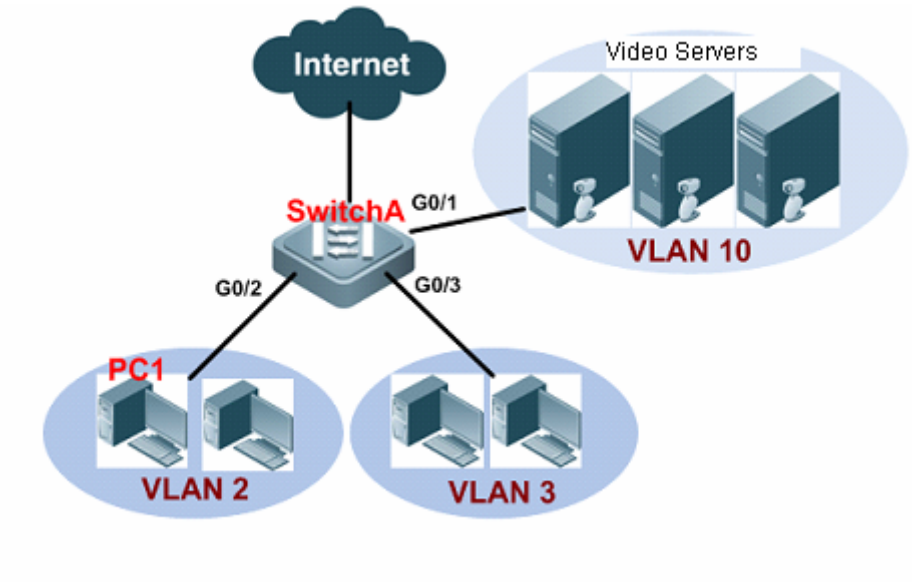
9.5.1 SHARE VLAN video-on-demand application

9.5.1.1 Networking Requirements

On an office network, SwitchA is connected with a video-on-demand PC user (PC1) belonging to VLAN 2. It is requested that the access users in VLAN 3 won't be affected while the users in VLAN 2 is access the video server

(belonging to VLAN 10), making sure the network resources won't be wasted (namely users in VLAN 3 cannot receive the reply packets sent by video server).

9.5.1.2 Network Topology



SHARE VLAN video-on-demand application

9.5.1.3 Configuration Tips

To meet the needs, we must configure VLAN 10 as a SHARE VLAN on SwitchA.

After PC1 has requested the video program, the video server will reply to the request. When packets reach SwitchA, the switch will insert VLAN 10 Tag according to the PVID value.

On SwitchA, configure VLAN10 as the SHARE VLAN; the addresses learned by the switch will be:

Vlan	MAC	Address Type	Interface
2	PC1-MAC	DYNAMIC	G0/2
10	PC1-MAC	DYNAMIC	G0/2

Packets will be directly sent to PC1 through G0/2, and other users won't be able to receive these reply packets.

9.5.1.4 Configuration Steps

1. On SwitchA, configure G0/2 as a hybrid port (default VLAN is 2, and the allowed UNTAG VLANs include VLAN 2 and VLAN 10); configure G0/3 as a

hybrid port (default VLAN is 3, and the allowed UNTAG VLANs include VLAN 3 and VLAN 10); configure G0/1 as a hybrid port (default VLAN is 2, and the allowed UNTAG VLANs include all vlans).

```
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-GigabitEthernet 0/2)#switchport mode hybrid
DES-7200(config-GigabitEthernet 0/2)#switchport hybrid native vlan 2
DES-7200(config-GigabitEthernet 0/2)#switchport hybrid allowed vlan untagged
2,10
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-GigabitEthernet 0/3)#switchport mode hybrid
DES-7200(config-GigabitEthernet 0/3)#switchport hybrid native vlan 3
DES-7200(config-GigabitEthernet 0/2)#switchport hybrid allowed vlan untagged
3,10
DES-7200(config-GigabitEthernet 0/1)#switchport mode hybrid
DES-7200(config-GigabitEthernet 0/1)#switchport hybrid native vlan 10
DES-7200(config-GigabitEthernet 0/1)#switchport hybrid allowed vlan untagged
1-4094
```

2. On SwitchA, configure VLAN 10 as the SHARE VLAN;

```
DES-7200(config)#vlan 10
DES-7200(config-vlan)#share
```

9.5.1.5 Verification

Step 1: PC1 (assuming that its IP address is 192.168.12.4) shall be able to ping the server (assuming that its IP address is 192.168.12.6);

Step 2: View the information about SHARE VLAN on SwitchA;

```
DES-7200(config-vlan)#show vlan
VLAN  Name      Status    Ports
----  --------  -------  --- --------------------------------
  1   VLAN0001  STATIC    Gi0/1, Gi0/2, Gi0/3, Gi0/4
                          Gi0/5, Gi0/6, Gi0/7, Gi0/8
                          Gi0/9, Gi0/10, Gi0/11, Gi0/12
                          Gi0/13, Gi0/14, Gi0/15, Gi0/16
                          Gi0/17, Gi0/18, Gi0/19, Gi0/20
                          Gi0/21, Gi0/22, Gi0/23, Gi0/24
  2   VLAN0002  STATIC    Gi0/1, Gi0/2, Gi0/3
  3   VLAN0003  STATIC    Gi0/1, Gi0/2, Gi0/3
10  VLAN0010  SHARE     Gi0/1, Gi0/2, Gi0/3
```

Step 3: View MAC address status on SwitchA (only display the information of port 2; other ports are omitted):

```
DES-7200(config)#show mac-address-table share
Vlan  MAC Address     Type     Interface             Status
----  --------------  -------  ------------------  ----------
```

```
 2   00d0.f864.6909 DYNAMIC GigabitEthernet 0/2 original
10   00d0.f864.6909 DYNAMIC GigabitEthernet 0/2 duplicated
```

10 MSTP Configuration

10.1 MSTP Overview

10.1.1 STP and RSTP

10.1.1.1 STP and RSTP Overview

DES-7200 series supports both the STP protocol and the RSTP protocol, as well as complying with the IEEE 802.1D and IEEE 802.1w standards.

The STP protocol can prevent broadcast storm caused by link loops and provide link redundancy and backup.

For the layer 2 Ethernet, there is only one active channel between two LANs to avoid broadcast storm. However, it is necessary to set up redundant links to improve the reliability of a LAN. Furthermore, some channels should be in the backup status in order to take up its work when a link fails. It is obviously hard to control this process by manual. The STP protocol can complete this work automatically. It enables a device in a LAN to:

- Discover and activate an optimal tree-type topology of the LAN.
- Detect and fix failures and automatically update the network topology to offer the possible optimal tree-type structure at any time.

The LAN topology is automatically calculated by a set of bridge parameters set by the administrator. The proper configuration of these parameters is helpful to offer an optimal solution.

The RSTP protocol is completely compatible with the 802.1D STP protocol downward. As with traditional protocol, the RSTP protocol can prevent loop and offer link redundancy. The most critical feature of the RSTP protocol is quickness. If the bridges in a LAN support the RSTP protocol and are configured appropriately by administrators, it will take no more than 1 second to re-span the topology tree once the network topology changes (it takes about 50 seconds for traditional STP protocol to re-span the topology tree).

Caution

For the switch buffer control, see the chapter *Buffer Control* in *Configuring QOS*.

10.1.1.2 Bridge Protocol Data Units (BPDU):

A stable tree-type topology depends on the following elements :

- The unique bridge ID of each bridge consists of the bridge priority and the MAC address.
- The root path cost refers to the cost from a bridge to the root bridge.
- Each port ID consists of the port priority and port number.

By exchanging the Bridge Protocol Data Units (BPDU) frame destined to the multicast address 01-80-C2-00-00-00 (in hex), bridges gets the information necessary for building the optimal tree-type topology.

A BPDU is comprised of the following elements:

- Root Bridge ID (root bridge ID that a bridge considers)
- Root Path cost (Root Path cost of a bridge).
- Bridge ID (ID of a bridge).
- Message age (the live time of the message)
- Port ID (port ID sending the message).
- Forward-Delay Time, Hello Time and Max-Age: time parameters.
- Other flag bits, such as network topology change and port status.

Once a port of a bridge receives a BPDU message whose priority is higher than its priority (or smaller bridge ID and smaller root path cost), the bridge will store this message on the port while updating and propagating them to all other ports. If the BPDU with lower priority is received, the bridge will discard this message.

This mechanism propagates a BPDU message of higher priority in the whole network. As a result:

- A bridge is elected to be the root bridge in the network.
- Each bridge other than the root bridge has a root port that offers a shortest path to the root bridge.
- Each bridge will calculate the shortest path to the root bridge.
- Each LAN has a designated bridge that lies in the shortest path between this LAN and the root bridge. The port for connecting the designated bridge and the LAN is referred to as the designated port.
- The root port and the designated port are in the forwarding status.
- Other ports beyond the spanning tree are in the discarding status.

10.1.1.3 Bridge ID

As specified in IEEE 802.1W standard, each bridge has an unique bridge ID based on which the root bridge is elected in spanning tree algorithm. The bridge ID consists of eight bytes, in which the last six bytes are the MAC address of the bridge, and the first two bytes are shown in the table below. Of which, the first

four bits denote the priority, while the last twelve bits denote the system ID for extending the protocol in the future. This value is 0 in the RSTP, so the priority of the bridge should be configured as the multiple of 4096.

	Priority value				System ID											
Bit	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1
Value	32768	16384	8192	4096	2048	1024	512	256	128	64	32	16	8	4	2	1

10.1.1.4 Spanning-Tree Timers

The following describes three timers impacting the performance of spanning tree.

- Hello timer: Interval to send the BUDU message.
- Forward-Delay timer: Interval to change the port status, that is, the time interval at which the port switches from the listening status to the learning status and vice versa when the RSTP protocol runs in the compatible STP protocol mode.
- Max-Age timer: The longest time for the BPDU message. The system will discard the message when the timer times out.

10.1.1.5 Port Roles and Status

A port plays a role to present its function in the network topology.

- Root port: The port that provides the shortest path to the root bridge.
- Designated port: The port through which each LAN is connected to the root bridge.
- Alternate port: The alternate port of the root port that will take up its work when the root port fails.
- Backup port: The backup port of the designated port. If two ports of a bridge are connected to a LAN, the port with higher priority is the designated port and the other one is the backup port.
- Disable port: The port that is not in the active status, namely, the ports whose operation status is down.

Figure 1, Figure 2 and Figure 3 below show the roles of various ports:

R = Root port D = Designated port A = Alternate port B = Backup port

Unless otherwise stated, the priorities of these ports are in the descending order from left to right.

Figure-1

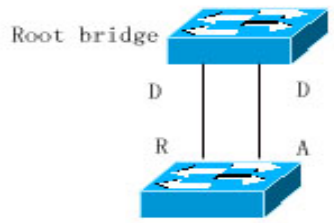


Figure-2

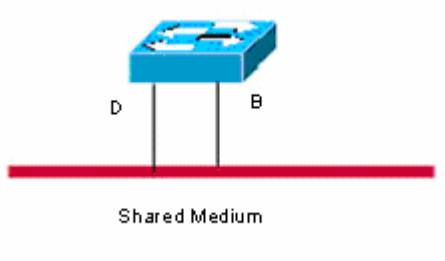
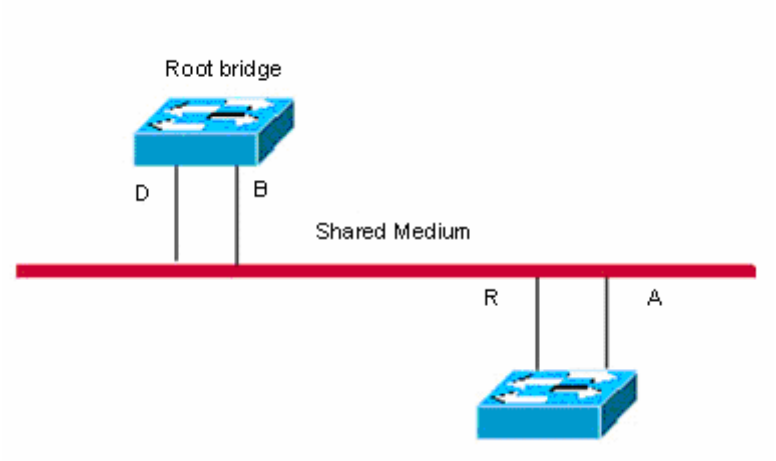


Figure-3



There are three port states for every port to indicate whether the data packet is forwarded and control the topology of the whole spanning tree.

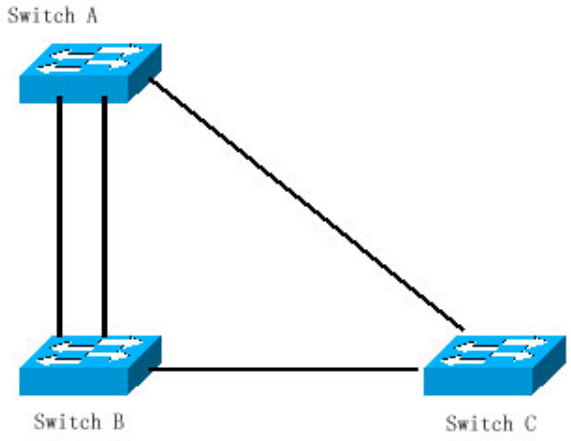
- Discarding: Neither forward the received frame nor learn about the source Mac address.
- Learning: Do not forward the received frame, but learn about the source Mac address, so it is a transitional status.
- Forwarding: Both forward the received frame and learn about the source Mac address.

For the stable network topology, only the root port and designated port can be the forwarding status, while other ports are only in the discarding status.

10.1.1.6 Generating a Network Topology Tree (Typical Application Solution)

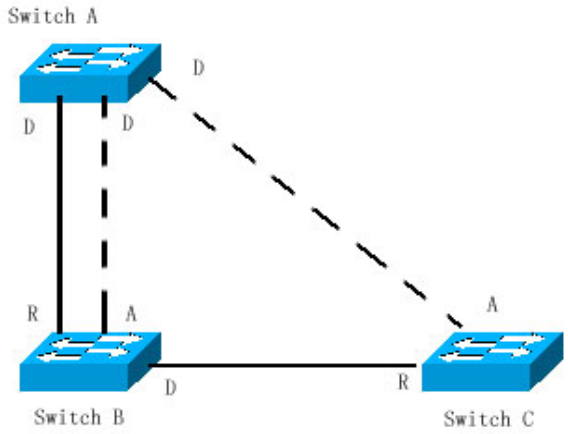
We now describe how the STP and RSTP protocols span a tree-type structure by the mixed network topology. As shown in Figure 4, the bridge IDs of Switches A, B and C are assumed in the ascending order. Namely, Switch A presents the highest priority. There is the 1000M link between switch A and switch B, and the 100M link between switch A and switch C, while it is the 10M link between switch B and switch C. Switch A acts as the backbone switch of this network and implements the link redundancy for both Switch B and Switch C. Obviously, broadcast storm would occur if all these links are active.

Figure-4



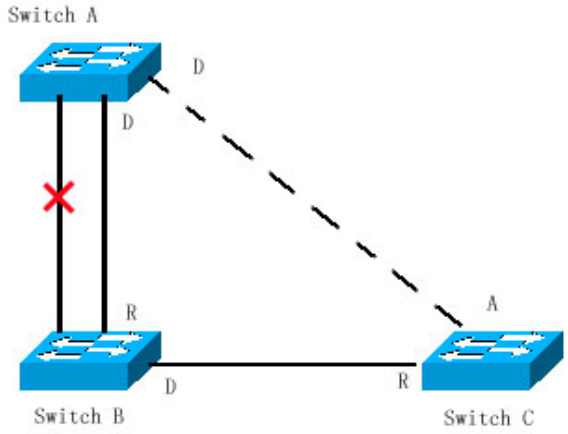
If all of these three switches enable the Spanning Tree protocol, they will select switch A as the root bridge by exchanging BPDU message. Once Switch B detects that two ports are connected to Switch A, it will select the port with the highest priority as the root port, while another one is selected as the alternate port. Meanwhile, Switch C detects that it can reach Switch A through Switch B or directly. However, Switch C discovers that the cost of the path from Switch B to Switch A is lower than that directly (For the costs corresponding to various paths, refer to table ***), so Switch C selects the port connected with Switch B as the root port, while the one that connected with Switch A as the alternate port. Various ports enter the corresponding status after their roles are determined. As a result, the network topology is generated as shown in Figure 5.

Figure-5



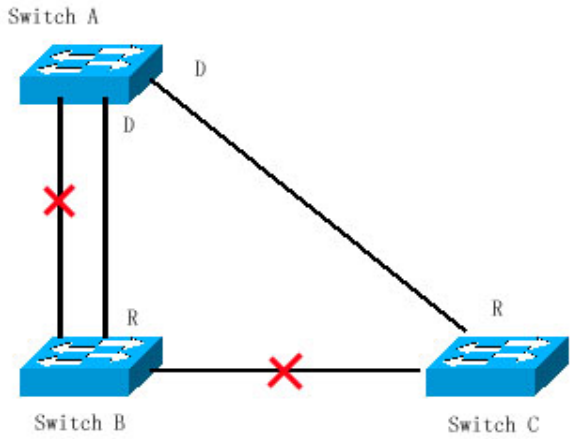
If the active path between Switch A and Switch B fails, the backup path will work. Consequently, the network topology is generated as shown in Figure 6.

Figure-6



If the path between Switch B and Switch C fails, Switch C will automatically switch the alternate port to the root port. Consequently, the network topology is generated as shown in Figure 7.

Figure-7



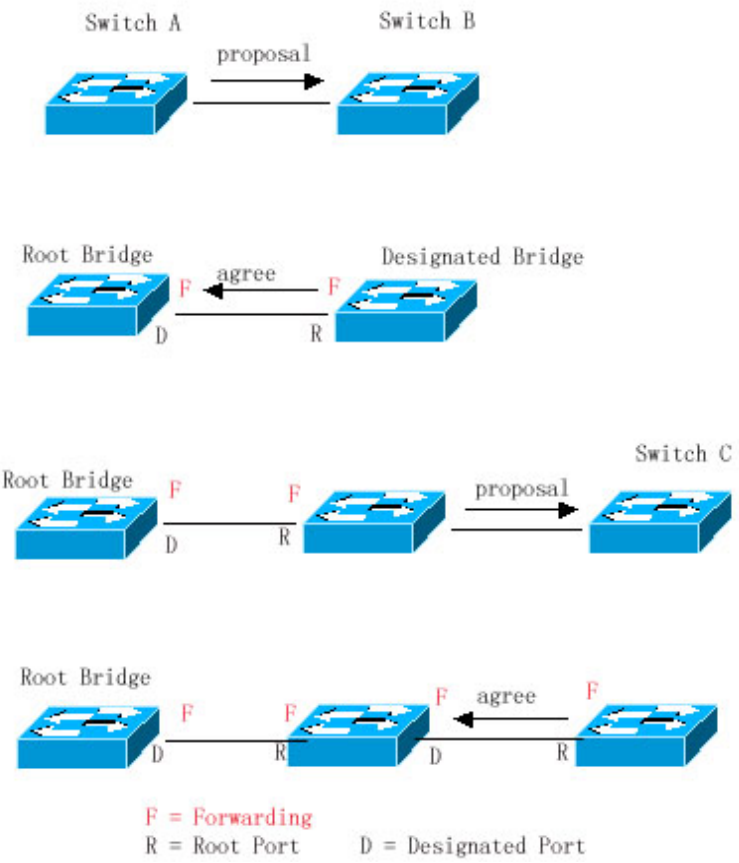
10.1.1.7 Rapid Convergence of RSTP

The following introduces the special function of RSTP: enabling rapid forwarding on a port.

The STP protocol will forward packets after 30s since the port roles are selected, which is twice as the Forward-Delay Time (you can set the Forward-Delay Time, which is 15s by default). Furthermore, the root port and designated port of each bridge will carry out the forwarding again after 30s, so it will take about 50s to stabilize the tree-type structure of the whole network topology.

The forwarding procedure of the RSTP protocol is different from that of the STP protocol. As shown in Figure 8, Switch A sends the specific proposal message of the RSTP protocol. Switch B detects that the priority of Switch A is higher than itself, takes the Switch A as the root bridge and the port that receives the message as the root port and forwards the proposal message. Then it sends the Agree message to Switch A through the root port. Upon the receipt of the proposal message, Switch A will forward the message through its designated port. After that, Switch sends the proposal message through the designated port to extend the spanning tree in turn. In theory, the RSTP protocol can immediately restore the tree-type network structure to implement rapid convergence when the network topology changes.

Figure-8



Caution

"Point-to-point Connection" between ports is required for the above "handshaking" process. In order to make full use of you device, do not use non-point-to-point connection between devices.

Other than Figure 9, other schematics in this chapter are the point-to-point connection. The following lists the example figure of the non point-to-point connection.

Example of Non Point-to-point Connection:

Figure-9

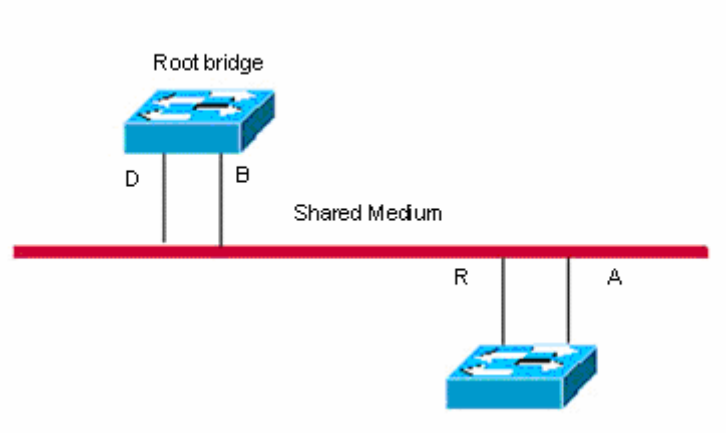
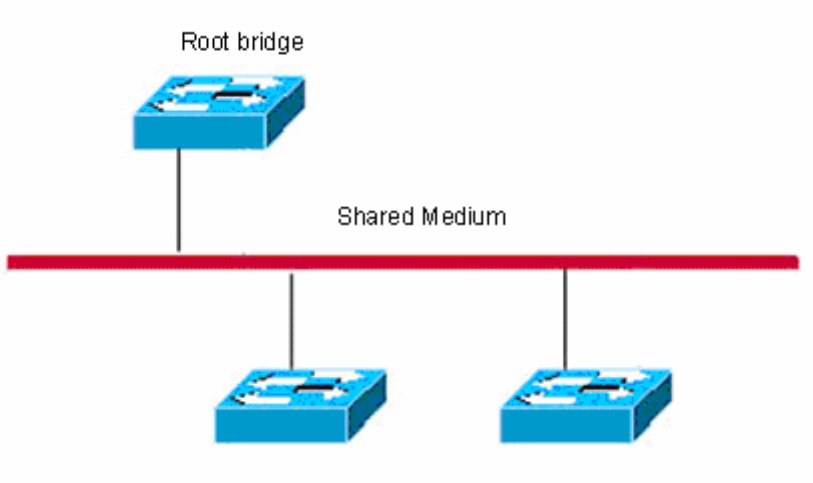
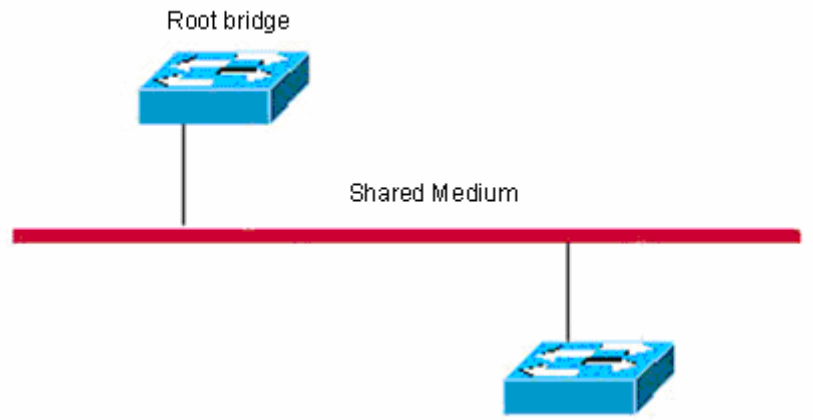


Figure-10



In addition, the following figure is a point-to-point connection and should be differentiated by users carefully.

Figure-11



10.1.1.8 Compatibility of RSTP and STP

The RSTP protocol is completely compatible with the STP protocol. It will judge whether the connected bridge supports the STP protocol or the RSTP protocol by the version number of the received BPDU message automatically. Only the forwarding process of the STP protocol is executed in the case of that the bridge supports the STP protocol. This cannot maximize the performance of the RSTP protocol.

Furthermore, using the RSTP protocol and the STP protocol will cause a problem. As shown in Figure 17-12, Switch A supports the RSTP protocol, while Switch B supports the STP protocol. Both switches are connected with each other. Switch A will send the STP BPDU message to Switch B for compatibility. However, if Switch A is connected with the RSTP-enabled Switch C, Switch A still sends the STP BPDU message, and thus causing that Switch C considers Switch A a STP-enabled bridge. As a result, two RSTP-supported switches run the STP protocol, reducing their efficiency greatly.

For this reason, the RSTP protocol provides the protocol-migration function to send the RSTP BPDU message forcibly in case that the peer bridge must support RSTP. In this way, Switch C will detect the bridge connected with it supports the RSTP protocol, so both two devices can run the RSTP protocol as shown in Figure 13.

Figure-12 Protocol Migration

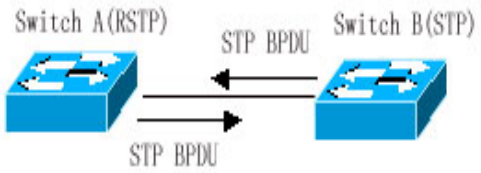
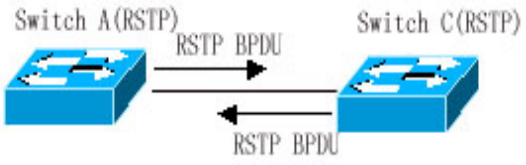


Figure-13



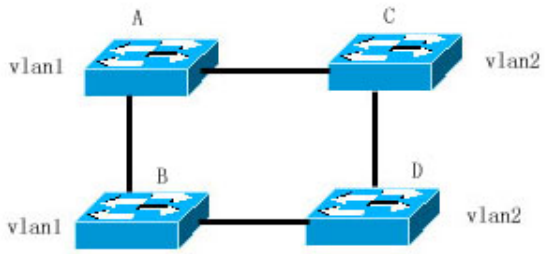
10.1.2 MSTP Overview

DES-7200 series supports the MSTP protocol, a new spanning-tree protocol derived from the traditional STP and RSTP protocols that includes the rapid forwarding mechanism of the RSTP protocol itself.

Since traditional spanning tree protocols are not related to a VLAN, the following problems may occur in a specific network topology.

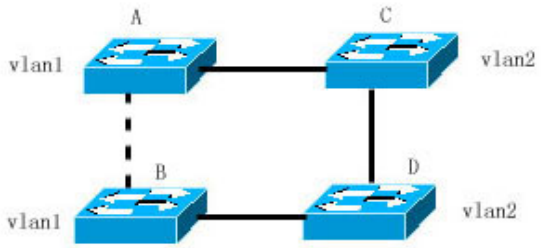
As shown in Figure 14, Switches A and B are located in Vlan1, and switches C and D in Vlan2. They form a loop.

Figure-14



If the cost of the path from Switch A through Switch C, Switch D to Switch B is smaller than that of the direct path from Switch A to Switch B, the latter path will be torn down, as shown in Figure 15. Packets in Vlan1 can not be forwarded because Switches C and D do not contain Vlan1. In this way, Vlan1 of Switch A cannot communicate with Vlan1 of Switch B.

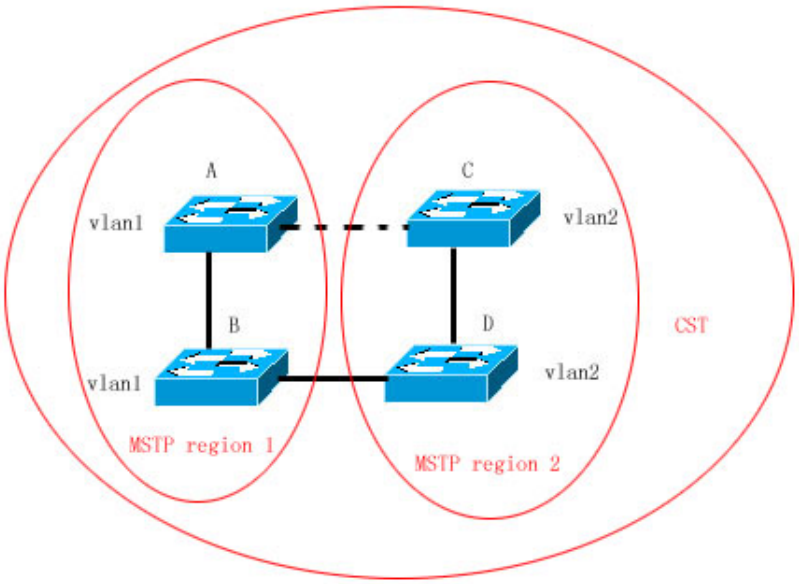
Figure-15



The MSTP protocol is developed to address this problem. It partitions one or more vlans of the switch into an instance, so the switches with the same instance configuration form a region (MST region) to run a separated spanning tree (this internal spanning-tree is referred to as the IST). The MST region is equivalent to a large device, which executes the spanning tree algorithm with other MST regions to obtain a whole spanning tree, referred to as the common spanning tree (CST).

With this algorithm, the above mentioned network can form the topology shown in Figure 16. Switches A and B are within the MSTP region 1 without a loop, so no path is discarded. This is also the case in the MSTP region 2. Region 1 and region 2 serve as two large devices respectively. There is a loop between them, so one path is discarded according to related configuration.

Figure-16



In this way, no loop occurs and the communication between the devices in a VLAN works as well.

10.1.2.1 How to Partition MSTP regions

According to above description, MSTP regions should be partitioned rationally and the switches in a MSTP region should be configured similarly for the MSTP protocol to work properly.

The MST configuration information contains:

- MST region name (name): A string of up to 32 bytes identifying the MSTP region.
- MST revision number: A revision number of 16 bits identifying the MSTP region.
- MST instance-vlan table: Each device can create up to 64 instances with IDs ranging from 1 to 64). Instance 0 always exists, so the system totally supports 65 instances. You can allocate 1 to 4094 VLANs for different instances (0 to 64) as needed, and the unallocated VLANs belong to instance 0 by default. In this way, each MSTI (MST instance) is a VLAN group and executes the spanning tree algorithm within the MSTI according to the MSTI information of the BPDU without the effect of the CIST and other MSTIs.

You can use the **spanning-tree mst configuration** command in the global configuration mode to enter the MST configuration mode and configure above information.

The MSTP BPDU carries above information. If a device has received the same MST configuration information of the BPDU as that of itself, it considers that the device connecting to this port belong to the same MST region as itself.

You are recommended to configure the instance-vlan table while the STP protocol is disable, and then enable the MSTP protocol to ensure the stability and convergence of the network topology.

10.1.2.2 Spanning Tree within a MSTP region (IST)

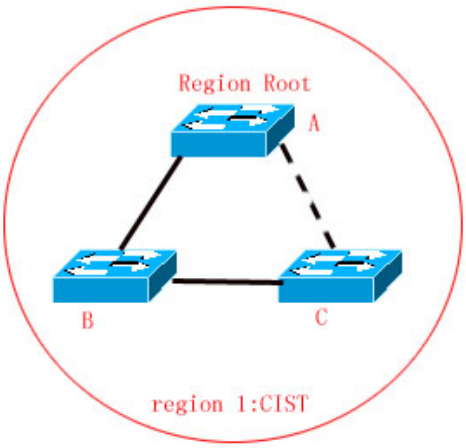
After MSTP regions are partitioned, a root bridge is elected for every instance within a region and the port role is determined for every port on a switch. A port is forwarded or discarded within an instance depneds on its role.

In this way, the IST (Internal Spanning Tree) is formed by exchanging the MSTP BPDU message, and various instances have their own spanning trees (MSTI). The spanning tree corresponding to the instance 0 is referred to as the CIST (Common Instance Spanning Tree) in conjunection with CST. That is to say, each instance provides each VLAN group with a single network topology without loop.

As shown in the following figure, Switches A, B and C form a loop within the region 1.

Switch A with the highest priority is selected as the region root in the CIST (instance 0). Then, the path between Switches A and C is discarded according to other parameters. Hence, for the VLAN group of instance 0, only the path from switch A to B and switch B to switch C are available, which break the loop of the VLAN group.

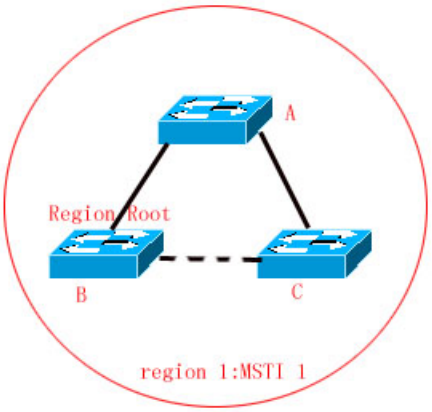
Figure-17



As shown in Figure 18, switch C with the highest priority is selected as the region root in the MSTI 1 (instance 1). Then, the path between switch A and B is

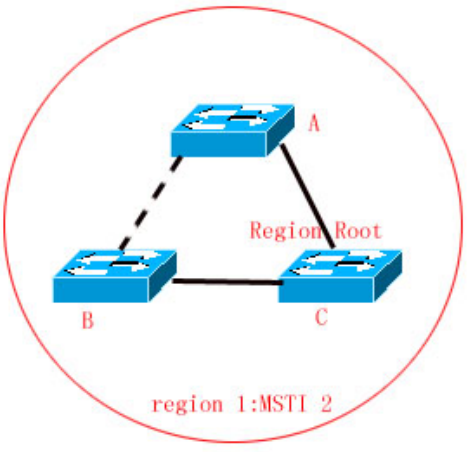
discarded according to other parameters. Hence, for the VLAN group of instance 1, only the path from switch A to switch B and switch A to switch C are available, which break the loop of the VLAN group.

Figure-18



As shown in Figure 19, switch B with the highest priority is selected as the region root in the MSTI 2 (instance 2). Then, the path between switch B and switch C is discarded according to other parameters. Hence, for the VLAN group of instance 2, only the path from switch A to switch B and switch B to switch C are available, which break the loop of the VLAN group.

Figure-19

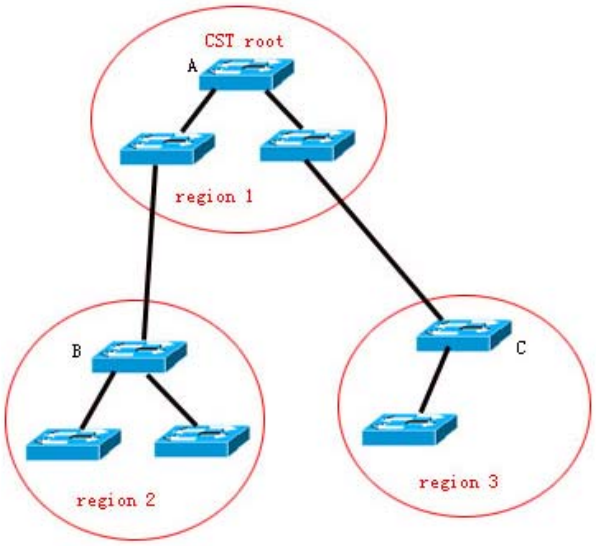


It should note that the MSTP protocol is not concerned on which VLAN a port belongs to, so users should configure corresponding path costs and priorities for ports according to actual VLAN configuration to prevent the MSTP protocol from breaking the loop unnecessarily.

10.1.2.3 Spanning Tree between MSTP regions (CST)

For CST, each MSTP region is equivalent to a large-sized device, and different MSTP regions also form a large-sized network topology tree, referred to as CST (common spanning tree). As shown in Figure 20, for CST, switch A with the smallest bridge ID is selected as the root of the entire CST (CST Root) and the CIST Regional Root in this region. In Region 2, since the root path cost from switch B to the CST root is the lowest one, switch B is selected as the CIST Regional Root in this region. Similarly, switch C is selected as the CIST Regional Root in Region 3.

Figure-20



The CIST Regional Root is not necessarily the device with the smallest bridge ID in that region. It is the device in the region that has the lowest root path cost to the CST root.

At the same time, the root port of the CIST regional root takes a new port role for the MSTI, namely the **Master port,** as the outlet of all instances, which is forwarded to all instances. In order to make the topology more stable, it is recommended to configure the outlet of the regions to the CST root on one device of this region as much as possible!

10.1.2.4 Hop Count

The IST and MSTI will not take the message age and Max age to calculate whether the BPDU message is timeout. Instead, they use the mechanism similar to the TTL of IP packets, namely hop count.

You can set it by using the **spanning-tree max-hops** command in the global configuration mode. The hop count is reduced by 1 when the BPDU message

psses through a device in a region starting from the region root bridge until it is 0, which means the BPDU message is timeout. A device will discard the BPDU message whose hop count is 0.

In order to be compatible with the STP protocol and the RSTP protocol out a region, the MSTP protocol still remains the Message age and Max age mechanisms.

10.1.2.5 Compatibility of MSTP with RSTP and STP

For the STP protocol, the MSTP protocol will send the STP BPDU to be compatible with it like the RSTP protocol. For detailed information, refer to the Compatibility of RSTP and STP section.

For the RSTP protocol, it will process the CIST part of the MSTP BPDU, so it is not necessary for the MSTP to send the RSTP BPDU to be compatible with it.

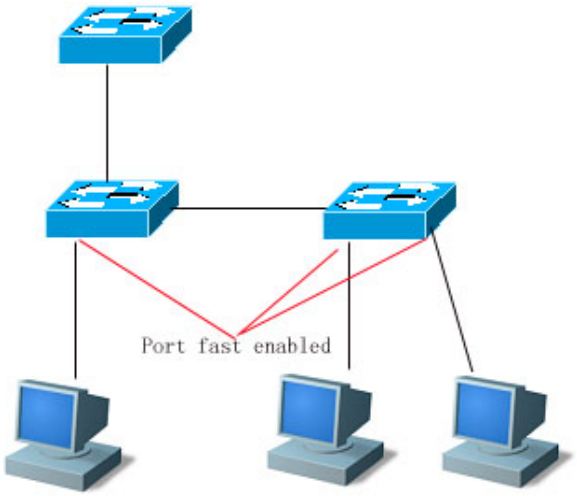
Each device that runs the STP or RSTP protocol is an independent region, and does not form the same region with any other device.

10.2 Overview of Optional Features of MSTP

10.2.1 Understanding Port Fast

If a port of a device is connected with the network terminal directly, this port can be set as the Port Fast to forward packets directly. The port does not need to wait 30 seconds before forwarding packets, which is the case when the port is not set to Port Fast. The following figure indicates which ports of a device can be set to Port Fast.

Figure-21



If the BPDU message is received from the Port Fast enabled port, its Port Fast operational state is disabled. At this time, this port will execute the forwarding by normal STP algorithm.

10.2.2 Understanding AutoEdge

If the specified port doesn't receive the BPDU message sent by the downstream port within a certain period of time (3 seconds), the port will be considered that it connects a network device and set as an edge port to enter the Forwarding status directly. An edge port will be automatically identified as a non-edge port after receiving the BPDU message.

You can disable the automatic identification function of the edge port by the **spanning-tree autoedge disabled** command.

This function is enabled by default.

1)When the AutoEdge function conflicts with the manually-configured Port Fast function, the latter shall prevail.

2) AutoEdge function can be used for rapid negotiation forwarding between the designated port and the downstream port, so the STP protocol doesn't support AutoEdge. If the designated port is in the forwarding status, Autoedge does not take effect on the port. It will take effect during repaid renegotiation such as pluging/unpluging network cables.

Caution

3) If a port enables the BPUD Filter, it forwards the BPDU message directly, but not be identified as the edge port automatically.

4) AutoEdge function is only applicable for the designated port.

5) AutoEdge complies with the standard definition of IEEE 802.1D (version 2004), in which the parameter range of Bridge Hello Time has been modified as 1.0-2.0. Therefore, you shall confirm that the Hello Time value is within the range when using AutoEdge function, or the risk of temporary loop will occur. It is recommended to disable AutoEdge function if it is neccesary to exceed the range of Hello Time.

10.2.3 Understanding BPDU Guard

The BPDU guard can be enabled globally or on individual interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpduguard default** command to open the global BPDU guard enabled status in the global configuration mode. In this status, if the BPDU message is received through a Port Fast-enabled port or a AutoEdge port, this port will enter the error-disabled status, indicating the configuration error. At the same time, the port will be closed to show that some illegal users may add a network device to the network, which change the network topology.

You can also use the **spanning-tree bpduguard enable** command to enable BPDU guard on individual interface in the interface configuration mode (it is not related to whether it is AutoEdge port or not). Under this situation, it will enter the error-disabled status if this interface receives the BPDU message.

10.2.4 Understanding BPDU Filter

The BPDU filter can be enabled globally or on individual interface. There are some slightly difference between these two ways.

You can use the **spanning-tree portfast bpdufilter default** command to enable the BPDU filter globally in the global configuration mode. In this status, the BPDU messages can not be received or sent through a Port Fast-enabled port or a AutoEdge port, leading to no BPDU messages received by the host directly connecting the port. The BPDU filter will be disabled when the Port Fast is disabled for the AutoEdge port receives the BPDU message.

You can also use the **spanning-tree bpdufilter enable** command to enable the BPDU filter on individual interface in the interface configuration mode (it is not related to whether it is AutoEdge port or not). In this situation, this interface will not receive or transmit the BPDU message, but execute the forwarding directly.

10.2.5 Understanding Tc-protection

TC-BPDU messages are BPDU messages carrying with TC flag. When the L2 switch receives these messages, the network topology will change and the MAC address table will be deleted. And for L3 switch, the route table will be deleted and the port state in the ARP entry will change. To prevent the switch from processing abovementioned operations when pseudo TC-BPDU messages attack maliciously, too-heavy burden and network turbulance, the TC-protection function comes into being.

Tc-protection can only be enabled or disabled globally. It is enabled by default.

Once Tc-protection is enabled, the switch will delete the message within a certain period of time (usually 4 seconds) after receiving the TC-BPDU message while monitoring the TC-BPDU message. If it receives the TC-BPDU message during this period, it will perform the delete operation again after this period expires. This eliminates the need of frequently deleting MAC address entries and ARP entries.

10.2.6 Understanding TC Guard

The Tc-Protection function can reduce the removal of MAC address entries and ARP entries when a lot number of TC messages are generated in a network. However, you need to do more delete oeprations in case of TC message attack. Furthermore, the TC message is propagated and will have an effect on the whole network. The TC Guard function allows you to disable the propagation of the TC message globally or on ports. When TC Guard function is configured

globally or on a port, the port will shield the TC messages received or produced to prevent from propagating them to other ports. In this way, this funciton can manage TC message attack in the network and maintain the network stability. Moreover, this function can prevent from interrupting core routes due to the oscillation of the devices on the access layer.

Caution

Network communication will be broken off if you use tc-guard function incorrectly.

You are recommended to enable this function when you ensure that there is illegal tc message attack in the network.

If you enable global tc-guard, then all the ports will not spread tc message. It is applicable for those devices that are accessed on the desk to enable this function.

If you enable interface tc-guard, then the topology change and tc message received on this port will not be spreaded to other ports. It is applicable for up-link ports especially aggregated ports to enable this function.

10.2.7 Understanding BPDU Source MAC Check

The gobal of the BPDU source MAC check funciton is to prevent malicious attack on the switch by sending the BPDU message manually and thus cause the MSTP protocol work abnormally. When the peer switch connected to a port in the point-to-point mode is determined, enabling the BPDU source MAC check function can receive only the BPDU message from the remote switch and discard all other BPDU messages to protect against malicious attacks. You can configure the corresponding MAC addresses for the BPDU source MAC check fucntion on a specific port in the interface mode. Only one MAC address is configured for one port. BPDU source MAC check can be disabled by using the **no bpdu src-mac-check** command. In this case, any BPDU message is received on the port.

10.2.8 Understanding Invalid Length Filtering for BPDU

When the Ethernet length field of the BPDU message exceeds 1500 bits, this BPDU message is discarded in order to avoid receiving invalid BPDU messages.

10.2.9 Understanding ROOT Guard

In network design, root bridge and backup root bridge are always divided in the same region. Due to error configuration of accendant and malicious attack in the network, it is possible that root bridge receives configuration message of higher priority and loses the current root bridge position, leading to error turbulance of network topology, which Root Guard function can prevent from occuring.

When enabling Root Guard, it enforces the port role of all the instances as specified port. Once the port receives configuration message of higher priority, Root Guard will set the interface as root-inconsistent (blocked). If there is no configuration message of higher priority during the time long enough, the port will be restored to be the original normal status.

You shall disable ROOT Guard function if this function results in the blocked status for interfaces and it needs manual configuration to restore to the normal status. You can use the command **spanning-tree guard none** in the interface configuration mode to disable Root Guard function.

Caution

1. Incorrectly using ROOT Guard leads to network link breakdown.
2. If you enable ROOT Guard on non-designated port, the non-designated port will be enforced as designated port and show BKN status(blocking status).
3. If MST0 enters BKN status because it receives configuration message of higher priority on a port, ROOT Guard will enforce the port in all the other instances to enter BKN status.
4. ROOT Guard or LOOP Guard takes effect at the same time. That is , they can not both take effect at the same time .
5. The AutoEdge function is disabled when enabling the ROOT Guard-enabled port.

10.2.10 Understanding LOOP Guard

Due to breakdown of one-way link, root port or backup port becomes designated port, being ready to forward because they can not receive BPDU, causing the loop in the network, which Loop Guard function can prevent.

For the ports configured loop guard, if they can not receive BPDU, the port roles will be migrated. However, the port state is always set as discarding till the port receive BPDU again and recalculate spanning tree.

Caution

You can enable LOOP Guard based on global or interface.

ROOT Guard or LOOP Guard takes effect at the same time. That is , they can not both take effect at the same time .

The AutoEdge function on all interfaces is ineffective when enabling LOOP Guard function globally.

The AutoEdge function on the interface is ineffective when enabling LOOP Guard function in the interface configuration mode.

10.3 Configuring MSTP

10.3.1 Default Spanning Tree Configuration

The following table lists the default configuration of the Spanning Tree protocol.

Item	Default value
Enable State	Disable
STP MODE	MSTP
STP Priority	32768
STP port Priority	128
STP port cost	Automatically determine according to port rate.
Hello Time	2 seconds
Forward-delay Time	15 seconds
Max-age Time	20 seconds
Default calculation method of the Path Cost	Long
Tx-Hold-Count	3
Link-type	Automatically determine by the duplex status of the port.
Maximum hop count	20
Corresponding relationship between vlan and instance	All VLANs belong to instance 0 Only instance 0 exists

You can restore the STP parameters to its default configuration (except for disabling STP) by using the **spanning-tree reset** command.

10.3.2 Enabling and Disabling the Spanning Tree Protocol

By default, DES-7200 series runs the MSTP protocol.

The spanning tree protocol is disabled on the device by default.

To enable the spanning tree protocol, execute the following command in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree**	Enable the spanning tree protocol.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable the spanning tree protocol, use the **no spanning-tree** command in the global configuration mode.

10.3.3 Configuring the Spanning Tree Mode

According to the 802.1-related protocols, it is not necessary for administrators to set much for three versions of the spanning tree protocols such as the STP, RSTP and MSTP. These versions are compatible with one another naturally. However, given that some manufacturers will not develop the spanning tree protocol by standards, it may cause some compatibility problem. Hence, we provide a command to facilitate administrators to switch to the lower version of the spanning tree protocol for compatibility when they detect that this device is not compatible with that of other manufacturers.

Note: When you switch to the RSTP or STP version from the MSTP version, all information about MSTP Region will be cleared.

The default mode of the device is MSTP.

To enable the spanning tree protocol, execute the following command in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.

Command	Function
DES-7200(config)# **spanning-tree mode mstp/rstp/stp**	Switch the spanning tree version.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the spanning tree mode to the default value, use the **no spanning-tree mode** command in the global configuration mode.

10.3.4 Configuring Switch Priority

Switch priority allows you to select the root and draw the topology of a network. It is recommended that administrators set the core device with higher priority (or smaller value) to facilitate the stablization of the whole network. You can assign different switch priorities for various instances so that various instances can run separate spanning tree protocol.Only the priority of CIST (Instance 0) is related to the devices between different regions.

As mentioned in Bridge ID, there are 16 values for the priority, and all of them are multiples of 4096, which are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. The default value is 32768.

To configure switch priority, execute the following command in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree** [**mst** *instance-id*] **priority** *priority*	Configure different switch priorities for different instances. This command configures the switch priority for instance 0 without the instance-id parameter. *instance-id*: ID of the instance in the range from 0 to 64. *priority*: switch priority in the range from 0 to 61440 and is increased by the integral multiple of 4096, 32768 by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.

Command	Function
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the switch priority to the default value, use the **no spanning-tree mst** *instance-id* **priority** command in the global configuration mode.

10.3.5 Configuring Port Priority

When two ports are connected to the shared media, the device will set the one of the higher priority (or smaller value) to be the forwarding status and the one of the lower priority (or larger value) to be the discarding status.If the two ports are of the same priority, the device will set the one with the smaller port number to the forwarding status. You can assign different port priorities to various instances on one port, by which various instances can run the separated spanning tree protocols.

Same as device priority, it has 16 values, all a multiple of 16. They are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240 respectively. The default value is 128.

To configure a port priority, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate Link.
DES-7200(config-if)# **spanning-tree** [**mst** *instance-id*] **port-priority** *priority*	Configure different priorities for different instances. The command without the *instance-id* parameter will configure a port priority for instance 0. *instance-id*: Interface ID in the range of 0 to 64. *priority*: Port priority of an instance in the range 0 to 240. Furthermore, it is increased by the integral multiple of 16, 128 by default.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Verify the configuration.

Command	Function
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the port priority to the default value, execute the **no spanning-tree mst** *instance-id* **port-priority** command in the interface configuration mode.

10.3.6 Configuring Path Cost of a Port

The switch determines a root port upon the total of the path costs along the path from a port to the boot bridge. The port the total of paths costs from the port to the root brdige is the smallest is elected the root port. Its default value is calculated by the media speed of the port automatically. The higher the media speed, the smaller the cost is. It is not necessary for administrators to change it for the path cost calculated in this way is most scientific. You can assign different cost paths for various instances on one port, by which various instances can run the separated spanning tree protocols.

To configure the path cost of a port, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate Link.
DES-7200(config-if)# **spanning-tree** [**mst** *instance-id*] **cost** *cost*	Configure different priorities for different instances. The command without the *instance-id* parameter will configure a port priority for instance 0. *instance-id*: Interface ID in the range of 0 to 64. *cost*: Path cost of the port in the range of 1 to 200,000,000. The default value is calculated by the media rate of the port automatically.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree** [**mst** *instance-id*] **interface** *interface-id*	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the path cost of a port to the default value, execute the **no spanning-tree mst** *cost* command in the interface configuration mode.

10.3.7 Configuring the Default Calculation Method of Path Cost (path cost method)

If the path cost of a port is the default value, the device will calculate the path cost of this port by port rate. However, IEEE 802.1d and IEEE 802.1t specify different path cost values for a port rate respectively. The value range of the 802.1d is short (1 to 65535), while the value range of the 802.1t is long (1 to 200,000,000). Administrators should unify the path cost standard of the whole network. The default mode is long (IEEE 802.1t Mode).

The following table lists the path costs set for different port rates in two standards.

Port Rate	Interface	IEEE 802.1d (short)	IEEE 802.1t (long)
10M	Common Port	100	2000000
	Aggregate Link	95	1900000
100M	Common Port	19	200000
	Aggregate Link	18	190000
1000M	Common Port	4	20000
	Aggregate Link	3	19000

To configure the default calculation method of path cost, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree pathcost method long/short**	Configure the default calculation method of the port path cost as long or short, with long by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the setting to the default value, execute the **no spanning-tree pathcost** method command in the global configuration mode.

10.3.8 Configuring Hello Time

Configure the interval of sending the BPDU message. The default value is 2s.

To configure the Hello Time, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree hello-time** *seconds*	Configure the hello time ranging from 1 to 10s, 2s by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the hello time to the default value, execute the **no spanning-tree hello-time** command in the global configuration mode.

10.3.9 Configuring Forward-Delay Time

Configure the interval for changing port status. The default value is 15s.

To configure the forward-delay time, execute the following commands in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree forward-time** *seconds*	Configure the forward delay time ranging from 4 to 30s, 15s by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the forward-delay time to the default value, execute the **no spanning-tree forward-time** command in the global configuration mode.

10.3.10 Configuring Max-Age Time

Configure the maximum period of time before the BPDU message is aged out. The default value is 20s.

In the privilege mode, perform these steps to configure the Max-Age Time:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree max-age** *seconds*	Configure the max age time ranging from 6 to 40s, 20s by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the max age time to the default value, execute the **no spanning-tree max-age** command in the global configuration mode.

Caution

Hello Time, Forward-Delay Time and Max-Age Time have their own value ranges. Meanwhile, the following condition must be addressed: 2*(Hello Time + 1.0 seconds) <= Max-Age Time <= 2*(Forward-Delay – 1.0 second). Otherwise, it may cause the topology instability

10.3.11 Configuring Tx-Hold-Count

Configure the maximum number of the BPDU message sent per second, 3 by default.

To configure the Tx-Hold-Count, execute the following commands in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree tx-hold-count** *numbers*	Configure the maximum number of the BPDU message sent per second in the range of 1 to10, 3 by default.

Command	Function
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the Tx-Hold-Count to the default value, execute the **no spanning-tree tx-hold-count** command in the global configuration mode.

10.3.12 Configuring Link-type

Configure the link-type of a port. This is crucial for rapid RSTP convergence. For details, refer to Rapid RSTP Convergence. Without configuration, the device will set the link type of a port according to its duplex status automatically, with point-to-point for the full duplex port and shared for the half duplex port.

To configure the link type of a port, execute the following commands in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **spanning-tree link-type point-to-point/shared**	Configure the link type of the interface, with point-to-point for the full duplex port and shared for the half duplex port. Point-to-point indicates the rapid forwarding is enabled on the port.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the link type of a port to the default value, execute the **no spanning-tree link-type** command in the interface configuration mode.

10.3.13 Configuring Protocol Migration Processing

This command is to check the version globally or on individual port. For related information, refer to Compatibility of RSTP and STP.

Command	Function
DES-7200# **clear spanning-tree detected-protocols**	Forcibly check the version on all ports.
DES-7200# **clear spanning-tree detected-protocols interface** *interface-id*	Check the version forcibly on the port.

10.3.14 Configuring a MSTP Region

To deploy several devices in the same MSTP Region, you have to configure these devices with the same name, the same revision number, and the same Instance-VLAN table.

You can assign a VLAN to instances 0 to 64 respectively as required. The remaining VLANs will be automatically assigned to instance 0. One vlan can only be of an instance.

It is recommended to configure the Instance-VLAN table when the MSTP protocol is disabled. After configuration, you should enable the MSTP protocol again to ensure the stability and convergence of the network topology.

To configure a MSTP region, execute the following commands in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree mst configuration**	Enter the MST configuration mode.
DES-7200(config-mst)# **instance** *instance-id* **vlan** *vlan-range*	Add a VLAN group to a MST instance. *instance-id*: Instance ID ranging from 0 to 64. *vlan-range:* VLAN range in the range 1 to 4094. For instance: The **instance 1 vlan 2-200** command is to add VLAN 2-200 to instance 1.

Command	Function
	The **instance 1 vlan 2,20,200** command is to add VLAN 2, VLAN 20 and VLAN 200 to instance 1. You can use the **no** option of this command to delete a VLAN from an instance, and the deleted VLAN will be added to instance 0 automatically.
DES-7200(config-mst)# **name** *name*	Specify the MST configuration name, a string of up to 32 bytes.
DES-7200(config-mst)# **revision** *version*	Specify the MST revision number in the range 0 to 65535. The default value is 0.
DES-7200(config-mst)# **show**	Verify the configuration.
DES-7200(config-mst)# **end**	Return to the privileged EXEC mode.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the MST region configuration to the default value, execute the **no spanning-tree mst configuration** command in the global configuration mode. You can use the **no instance** *instance-id* command to delete an instance. Similarly, the **no name** and **no revision** commands can be used to restore the MST name and MST revision number settings to the default value, respectively.

The following is the example of configuration:

```
DES-7200(config)# spanning-tree mst configuration
DES-7200(config-mst)# instance 1 vlan 10-20
DES-7200(config-mst)# name region1
DES-7200(config-mst)# revision 1
DES-7200(config-mst)# show
Multi spanning tree protocol : Enable Name [region1]
Revision 1
Instance Vlans Mapped
-------- --------------------
0 1-9,21-4094
1 10-20
------------------------------
DES-7200(config-mst)# exit
DES-7200(config)#
```

Caution

Before configuring vlan and instance mapping relationship, please ensure that all configured VLANs have been created. Otherwise, the association of vlan and instance on part of the products may be failed.

10.3.15 Configuring Maximum-Hop Count

Maximum-Hop Count means how many devices the BPDU message will pass through in a MSTP region before being discarded. This parameter takes effect for all instances.

To configure the Maximum-Hop Count, execute the following commands in the global configuraiton mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree max-hops** *hop-count*	Configure the Maximum-Hop Count ranging from 1 to 40, 20 by default.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To restore the Maxium-Hop Count to the default value, execute the **no spanning-tree max-hops** command in the global configuration mode.

10.3.16 Configuring Intereface Compatibility Mode

In interface compatibility mode, when a port sends BPDU, it will carry different MSTI information according to the current port attribute to realize interconnection with other vendors.

To configure the interface compatibility mode, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)**#interface** *interface-id*	Enter the Interface configuration mode.
DES-7200(config-if)# **spanning-tree compatible enable**	Enable interface compatibility mode.

DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show running-config**	Check configuration items.
DES-7200# **copy running-config startup-config**	Save the configuration.

To remove the settings, you can execute command **no spanning-tree compatible enable.**

10.4 Configuring Optional MSTP Features

10.4.1 Default Setting of Optional Spanning Tree Features

All the optional features are disabled by default, except for AutoEdge function.

10.4.2 Enabling Port Fast

Enabling Port Fast lets a port directly forward the BPDU message. When Port Fast is disabled due to the receipt of the BPDU message, the port will participate in the STP algorithm and forward the BPDU message normally.

To enable Port Fast, execute the following commands in the global configuraiton mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an Aggregate Link.
DES-7200(config-if)# **spanning-tree Portfast**	Enable Port Fast on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.

Command	Function
DES-7200# **show spanning-tree interface** *interface-id* **portfast**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable Port Fast, execute the **spanning-tree portfast disable** command in the interface configuration mode.

You can use the **spanning-tree portfast default** command in the global configuration mode to enable Port Fast on all ports.

10.4.3 Disabling AutoEdge

If the designated port does not receive any BPDU messages within 3 seconds, it is identified as the edge port automatically. However, Port Fast Operational State is disabled if the AutoEdge port receives BPDU messages. AutoEdge is enabled by default.

To disable AutoEdge, execute the following commands in the global configuraiton mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an Aggregate Link.
DES-7200(config-if)# **spanning-tree autoedge**	Enable AutoEdge on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show spanning-tree interface** *interface-id* **portfast**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable AutoEdge, execute the **spanning-tree autoedge disable** command in the interface configuration mode.

10.4.4 Enabling BPDU Guard

After BPDU Guard is enabled, a port will in the error-disabled status after receiving the BPDU packet.

To configure the BPDU guard, execute the following commands in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree portfast Bpduguard default**	Enable the BPDU Guard globally.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate link.
DES-7200(config-if)# **spanning-tree portfast**	Enable Port Fast on the interface before the bpduguard configuration takes effect globally.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable BPDU Guard, execute the **no spanning-tree portfast bpduguard default** command in the global configuration command.

To enable or disable BPDU Guard on an interface, execute the **spanning-tree bpduguard enable** command or the **spanning-tree bpduguard disable** command on the interface respectively.

10.4.5 Enabling BPDU Filter

A port neither transmit nor receive the BPDU message after the BPDU filter is enabled.

To configure the BPDU Filter, execute the following commands in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.

Command	Function
DES-7200(config)# **spanning-tree portfast bpdufilter default**	Enable BPDU filter globally.
DES-7200(config)# **interface** *Interface-id*	Enter the interface configuration mode. A legal interface contains a physical port and an aggregate link.
DES-7200(config-if)# **spanning-tree Portfast**	Enable portfast on this interface before the bpduguard configuration takes effect globally.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable BPDU Filter, execute the **no spanning-tree portfast bpdufilter default** command in the global configuration mode.

To enable or disable BPDU Filter on an interface, execute the **spanning-tree bpdufilter enable** command or the **spanning-tree bpdufilter disable** command in the interface configuration mode.

10.4.6 Enabling Tc_Protection

To configure Tc_Protection, execute the following commands in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree tc-protection**	Enable Tc-Protection
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable Tc_Protection, execute the **no spanning-tree tc-protection** command in the global configuration mode.

10.4.7 Enabling TC Guard

To enable TC Guard globally, execute the following commands in the global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **spanning-tree tc-protection tc-guard**	Enable TC Guard globally.
DES-7200(config)# **end**	Return to the privileged EXEC mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To configure TC Guard on an interface, execute the following commands in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *Interface-id*	Enter the interface configuration mode. A legal interface includes a physical port and an aggregate link.
DES-7200(config-if)# **spanning-tree tc-guard**	Enable TC Guard on this interface.
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

10.4.8 Enable BPDU Source MAC check

After the BPDU source MAC check is enabled, the switch accepts only the BPDU message from the specified MAC address.

To configure the BPDU source MAC check, execute the following commands in the interface configuration mode:

Command	Function

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode. A legal interface includes a physical port and an aggregate link.
DES-7200(config-if)#**bpdu src-mac-check** H.H.H	Enable BPDU source MAC check.
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To disable BPDU source MAC check, execute the **no bpdu src-mac-check** command in the interface mode.

10.4.9 Enabing Root Guard

To configure interface ROOT Guard, execute the following commands in the privileged mode:

Command	**Function**
DES-7200# **configure terminal**	Enter the global configuration mode,
DES-7200(config)**#interface** *interface-id*	Enter the interface configuration mode.Valid interface includes physical port and Aggregate Link.
DES-7200(config-if)**#spanning-tree guard root**	Enable interface ROOT Guard.
DES-7200(config-if)**# end**	Return to the privileged mode.
DES-7200**#show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

10.4.10 Enabling Loop Guard

To configure global LOOP Guard, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode,
DES-7200(config)#**spanning-tree loopguard default**	Enable global LOOP Guard.
DES-7200(config)# **end**	Return to the privileged mode.
DES-7200#**show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

To configure interface LOOP Guard, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *Interface-id*	Enter the interface configuration mode. Valid interface includes physical port and Aggregate Link.
DES-7200(config-if)#**spanning-tree guard loop**	Enable interface Loop Guard.
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

10.4.11 Disabling Interface Guard

To disable interface ROOT or LOOP Guard, execute the following commands in the privileged mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode,
DES-7200(config)# **interface** *Interface-id*	Enter the interface configuration mode.Valid interface includes physical port and Aggregate Link.
DES-7200(config-if)#**spanning-tree guard none**	Disable interface Loop Guard.
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show running-config**	Verify the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

10.5 Showing MSTP Configuration and Status

You can use the following show commands to view the configuration of MSTP:

Command	Meaning
DES-7200# **show spanning-tree**	Show the information on the parameters and topology of MSTP.
DES-7200# **show spanning-tree summary**	Show the information on various instances and port forwarding status of MSTP.
DES-7200# **show spanning-tree inconsistentports**	Show the block port due to root guard or loop guard.
DES-7200# **show spanning-tree mst Configuration**	Show the configuration information of the MST region.
DES-7200# **show spanning-tree mst** *instance-id*	Show the MSTP information of an instance.

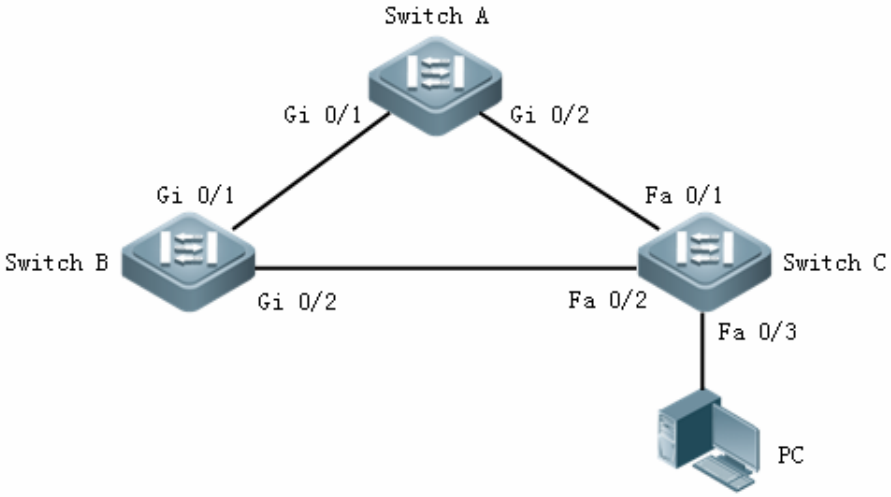
Command	Meaning
DES-7200# **show spanning-tree mst** *instance-id* **interface** *interface-id*	Show the MSTP information of the specified instance of the interface.
DES-7200# **show spanning-tree interface** *interface-id*	Show the MSTP information of all the instances of the interface.
DES-7200# **show spanning-tree forward-time**	Show forward-time.
DES-7200# **show spanning-tree Hello Time**	Show Hello time.
DES-7200# **show spanning-tree max-hops**	Show max-hops.
DES-7200# **show spanning-tree tx-hold-count**	Show tx-hold-count.
DES-7200# **show spanning-tree pathcost Method**	Show pathcost method.

10.6 MSTP Configuration Example

10.6.1 Configuration Purpose

1. Interconnect three switches to construct a triangle ring network and MSTP configuration mode.
2. Set the corresponding VLAN-INSTANCE mapping, MST configuration name, MST Revision Number and the instance priority on the switches.
3. View the MSTP configurations.
4. Enable BPDU Guard function globally and set PortFast function on the port connecting to the PC directly.

10.6.2 Topology



10.6.3 Configuration Steps

1) **Configuring Switch A**

Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
DES-7200# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)# interface gigabitEthernet 0/1

DES-7200(config-if)# switchport mode trunk
```

```
DES-7200(config-if)# exit

DES-7200(config)# interface gigabitEthernet 0/2

DES-7200(config-if)# switchport mode trunk

DES-7200(config-if)# exit

DES-7200(config)# vlan 2

DES-7200(config-vlan)# exit

DES-7200(config)# vlan 3

DES-7200(config-vlan)# exit
```

Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to DES-7200, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
DES-7200(config)# spanning-tree mode mstp

DES-7200(config)# spanning-tree mst configuration

DES-7200(config-mst)# instance 1 vlan 2

%Warning:you must create vlans before configuring instance-vlan relationship

DES-7200(config-mst)# instance 2 vlan 3

%Warning:you must create vlans before configuring instance-vlan relationship

DES-7200(config-mst)# name DES-7200

DES-7200(config-mst)# revision 1

DES-7200(config-mst)# show

Multi spanning tree protocol : Enable

Name    : DES-7200

Revision : 1

Instance  Vlans Mapped

-------- ---------------------------------------------

0       : 1, 4-4094

1       : 2

2       : 3

---------------------------------------------------

DES-7200(config-mst)# exit
```

```
DES-7200(config)# spanning-tree

Enable spanning-tree.
```

Set the priority for Instance 0 to 4096

```
DES-7200(config)# spanning-tree mst 0 priority 4096
```

2) **Configuring Switch B**

Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
DES-7200(config)# interface gigabitEthernet 0/1

DES-7200(config-if)# switchport mode trunk

DES-7200(config-if)# exit

DES-7200(config)# interface gigabitEthernet 0/2

DES-7200(config-if)# switchport mode trunk

DES-7200(config-if)# exit

DES-7200(config)# vlan 2

DES-7200(config-vlan)# exit

DES-7200(config)# vlan 3

DES-7200(config-vlan)# exit
```

Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to DES-7200, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
DES-7200(config)# spanning-tree mode mstp

DES-7200(config)# spanning-tree mst configuration

DES-7200(config-mst)# instance 1 vlan 2

%Warning:you must create vlans before configuring instance-vlan relationship

DES-7200(config-mst)# instance 2 vlan 3

%Warning:you must create vlans before configuring instance-vlan relationship

DES-7200(config-mst)# name DES-7200

DES-7200(config-mst)# revision 1

DES-7200(config-mst)# exit

DES-7200(config)# spanning-tree

Enable spanning-tree.
```

Set the priority for Instance 0 to 4096

```
DES-7200(config)# spanning-tree mst 1 priority 4096
```

3) **Configuring Switch C**

Set interface Gi0/1 and Gi 0/2 as Trunk port and create VLAN 2 and VLAN 3

```
DES-7200(config)# interface fastEthernet 0/1

DES-7200(config-if)# switchport mode trunk

DES-7200(config-if)# exit

DES-7200(config)# interface fastEthernet 0/2

DES-7200(config-if)# switchport mode trunk

DES-7200(config-if)# exit

DES-7200(config)# vlan 2

DES-7200(config-vlan)# exit

DES-7200(config)# vlan 3

DES-7200(config-vlan)# exit
```

Set the spanning tree to MSTP mode, VLAN 2-Instance 1 and VLAN 3-Instance 2 mapping, and set the MST configuration name to DES-7200, MST Revision Number to 1. View the MST configurations and enable the spanning tree protocol.

```
DES-7200(config)# spanning-tree mode mstp

DES-7200(config)# spanning-tree mst configuration

DES-7200(config-mst)# instance 1 vlan 2

%Warning:you must create vlans before configuring instance-vlan relationship

DES-7200(config-mst)# instance 2 vlan 3

%Warning:you must create vlans before configuring instance-vlan relationship

DES-7200(config-mst)# name DES-7200

DES-7200(config-mst)# revision 1

DES-7200(config-mst)# exit

DES-7200(config)# spanning-tree

Enable spanning-tree.
```

Set the highest priority for Instance 2

```
DES-7200(config)# spanning-tree mst 2 priority 4096
```

Enable BPDU Guard function globally and set the interface Fa 0/3 to Port Fast-enabled port.

```
DES-7200(config)# spanning-tree portfast bpduguard default

DES-7200(config)# interface fastEthernet 0/3

DES-7200(config-if)#spanning-tree portfast

%Warning: portfast should only be enabled on ports connected to a single host.
Connecting hubs, DES-7200es, bridges to this interface when portfast is enabled,can
cause temporary loops.

DES-7200(config-if)# end
```

View the spanning tree configurations

```
DES-7200# show spanning-tree

StpVersion : MSTP

SysStpStatus : ENABLED

MaxAge : 20

HelloTime : 2

ForwardDelay : 15

BridgeMaxAge : 20

BridgeHelloTime : 2

BridgeForwardDelay : 15

MaxHops: 20

TxHoldCount : 3

PathCostMethod : Long

BPDUGuard : enabled

BPDUFilter : Disabled

LoopGuardDef  : Disabled

###### mst 0 vlans map : 1, 4-4094

BridgeAddr : 00d0.f82a.aa8e

Priority: 32768

TimeSinceTopologyChange : 0d:0h:19m:44s

TopologyChanges : 1

DesignatedRoot : 1000.00d0.f822.33aa
```

```
RootCost : 0

RootPort : 1

CistRegionRoot : 1000.00d0.f822.33aa

CistPathCost : 200000

###### mst 1 vlans map : 2

BridgeAddr : 00d0.f82a.aa8e

Priority: 32768

TimeSinceTopologyChange : 0d:0h:1m:46s

TopologyChanges : 7

DesignatedRoot : 1001.00d0.f834.56f0

RootCost : 200000

RootPort : 2

###### mst 2 vlans map : 3

BridgeAddr : 00d0.f82a.aa8e

Priority: 4096

TimeSinceTopologyChange : 0d:0h:1m:44s

TopologyChanges : 5

DesignatedRoot : 1002.00d0.f82a.aa8e

RootCost : 0

RootPort : 0
```

View the spanning tree configurations on the interface Fa 0/1

```
DES-7200# show spanning-tree interface fastEthernet 0/1

PortAdminPortFast : Disabled

PortOperPortFast : Disabled

PortAdminAutoEdge : Enabled

PortOperAutoEdge : Disabled

PortAdminLinkType : auto

PortOperLinkType : point-to-point

PortBPDUGuard : Disabled

PortBPDUFilter : Disabled
```

```
PortGuardmode  : None

###### MST 0 vlans mapped :1, 4-4094

PortState : forwarding

PortPriority : 128

PortDesignatedRoot : 1000.00d0.f822.33aa

PortDesignatedCost : 0

PortDesignatedBridge :1000.00d0.f822.33aa

PortDesignatedPort : 8002

PortForwardTransitions : 1

PortAdminPathCost : 200000

PortOperPathCost : 200000

Inconsistent states : normal

PortRole : rootPort

###### MST 1 vlans mapped :2

PortState : discarding

PortPriority : 128

PortDesignatedRoot : 1001.00d0.f834.56f0

PortDesignatedCost : 0

PortDesignatedBridge :8001.00d0.f822.33aa

PortDesignatedPort : 8002

PortForwardTransitions : 5

PortAdminPathCost : 200000

PortOperPathCost : 200000

Inconsistent states : normal

PortRole : alternatePort

###### MST 2 vlans mapped :3

PortState : forwarding

PortPriority : 128

PortDesignatedRoot : 1002.00d0.f82a.aa8e

PortDesignatedCost : 0
```

```
PortDesignatedBridge :1002.00d0.f82a.aa8e

PortDesignatedPort : 8001

PortForwardTransitions : 1

PortAdminPathCost : 200000

PortOperPathCost : 200000

Inconsistent states : normal

PortRole : designatedPort
```

11 GVRP Configuration

11.1 Overview

GVRP (GARP VLAN Registration Protocol) is a GARP (Generic Attribute Registration Protocol) application that dynamically configures and propagates VLAN membership.

Through GVRP protocol, the device can:

- Listen to GVRP PDUs on each port, learn the VLAN information registered on GVRP-aware devices connected according to such GVRP PDUs, and then configure VLAN members on the port receiving GVRP PDUs.
- Propagate VLAN information on each port by sending GVRP PDUs. The VLAN information propagated includes the statically configured VLANs and those learned from other devices via GVRP.

Through GVRP, devices on the switching network can dynamically create VLAN and maintain the consistency of VLAN configurations in a real-time manner. Through automatic declaration of VLAN ID within the network, GVRP well reduces the possibility of faults caused by inconsistent configurations. In case of any change in the VLAN configurations on a device, GVRP can automatically change the VLAN configurations on the connected devices, thus reducing manual configuration works to be done by the user.

GARP and GVRP are defined in the following standards:

- IEEE standard 802.1D
- IEEE standard 802.1Q

11.2 Configure GVRP

11.2.1 Default Configurations

The following table shows the default configurations of GVRP:

Function	Default setting
GVRP global enable state	Disabled
GVRP dynamic creation of VLANs	Disabled

GVRP base vlan id	VLAN 1 (only effective under MSTP environment)
GVRP registration mode	Enable
GVRP applicant state	Normal, (Ports do not declare VLANs when in STP blocking state)
GVRP timers	Join Time: 200 ms Leave Time: 600 ms Leaveall Time: 10,000 ms

11.2.2 GVRP Configuration Guidelines

- GVRP must be enabled on two interconnected devices. GVRP information will only be propagated on Trunk Links, and the information propagated includes all VLANs on the current device, no matter they are dynamically learned or manually configured.
- When running STP (Spanning-tree Protocol), only ports in "Forwarding" state will be GVRP participants (receiving and sending GVRP PDUs); only ports in "Forwarding" state will have their VLAN information propagated by GVRP.
- All VLAN Ports added by GVRP are Tagged Ports.
- All VLAN information dynamically learned by GVRP will not be saved in the system. It means that such information will be lost after the device resets. The user cannot save such dynamically learned VLAN information.
- The user cannot change the parameters of dynamic VLANs created by GVRP.
- All devices requiring exchanging GVRP information must have consistent GVRP Timers (Join, Leave, Leaveall).

11.2.3 Enable GVRP

You must enable GVRP globally before running GVRP.

When GVRP is not enabled globally, you can configure other GVRP parameters, but these GVRP configurations will only take effect after running GVRP.

Enable GVRP globally:

Command	Function
DES-7200(config)**# [no] gvrp enable**	Enable GVRP (if it is disabled)

Configuration example:

```
DES-7200# configure
Enter configuration commands, one per line. End with CNTL/Z.
```

```
DES-7200(config)# gvrp enable
DES-7200(config)# end
```

11.2.4 Enable Dynamic VLAN Creation

When a port receives messages (limited only to Joinin Joinempty) indicating a VLAN which doesn't exist on the local device, GVRP may create this VLAN. The user can control whether or not to create VLAN dynamically.

Enable dynamic VLAN creation:

Command	Function
DES-7200(config)# [**no**] **gvrp dymanic-vlan-creation enable**	Enable GVRP to create VLAN dynamically (if it is disabled)

The user cannot change the parameters of dynamic VLANs created by GVRP.

Configuration example:

```
DES-7200# configure
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# gvrp dymanic-vlan-creation enable
DES-7200(config)# end
```

11.2.5 Configure the GVRP VLAN

In the context without STP (Spanning-tree protocol), all available ports can be GVRP participants.

In the context with SST (Single Spanning-tree), only ports showing "Forwarding" state in the current SST Context can be GVRP participants. In the context with MST (Multiple Spanning-tree), GVRP can run in the Spanning-tree Context which VLAN 1 is affiliated with, and the user cannot specify other Spanning-tree Contexts.

11.2.6 Configure Port Registration Mode

There are two port registration modes:

- GVRP Registration Normal
- GVRP Registration Disabled

Configuring a port in **normal registration** mode allows dynamic creation (if dynamic VLAN creation is enabled), registration, and deregistration of VLANs on the port.

When a port is configured to "disabled registration" mode, no dynamic VLAN registration or deregistration will be allowed.

Configure GVRP Registration Mode of port:

Command	Function
DES-7200(config-if)# [**no**] **gvrp registration mode** {**normal** | **disabled**}	Configure GVRP registration mode of the port

These two registration modes will not affect static VLANs on the port. The static VLANs created by the user are always "Fixed Registrar".

Example of enabling Registration Mode on port 1:

```
DES-7200# configure
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# gvrp registration mode enable normal
DES-7200(config-if)# end
```

11.2.7 Configure Port Declaration Mode

There are two declaration modes to control whether the port will send GVRP declarations.

- GVRP Normal Applicant

Allowing the declaration of VLANs on the port, including all dynamic and static VLANs.

- GVRP Non-Applicant

Prohibiting the declaration of VLANs on the port.

Configure declaration mode of the port:

Command	Function
DES-7200(config-if)# [**no**] **gvrp applicant state** {**normal** | **non-applicant**}	Configure GVRP declaration mode of the port

Example of configuring Applicant Mode on port 1:

```
DES-7200# configure
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# gvrp applicant state normal
DES-7200(config-if)# end
```

11.2.8 Configure GVRP Timers

GVRP uses three timers:

1. Join Timer

Join timer controls the maximum latency before the port sends declaration, and the actual sending interval will range between 0 and this maximum latency. The default value is 200ms.

2. Leave Timer

Leave Timer controls the time required to delete port from VLAN after receiving the Leave Message. If the port receives Join Message again during this period, then the port will maintain VLAN membership, and the timer become void. If the port doesn't receive Join Message before the timer runs out, then the port will be deleted from the VLAN membership table. The default value is 600ms.

3. LeaveAll Timer

LeaveAll Timer controls the minimum interval to send LeaveAll Message on the port. If the port receives LeaveAll Message before the timer runs out, then the timer will start timing again; if the timer runs out, it will send LeaveAll Message on the port and to the port as well, thus triggering the Leave Timer. The default value is 10,000ms. The actual sending interval ranges between Leaveall and Leaveall+Join.

Caution

When configuring the timer, make sure Leave Value is greater than or equal to three times the Join Value (Leave >= Join *3). Meanwhile, Leaveall must be greater than Leave (Leaveall > Leave). If the aforementioned conditions cannot be met, the timer configuration may fail. For example, after setting Leave Timer to 600ms, the system may prompt an error if you configure Join Timer to 320ms. To achieve successful configuration, when Join Timer is set to 350ms, the Leave Timer must be greater than 1050ms.

The effective size for timer configuration is 10ms.

Make sure all interconnected GVRP devices use the same GVRP Timer configurations, or else the GVRP may not function well.

Adjust the value of GVRP Timer:

Command	Function
DES-7200(config)# [**no**] **gvrp timer** {**join** | **leave** | **leaveall**} *timer-value*	Set the timer value of port

Example of setting GVRP Join Timer:

```
DES-7200# configure
Enter configuration commands, one per line. End with CNTL/Z.
```

```
DES-7200(config)# gvrp timer join 1000
DES-7200(config)# end
```

11.3 Display the GVRP Configurations

11.3.1 Display GVRP Statistics

GVRP statistics are calculated by port. For details about how to use the command to display statistics and the meaning of each statistical value, please refer to the command of "**show gvrp statistics**".

Display the GVRP statistics for the port:

Command	Function
DES-7200# **show gvrp statistics** {*interface-id* | **all**}	Display statistics for the port

Example of displaying GVRP statistics:

```
DES-7200# show gvrp statistics gigabitethernet 1/1
Interface  GigabitEthernet 3/1
RecValidGvrpPdu   0
RecInvalidGvrpPdu  0
RecJoinEmpty   0
RecJoinIn      0
RecEmpty       0
RecLeaveEmpty  0
RecLeaveIn     0
RecLeaveAll    0
SentGvrpPdu    0
SentJoinEmpty  0
SentJoinIn     0
SentEmpty      0
SentLeaveEmpty  0
SentLeaveIn    0
SentLeaveAll   0
JoinIndicated  0
LeaveIndicated  0
JoinPropagated  0
LeavePropagated  0
```

To clear all GVRP statistics so that it will restart calculation:

Command	Function
DES-7200# **clear gvrp statistics** {*interface-id* | **all**}	Clear all statistics for the port

Example of clearing GVRP statistics for port 1:

```
DES-7200# clear gvrp statistics gigabitethernet 1/1
```

11.3.2 Display GVRP status

Execute "**show gvrp status**" command to display the current GVRP status. This command can be used to display the dynamic ports of dynamically created VLANs and static VLANs.

Command	Function
DES-7200# **show gvrp status**	Display current GVRP status

Configuration example:

```
DES-7200# show gvrp status
VLAN 1
Dynamic Ports:
DVLAN 5
Dynamic Ports:
Port:GigabitEthernet 3/1
```

11.3.3 Display Current GVRP Configurations

Execute "**show gvrp configuration**" command to display the current GVRP status. This command can be used to display the dynamic ports of dynamically created VLANs and static VLANs.

Command	Function
DES-7200# **show gvrp configuration**	Display current GVRP configurations

Configuration example:

```
DES-7200# show gvrp configuration
Global GVRP Configuration:
GVRP Feature:enabled
GVRP dynamic VLAN creation:enabled
Join Timers(ms):200
```

```
Join Timers(ms):600
Join Timers(ms):10000
Port based GVRP Configuration:
Port:GigabitEthernet 3/1 app mode:normal reg mode:normal
Port:GigabitEthernet 3/2 app mode:normal reg mode:normal
Port:GigabitEthernet 3/3 app mode:normal reg mode:normal
Port:GigabitEthernet 3/4 app mode:normal reg mode:normal
Port:GigabitEthernet 3/5 app mode:normal reg mode:normal
Port:GigabitEthernet 3/6 app mode:normal reg mode:normal
Port:GigabitEthernet 3/7 app mode:normal reg mode:normal
Port:GigabitEthernet 3/8 app mode:normal reg mode:normal
Port:GigabitEthernet 3/9 app mode:normal reg mode:normal
Port:GigabitEthernet 3/10 app mode:normal reg mode:normal
Port:GigabitEthernet 3/11 app mode:normal reg mode:normal
Port:GigabitEthernet 3/12 app mode:normal reg mode:normal
```

12 QinQ Configuration

12.1 Introduction to QinQ

For QinQ, as specified in IEEE 802.1ad, there are so many names in the industry, for instance, dot1q-tunneling, Tag in Tag, VLAN VPN and Stack VLAN. Since the VLAN Tag domain defined in IEEE 802.1Q has only 12 bits for VLAN ID, the device supports up to 4094 VLANs. In real applicatioin environments, for example, especially in MAN, a lot number of VLANs are necessary for separation of users. 4094 VLANs is not enough to address this requirement. The principle of QinQ is that a packet is encapsulated with the VLAN tag of the network of an ISP before arriving the network and the original VLAN tag iin the packet serves as data, so that the packet travels the network with two tags. The packet is propagated in the ISP's network by outer VLAN tag (or the VLAN tag of ISP's network), which is stripped when the packet leaves. Then the packet is propagated in the private network by the VLAN tag of the private network.

As shown in Figure 1, the packets from Network A's VLAN 1001 are added with the outer VLAN tag 1005 before entering the ISP's network. Hence, the packets carry with two tags and be propagated in the ISP's network by the outer VLAN tag 1005. The outer VLAN tag 1005 will be stripped when the pakcets leave the ISP's network. In Network B, the packets are propagated by VLAN tag 1001.

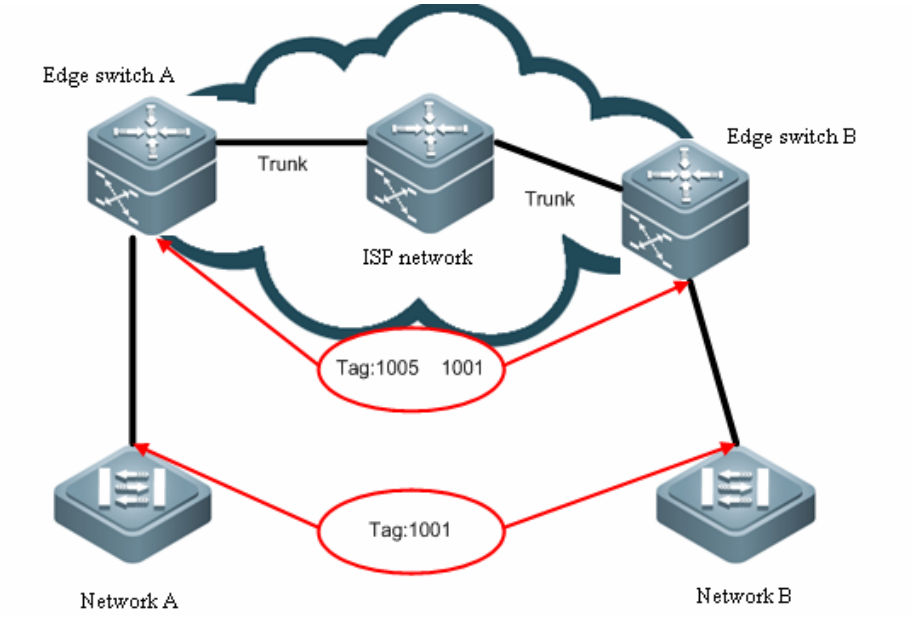
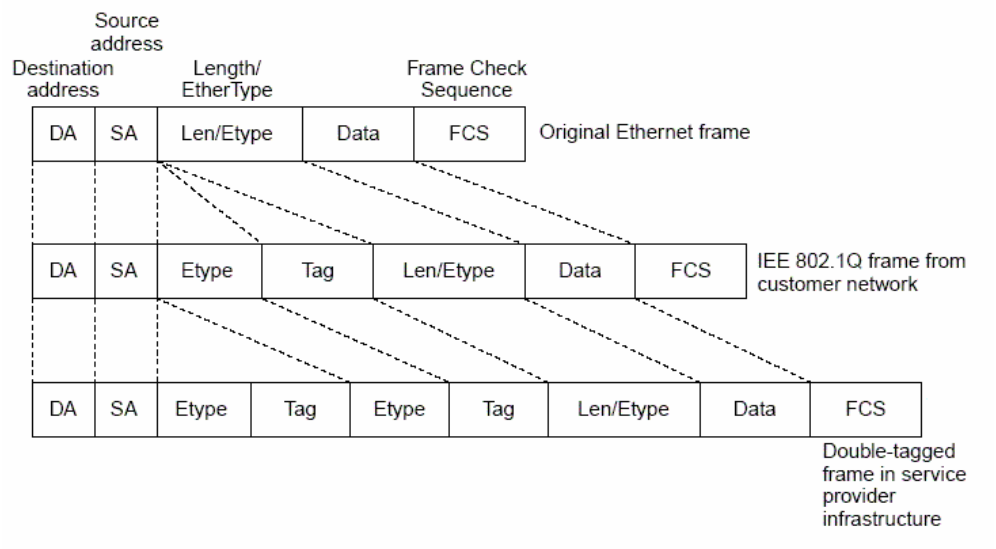


Figure 1 QinQ sketch map

The following figure illustrates the course of adding two tags. The ingress of edge device is dot1q-tunnle port (or abbreviated as tunnel port). All frames entering the edge device are considered to be untagged, no matter wheter are really untagged or tagged with 802.1Q tag, and then are encapsulated with the tag of ISP. VLAN ID is the default VLAN of tunnle port.



Fiugre 2 Packet structure with two tags

12.1.1 Basic QinQ

Basic QinQ is enabled based on port. When tunnel port is configured, the device will add the VLAN tag of the default VLAN of the tunnel port to the packet arriving the tunnel port. If the packet is already of a VLAN tag, this means it has two tags. Basic QinQ is simple, but the encapsulation of outer VLAN tag is not flexible enough.

12.1.2 Flexible QinQ

Flexible QinQ can flexibly encapsulate different outer VLAN tags for different flows by flow classification method like user VLAN tag, MAC address, IP protocol, source address, destination address, priority or port number of application program.

You can:

- Add outer VLAN tag by inner VLAN tag
- Modify inner VLAN tag by outer VLAN tag
- Modify outer VLAN tag by inner VLAN tag
- Add outer VLAN tag by ACL
- Modify outer VLAN tag by ACL

- Modify inner VLAN tag by ACL

12.1.3 Other functions

- TPID setting and priority duplication and mapping
- MAC address duplication
- Layer 2 protocol transparent transmission
- Uplink port

12.1.3.1 TPID setting and priority duplication and mapping

The Ethernet frame tag includes four fields-TPID (Tag Protocol Identifier), User Priority, CFI and VLAN ID. By default, TPID uses 0x8100 specified in IEEE 802.1Q. Some vendors' devices, however, set the TPID of the outer tag of packes to 0x9100 or other values. To compatible with these devices, QinQ offers the function to configure the TPID of packets based on port. In the course of packet transmission, the TPID of the outer VLAN tag of packets are replaced with the set value.

Priority duplication refers to duplicating the priority of inner tag (user tag) to outer tag (ISP tag) when adding outer tag.

Priority mapping refers to setting the priority of outer tag (ISP tag) by inner tag (user tag) when adding outer tag.

12.1.3.2 MAC address duplication

For flow-based flexible QinQ, the switch learns VID of native VLAN. Hence, in case of flow-based VLAN translation, when the peer sends back packets, flooding may occur for the MAC address cannot be obtained.

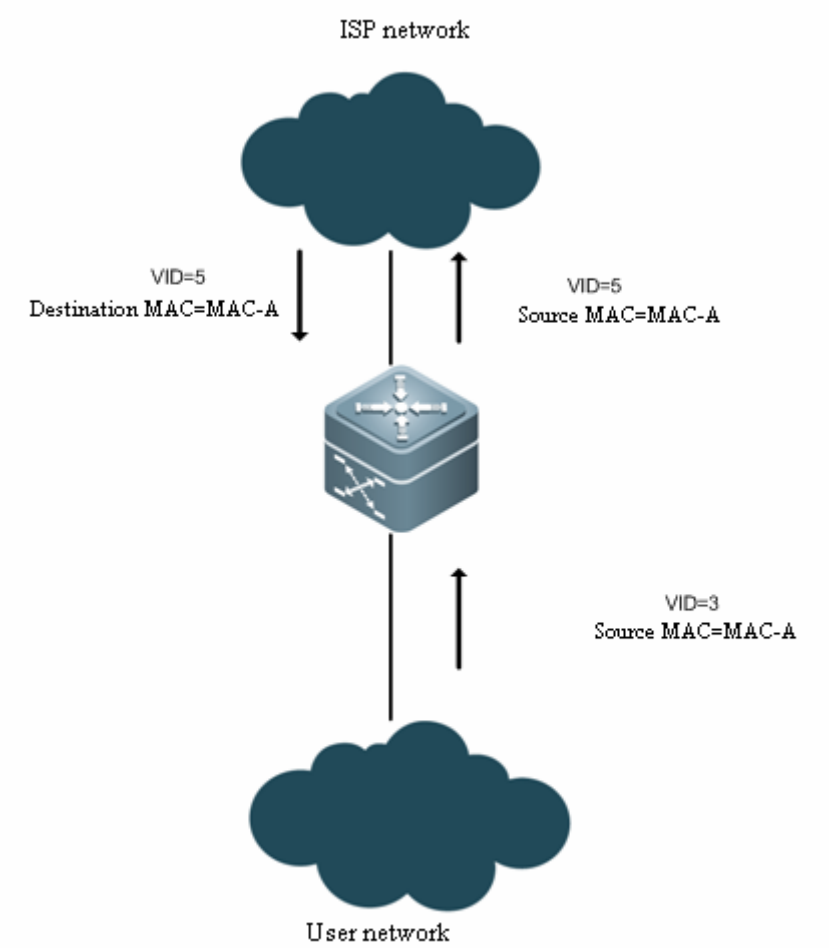


Figure 3 Learn MAC address of flexible QinQ packet

As shown in the above figure, the switch connects to user network through dot1q-tunnel port, on which VLAN 4 is set to be native VLAN. The packets of VLAN 3 are encapsualted with VLAN 5 tag as outer tag. When the switch receives a parcket from VLAN 3, it adds VLAN 5 tag as outer tag to the packet. Meanwhile, VLAN 4 learns MAC-A for the native VLAN of the receiving port is VLAN 4. Howover, VLAN 5 has not learned MAC-A and the packet is flooded.

To solve the problem on flooding the packets back from the public network, duplicate the MAC address of native VLAN to the VLAN whether outer tag locates. Similarly, you can execute reverse MAC address duplication to solve the problem on flooding the packets to the public network.

12.1.3.3 Layer 2 protocol transparent transmission

Layer 2 packet transparent transmission enables transmitting Layer 2 packets between networks without influencing ISP networks. When Layer 2 protocol packets arrive at the edge device on one side, the destination MAC address is

changed as private address for forwarding in ISP networks. Then when the packets arrive the edge device on other side,the destination MAC address is changed back to public address. This ensures transparent transmission of Layer 2 protocol packets in ISP networks.

12.1.3.4 Uplink port

Uplink port essentially is a special trunk port. The difference is that the packets outputted from the uplink port are tagged, but the packets outputted from the trunk port (when they are forwarded from native VLAN) are untagged. A typical example is the port of a user network connecting to an ISP network.

12.2 Configuring QinQ

This chapter includes:

- Default QinQ Configurations
- Restriction of QinQ Configuration
- Configuring Basic QinQ
- Configuring Flexible QinQ
- Configuring Other QinQ Functions

12.2.1 Default QinQ Configurations

By default, basic QinQ, flexible QinQ and other QinQ functions are disabled.

12.2.2 Restriction of QinQ Configuration

The following restrictions apply to QinQ configuration:

- The routed ports cannot be configured as tunnel ports.
- The 802.1x function cannot be enabled on the port configured as a tunnel port.
- Port security cannot be enabled on the port configured as a tunnel port.
- For the ACL applied on the tunnel port, the inner keyword is necessary to match the VID of user tag.
- It is recommended to configure the egress of user network connecting the ISP network as uplink port as well. If the TPID of ISP tag is set on the QinQ-enabled port of the user network, the TPID of ISP tag of uplink port should be set with the same value.
- QinQ does not support hot backup.
- The MTU of a port is 1500 bytes by default. A packet will be increased by 4 bytes when it is added with outer VLAN tag. It is recommended to increase

the MTU value of ports in ISP network at an appropriate extent, or at least 1504 bytes.

- Once QinQ is enabled on a port, to enable IGMP Snooping, you need set SVGL sharing mode or otherwise IGMP Snooping does not function on the port with QinQ enabled.

12.2.3 Configuring Basic QinQ

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure a tunnel port:

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface*>	Enter the interface configuration mode.
switchport mode dot1q-tunnel	Set the port as a dot1q-tunnel port.
switchport dot1q-tunnel allowed vlan [**add**] { **tagged** | **untagged** } *v_list*	Add the allowed VLAN for dot1q-tunnel port and specify that whether the VLAN is tagged or not when outputting the packets of allowed VLAN.
switchport dot1q-tunnel allowed vlan remove *v_list*	Delete the allowed VLAN on the dot1q-tunnel port.
switchport dot1q-tunnel native vlan *VID*	Set the default VLAN for the dot1q-tunnel port.
End	Exit the interface mode.
show running-config	Show the configuration.

Note	It is not recommended to set the native VLAN of trunk port in the ISP network as the default VLAN of tunnel port, because the tag with native VID will be stripped off on trunk port.

The following example demonstrates how to configure a QinQ port:

```
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# switchport mode dot1q-tunnel
DES-7200(config-if)# switchport dot1q-tunnel nativ vlan 20
DES-7200(config-if)# switchport dot1q-tunnel allowed vlan tagged 100-200
DES-7200(config)# end
```

12.2.4 Configuring Flexible QinQ

The section includes:

- Configure protocol-based VID change policy table
- Configure flow-based VID change policy table

12.2.4.1 Configure protocol-based VID change policy table

- Configure VID add policy table
- Configure outer tag-based VID change policy table
- Configure inner tag-based VID change policy table
- Configure inner tag-based+outer tag-based VID change policy table

Configure VID add policy table

For an incoming packet on dot1q-tunnel port, in some case, it is necessary to specify the VID of outer tag for the packet during forwarding according to the VID of the tags of the packet. Run the **dot1q outer-vid** command to specify the outer VID when adding outer tag to inner VID list. With this command, you can specify an internal VLAN and add the same outer VID as the inner VID, and add the egress to the untagged port set of the VLAN. In addtion, the packets with original inner tag can be outputted via egress.

Command	Function
configure terminal	Enter the global configuration mode.
interface *intf-id*	Enter the interface configuration mode.
switchport mode dot1q-tunnel	Set the port as a dot1q-tunnel port.
dot1q outer-vid *VID* **register inner-vid** *v_list*	Configure the protocol-based policy to add the VID of outer tag.
no dot1q outer-vid *VID* **register inner-vid** *v_list*	Remove the configuration
end	Exit the interface mode.
show running-config	Show the configuration.

The following example adds the VID 3 of outer tag when the VID of the tag of incoming packet is 4-22:

```
DES-7200# configure
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode dot1q-tunnel
DES-7200(config-if)# switchport dot1q-tunnel allowed vlan add tagged 3
DES-7200(config-if)# dot1q outer-vid 3 register inner-vid 4-22
DES-7200(config-if)# end
```

Note	DES-7200 series support mapping 4K consecutive inner VIDs to one outer VID.

Configure outer tag-based VID change policy table

For the packets incoming from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of outer tags according to the VIDs of outer tags of incoming packets. Run the **dot1q relay-vid** *VID* **translate local-vid** *v_list* command to change the local VID (VID of outer tag before change) list.

Command	Function
configure terminal	Enter the global configuration mode.
interface *intf-id*	Enter the interface configuration mode.
switchport mode *port-type*	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
dot1q relay-vid *VID* **translate local-vid** *v_list*	Configure the policy to change the VID of outer tag according to original VID of outer tag.
no dot1q relay-vid *VID* **translate local-vid** *v_list*	Remove the configuration
end	Exit the interface mode.
show running-config	Show the configuration.

Note	This function is supported on the 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG, 7200-24GE and 7200-24G2XG line cards of DES-7200 series.

The following example changes the VID of outer tag as 100 when the VID of outer tag of incoming packets is 10-20.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# dot1q relay-vid 100 translate local-vid 10-20
DES-7200(config-if)# end
```

Configure inner tag-based VID change policy table

For the packets incoming from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of outer tags according to the VIDs of inner tags of incoming packets. Run the **dot1q relay-vid** *VID* **translate**

inner-vid *v_list* command to change the local VID (VID of outer tag before change) list.

Command	Function
configure terminal	Enter the global configuration mode.
interface *intf-id*	Enter the interface configuration mode.
switchport mode *port-type*	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
dot1q relay-vid *VID* **translate inner-vid** *v_list*	Configure the policy to change the VID of outer tag according to the inner tag.
no dot1q relay-vid *VID* **translate inner-vid** *v_list*	Remove the configuration
end	Exit the interface mode.
show running-config	Show the configuration.

Note	DES-7200 series support up to 2K policies.

The following example changes the VID of outer tag as 100 when the VID of inner tag of incoming packets is 10-20.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# dot1q relay-vid 100 translate inner-vid 10-20
DES-7200(config-if)# end
```

Configure inner tag+outer tag based VID change policy table

For ingress packets on Access, Trunk, Hybrid and Uplink ports, sometimes we need to change the VID of outer Tag to different values. Use "**dot1q new-outer-vlan** *VID* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*" command to specify the new outer VID, old outer VID and inner Tag list, and use "**no dot1q new-outer-vlan** *VID* **translate old-outer-vlan** *vid* **inner-vlan** *v_list*" command to remove the configuration. Please refer to command reference for detailed commands.

The configuration steps are shown below:

Command	Function
configure terminal	Enter the global configuration mode.
interface *intf-id*	Enter the interface configuration mode.

Command	Function
switchport mode *port-type*	Configure to Access, Trunk, Uplink or Hybrid port.
dot1q new-outer-vlan *VID* **translate old-outer-vlan** vid **inner-vlan** *v_list*	Configure outer Tag + inner Tag based outer Tag VID mapping rule.
no dot1q new-outer-vlan *VID* **translate old-outer-vlan** vid **inner-vlan** *v_list*	Remove the outer Tag + inner Tag based outer Tag VID mapping rule.
end	Exit the interface mode.
show translation-table	Show the configuration.

The following example shows how to map the vid to 3888 when inner Tag VID and outer Tag VID of ingress packets are 2001-3000 and 1888 respectively.

```
DES-7200(config)# vlan 1888, 3888
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# dot1q new-outer-vlan 3888 translate old-outer-vlan 1888
inner-vlan 2001-3000
DES-7200(config-if)# end
```

12.2.4.2 Configure flow-based VID change policy table

- Configure VID add policy table
- Configure outer VID change policy table
- Configure inner VID change policy table

Configure VID add policy table

For an incoming packet on dot1q-tunnel port, in some case, it is necessary to specify the VID of outer tag for the packet according to its content. Run the**traffic-redirect access-group** *acl* **nested-vlan** *VID* **in** comamnd to specify the VID of outer tag when the packet incoming from the dot1q-tunnel port matches ACL.

Command	Function
configure terminal	Enter the global configuration mode.
interface *intf-id*	Enter the interface configuration mode.
switchport mode dot1q-tunnel	Set the port as a dot1q-tunnel port.

Command	Function
traffic-redirect access-group ***acl*** **nested-vlan** *VID* **in**	Configure the flow-based policy to add the VID of outer tag.
no traffic-redirect access-group ***acl*** **nested-vlan** *VID* **in**	Remove the configuration
end	Exit the interface mode.
show running-config	Show the configuration.

Note

- When this function is enabled on the 7200-24P, 7200-24G, 7200-48P, 7200-2XG, 7200-4XG, and 7200-48 line cards of DES-7200 series, the egress should reside on the chipset different from dot1q-tunnel port (for DES-7200 series, number of chipsets on line cards is computed on the basis of one chipset per 24 gigabit ports or one chipset per 2 10G ports). Flow separation is enabled on the dot11-tunnle port to prevent broadcast, multicast or unknown unicast communications with any other interfaces of the chipset.
- Flow-based VID change policy table takes precedence over protocol-based VID change policy table.
- When you configure member port on AP, the configured VID add policy or VID change policy will be deleted. Reconfiguration of VID add policy or VID change policy is necessary. It is recommended to configure VID policy on AP after configuring member port.
- Once ACL is deleted, the ACL related policies will be deleted as well.
- When the packets with the tag larger than or equal to Layer 2 are received on the dot1q-tunnel port, you can add tag by flow-based match rule.
- If a packet matches two or more flow policies without priority specified simultaneously, the early configured policy takes effect.

The following example adds the VID 9 to the packets from 1.1.1.3:

```
DES-7200# configure
DES-7200(config)# ip access-list standard 20
DES-7200(config-acl-std)# permit host 1.1.1.3
DES-7200(config-acl-std)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode dot1q-tunnel
DES-7200(config-if)# traffic-redirect access-group 20 nested-vlan 10 in
```

```
DES-7200(config-if)# end
```

Configure outer VID change policy table

For the packets incoming from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of outer tags according to the contents of incoming packets. Run the **traffic-redirect access-group** *acl* **outer-vlan** *VID* **in** command to change the VID of outer tag of the packets matching ACL.

Command	Function
configure terminal	Enter the global configuration mode.
interface *intf-id*	Enter the interface configuration mode.
switchport mode *port-type*	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
traffic-redirect access-group *acl* **outer-vlan** *VID* **in**	Change the VID of outer tag according to the flow.
no traffic-redirect access-group *acl* **outer-vlan**	Remove the configuration
end	Exit the interface mode.
show running-config	Show the configuration.

Note	◆ Flow-based outer VID change policy table takes precedence over protocol-based outer VID change policy table. ◆ When you configure member port on AP, the configured VID add policy or VID change policy will be deleted. Reconfiguration of VID add policy or VID change policy is necessary. It is recommended to configure VID policy on AP after configuring member port. ◆ Once ACL is deleted, the ACL related policies will be deleted as well. ◆ If a packet matches two or more flow policies without priority specified simultaneously, the early configured policy takes effect.

Note	This function is supported on the 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG, 7200-24GE and 7200-24G2XG line cards of DES-7200 series.

The following example changes the VID of outer tag as 3 for the packets from 1.1.1.1:

```
DES-7200# configure
DES-7200(config)# ip access-list standard 2
DES-7200(config-acl-std)# permit host 1.1.1.1
DES-7200(config-acl-std)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# traffic-redirect access-group 2 outer-vlan 3 in
DES-7200(config-if)# end
```

Configure inner VID change policy table

For the packets outgoing from Access port, Trunk port, Hybrid port and Uplink port, sometimes you need to change the VIDs of inner tags according to the contents of outgoing packets. Run the **traffic-redirect access-group** *acl* **inner-vlan** *VID* **out** command to change the VID of inner tag of the packets matching ACL.

Command	Function
configure terminal	Enter the global configuration mode.
interface *intf-id*	Enter the interface configuration mode.
switchport mode *port-type*	Set the port as Access port, Trunk port, Uplink port or Hybrid port.
traffic-redirect access-group *acl* **inner-vlan** *VID* **out**	Change the VID of inner tag according to the flow.
no traffic-redirect access-group *acl* **inner-vlan**	Remove the configuration
end	Exit the interface mode.
show running-config	Show the configuration.

 **Note**	◆ Flow-based outer VID change policy table takes precedence over protocol-based outer VID change policy table. ◆ When you configure member port on AP, the configured VID add policy or VID change policy will be deleted. Reconfiguration of VID add policy or VID change policy is necessary. It is recommended to configure VID policy on AP after configuring member port. ◆ Once ACL is deleted, the ACL related policies will be deleted as well. ◆ If a packet matches two or more flow policies without priority specified simultaneously, the early configured policy takes effect.

 **Note**	This function is supported on the 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG, 7200-24GE and 7200-24G2XG line cards of DES-7200 series.

The following example changes the VID of inner tag as 6 for the packets to 1.1.1.2:

```
DES-7200# configure
DES-7200(config)# ip access-list standard to_6
DES-7200(config-acl-std)# permit host 1.1.1.2
DES-7200(config-acl-std)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# traffic-redirect access-group to_6 inner-vlan 6 out
DES-7200(config-if)# end
```

 **Caution**	When you configure flow-based policy table, inner VID is necessary to match user VID, or otherwise outer VID is matched.

12.2.5 Configuring Other QinQ Functions

- Configure an uplike port
- Configure the TPID of the ISP tag
- Configure priority duplication
- Configure priority mapping
- Configure address duplication

- Configure transparent transmission of Layer 2 protocol

12.2.5.1 Configuring an Uplink Port

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure an uplink port:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface*>	Enter the interface configuration mode.
switchport mode uplink	Configure the port as an uplink port.
end	Exit the interface mode.
show running-config	Show the configuration.

The following example demonstrates how to configure an uplink port:

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport mode up-link
DES-7200(config)# end
```

12.2.5.2 Configuring the TPID Value of ISP Tag

In the global configuration mode, input the **interface** command to enter the interface configuration mode. Follow these steps to configure the TPID value of ISP tag:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface*>	Enter the interface configuration mode.
frame-tag tpid <*tpid*>	Set the TPID value of ISP tag. If you want to set it as 0x9100, directly enter frame-tag tpid 9100. Note that the hexadecimal system is used by default. This function takes effect on egress.
end	Exit the interface mode.
show frame-tag tpid	View the TPID value list on the port.

The following example demonstrates how to configure TPID:

```
DES-7200(config)# interface gigabitethernet 0/1
DES-7200(config-if)# frame-tag tpid 9100
DES-7200(config)# end
DES-7200# show frame-tag tpid interface gigabitethernet 0/1
Port    tpid
------- -------------
```

```
Gi0/1    0x9100
```

Note	◆ Do not set TPID to be 0x0806(ARP), 0x0200(PUP), 0x8035(RARP), 0x0800(IP), 0x86DD(IPv6), 0x8863/0x8864(PPPoE), 0x8847/0x8848(MPLS), 0x8137(IPX/SPX), 0x8000(IS-IS), 0x8809(LACP), 0x888E(802.1x), 0x88A7(cluster), and 0x0789(reserved).

12.2.5.3 Configuring Priority Duplication

Follow these steps to duplicate the priority of inner tag to outer tag:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface*>	Enter the interface configuration mode.
mls qos trust cos	Configure the interface to be trust CoS mode.
inner-priority-trust enable	Copy the priority value of the inner tag (user tag) to the priority value of the outer tag (ISP tag).
End	Exit the interface mode.
show inner-priority-trust	View the priority duplication configuration of the user tag.

Note	◆ You can configure priority duplication of the user tag only on the dot1q-tunnel port, whose priority is higher than QoS in the trusted mode but lower than flow-based QOS. ◆ Priority duplication and priority mapping cannot be enabled on one interface at the same time. ◆ For DES-7200 series, priority duplication takes effect only after this trust mode is enabled.

The following example shows how to configure the priority duplication of the user tag:

```
DES-7200(config)# interface gigabitethernet 0/1
DES-7200(config-if)# mls qos trust cos
DES-7200(config-if)# inner-priority-trust enable
DES-7200(config)# end
DES-7200# show inner-priority-trust interface gigabitethernet 0/1
Port     inner-priority-trust
------   --------------------
```

```
Gi0/1    enable
```

12.2.5.4 Configuring Priority Mapping

Follow these steps to set the priority of outer tag by the priority of inner tag:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface*>	Enter the interface configuration mode.
dot1q-Tunnel cos *inner-cos-value* **remark-cos** *outer-cos-value*	Set the priority of outer tag (ISP tag) by the priority value of the inner tag (user tag).
end	Exit the interface mode.
show interface intf-name remark	View the priority mapping configuration of the user tag.

Note	◆ You can configure priority duplication of the user tag only on the dot1q-tunnel port, whose priority is higher than QoS. ◆ Priority duplication and priority mapping cannot be enabled on one interface at the same time. ◆ Priority mapping takes effect only when trust none is configured.

The following example shows how to configure the priority mapping of the user tag:

```
DES-7200(config)# interface gigabitethernet 0/1
DES-7200(config-if)#dot1q-Tunnel cos 3 remark-cos 5
DES-7200(config)# end
DES-7200# show interface gigabitethernet 0/1 remark
Ports        Type       From value  To value
------------ ---------- ----------- --------
Gi0/1        Cos-To-Cos  3          5
```

12.2.5.5 Configuring Address Duplication

Follow these steps to duplicate the learned dynamic address form one VLAN to another VLAN:

Command	Description
configure terminal	Enter the global configuration mode.
interface <*interface*>	Enter the interface configuration mode.

Command	Description
mac-address-mapping *x* **source-vlan** *src-vlan-list* **destination-vlan** *dst-vlan-id*	Configure the learned dynamic address from the source VLAN to the destination VLAN.
end	Exit the interface mode.
show interface *intf-name* **mac-address-mapping** *x*	View the address duplication configuration.

 **Note**	◆ Disabling inter-VLAN MAC address duplication will remove all learned MAC address entries of other VLANs from the destination VLAN. ◆ Inter-VLAN MAC address duplication can be set only once for a VLAN on a port. To modify the configuration, delete it first. ◆ This function cannot be used in conjunction with share VLAN. MAC address cannot be duplicated into dynamic VLAN. ◆ Up to 8 destination VLANs can be configured on a port. Address duplication takes effect even though the port is not in the specific destination VLAN. ◆ Address duplication cannot be enabled on host/promiscuous port, mirroring destination port or the port with port security and 802.1x enabled. ◆ The priority of duplicated address is higher than dynamic address but lower than other types of address. ◆ When the source MAC address is aging, the duplicated address is aging as well. This also applies to deleting MAC address. ◆ Hot backup is not supported. When master-slave handover occurs, it is recommended users to disable and then enable address duplication. ◆ The MAC address entries obtained by inter-VLAN MAC address duplication cannot be deleted by hand. To delete these entries, disable inter-VLAN MAC address duplication. ◆ For the dot1q-tunnel port of the 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG, 7200-24GE and 7200-24G2XG line cards of DES-7200 series, MAC address is learned to flow-based outer tag. Hence, MAC address duplication is not mandatory. For other types of line cards, MAC address is learned to the default VLAN of the dot1q-tunnel ort. Hence, MAC address duplication is necessary.

The following example shows how to configure address duplication of the user tag:

```
DES-7200(config)# interface gigabitethernet 0/1
DES-7200(config)# switchport mode trunk
DES-7200(config-if)#mac-address-mapping destination-vlan5 source-vlan 1-3
DES-7200(config)# end
DES-7200# show interface mac-address-mapping
Ports    destination-VID    Source-VID-list
```

```
-------------------------------------------
Gi0/1        5               1-3
```

12.2.6 Configuring Transparent Transmission of L2 Protocol Packets

- Configure transparent transmission of STP protocol packets
- Configure transparent transmission of GVRP protocol packets
- Configure transparent transmission address

12.2.6.1 Configuring Transparent Transmission of STP Protocol Packets

In the privileged mode, you can configure transparent transmission of STP protocol packets by the following steps:

Command	Description
configure terminal	Enter the global configuration mode.
l2protocol-tunnel stp	Configure to enable transparent transmission of STP protocol packets globally.
interface *interface-id*	Enter the interface configuration mode.
l2protocol-tunnel stp enable	Enable transparent transmission of STP protocol packets on the interface.
show l2protocol-tunnel stp	View the configuration.

An example below shows how to enable transparent transmission of STP protocol packets:

```
DES-7200# configure
DES-7200(config)# l2protocol-tunnel stp
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# l2protocol-tunnel stp enable
```

12.2.6.2 Configuring Transparent Transmission of GVRP Protocol Packets

In the privileged mode, you can configure transparent transmission of GRVP protocol packets by the following steps:

Command	Description
configure terminal	Enter the global configuration mode.
l2protocol-tunnel gvrp	Configure to enable transparent transmission of GRVP protocol packets globally.
interface *interface-id*	Enter the interface configuration mode.
l2protocol-tunnel gvrp enable	Enable transparent transmission of GRVP protocol packets on the interface.
show l2protocol-tunnel gvrp	View the configuration.

An example below shows how to enable transparent transmission of GVRP protocol packets:

```
DES-7200# configure

DES-7200(config)# l2protocol-tunnel gvrp
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# l2protocol-tunnel gvrp enable
```

Note	Enabling transparent transmission on the interface takes effect only after this function is enabled globally. Once enabled, the interface does not join the protocol computation. If the packets received are destined to special multicast address, this implies that there is something wrong in the network and thus the packets are directly dropped.

12.2.6.3 Configuring Transparent Transmission Address

In the privileged mode, you can configure transparent transmission address by the following steps:

Command	Description
configure terminal	Enter the global configuration mode.

l2protocol-tunnel {stp | GVRP} tunnel-dmac *mac-address*	Configure the transparent transmission address of corresponding protocl.
show l2protocol-tunnel stp	View the configuration.

An example below shows how to configure the transparent transmission address of STP protocol:

```
DES-7200# configure
DES-7200(config)#l2protocol-tunnel stp tunnel-dmac 011AA9 000005
```

Note	The addresses available for STP protocol are 01d0f8 000005, 011AA9 000005, 010FE2 000003, 01000C CDCDD0, 01000C CDCDD1, 01000C CDCDD2, and the addresses available for GVRP protocol are 01d0f8 000006 and 011AA9 000006. Without transparent transmission address configured, by default, the last bit of the first byte of the OUI of the local device is set to 1 plus the next three bytes (stp:000005; gvrp:000006) as multicast address. For instance, the local device's MAC address is 00d0f8000001, then the transparent transmission address for STP protocol is 01d0f8000005.

12.2.7 Show QinQ Informaiton

In the privileged mode, use the following command to show QinQ configuration.

Command	Description
DES-7200# **show dot1q-tunnel**	Show the enablement state of dot1q-tunnel port.
DES-7200#**show interface**[*intf-id*]**dot1q-tunnel**	Show the configuration of dot1q-tunnel port.
DES-7200# **show registration-table** [**interface** *intf-id*]	Show the protocol-based VID change policy table on the dot1q-tunnle port.
DES-7200# **show translation-table** [**interface** *intf-id*]	Show the protocol-based VID change policy table on the Access, Trunk and Hybird ports.
DES-7200# **show traffic-redirect** [**interface** *intf-id*]	Show the flow-based VID change policy table.

DES-7200# **show frame-tag tpid interface** [*intf-id*]	Show the TPID value on the interface.
DES-7200# **show inner-priority-trust**	Show the priority duplication configuration.
DES-7200# **show interface intf-name remark**	Show the priority mapping configuration.
DES-7200# **show mac-address-mapping**	Show the address duplication configuration.
DES-7200# **show l2protocol-tunnel** { **gvrp** | **stp** }	Show the transparent transmisison configuration of Layer 2 protocols.

12.3 Typical QinQ configuration example

12.3.1 Using basic QinQ to realize layer-2 VPN service

12.3.1.1 Topological diagram

Company A and B have their respective offices, and each office has its respective network. As shown below, Customer A1, Customer A2, Customer B1 and Customer B2 are all edge devices of Company A and Company B. Customer A1 and Customer B1 access the public network through the provider edge device of Provider A, while Customer A2 and Customer B2 access the public network through the provider edge device of Provider B.

The VLAN range of the office network used by Customer A1-A2 is VLAN1-100, and that used by Customer B1-B2 is VLAN1-200.

Provider A and Provider B are devices of another manufacturer, with TPID being 0x9100.

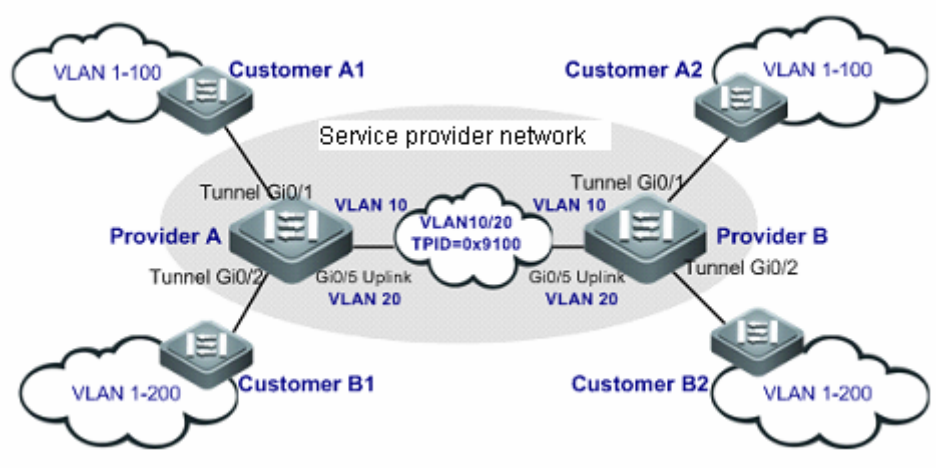


Figure 8 Topology for using basic QinQ to realize layer-2 VPN service

12.3.1.2 Application requirements

The service provider provides VPN service for Company A and Company B, and the specific requirements are shown below:

1. The data of both companies can preserve the original VLAN information when being sent to the peer side.

2. Data with same VLAN ID won't cause conflict during transmission over ISP network.

12.3.1.3 Configuration tips

1. You don't need to distinguish the traffic of downlink users. Enabling basic QinQ on the provider edge devices (Provider A and Provider B) will meet the needs.

2. The TPID of DES-7200 switches is different from the TPID used by other manufacturers. You need to configure on the Uplink interface of provider edge devices (Provider A and Provider B) and set TPID to the same value with third-party devices.

Note

1、 In QinQ configuration model, when the service-network-connecting uplink port of edge device or the interconnecting ports of service provider devices are Trunk ports or Hybrid ports, please don't set the native vlan of trunk ports or hybrid ports to the default vlan of tunnel port, because packets leaving the trunk port or hybrid port will be stripped off the Tag with VID being its native vlan.

2、 QinQ-enabled device will encapsulate the outer Tag of other VLAN for user packets and won't forward packets as per the original VLAN in the packets. Therefore, there is no need to create user's VLAN on the device.

12.3.1.4 Configuration Steps

1) Configure Provider A

Step 1: Create provider VLAN 10 and VLAN 20 to distinguish the traffic of two users

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan 10
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 20
DES-7200(config-vlan)#exit
```

Step 2: Enable basic QinQ on the interface connecting to the network of Company A, and use VLAN 10 to transmit the traffic of Company A through tunnel.

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel
DES-7200(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan
10
DES-7200(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed
vlan add untagged 10
```

Step 3: Enable basic QinQ on the interface connecting to the network of Company B, and use VLAN 20 to transmit the traffic of Company B through tunnel.

```
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#switchport mode dot1q-tunnel
DES-7200(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel native vlan
20
```

```
DES-7200(config-if-GigabitEthernet 0/2)#switchport dot1q-tunnel allowed
vlan add untagged 20
```

Step 4: Configure Uplink port

```
DES-7200(config)# interface gigabitEthernet 0/5
DES-7200(config-if-GigabitEthernet 0/5)#switchport mode uplink
```

Step 5: On the Uplink port, set the TPID value of egress packets to 0x9100, which can be recognized by third-party devices.

```
DES-7200(config-if-GigabitEthernet 0/5)#frame-tag tpid 9100
```

2) Configure Provider B

Configurations on Provider B are the same as those on Provider A. Please refer to the configurations on Provider A given above.

12.3.1.5 Verification

Step 1: Verify whether the tunnel ports have been properly configured. Key points: whether port type is dot1q-tunnel, whether the outer Tag VLAN is Native VLAN and is included in the allowed VLAN list of the port, and whether the uplink port on provider edge device is Uplink, Trunk or Hybrid port.

DES-7200#show running-config

```
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 10
 switchport dot1q-tunnel native vlan 10
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 20
 switchport dot1q-tunnel native vlan 20
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
 frame-tag tpid 0x9100
```

Step 2: Verify the QinQ configuration of respective ports again. Key points are the same as Step 1.

```
DES-7200#show interfaces dot1q-tunnel

========Interface Gi0/1========
Native vlan: 10
Allowed vlan list:1,10,
Tagged vlan list:

========Interface Gi0/2========
Native vlan: 20
Allowed vlan list:1,20,
Tagged vlan list:
```

Step 3: Verify the TPID configuration. Key point: whether the interface is Uplink port, TPID value.

```
DES-7200#show frame-tag tpid
Ports        Tpid
------- -------------
Gi0/5       0x9100
```

Steps to verify configurations on Provider B are the same as those on Provider A. Please refer to the verification steps on Provider A given above.

12.3.2 C-Tag based flexible QinQ to distinguish traffic

12.3.2.1 Topological diagram

The following figure shows the networking diagram of metropolitan area network for C-Tag based flexible QinQ to classify the traffic. Broadband Internet and IPTV are all important services carried on the metropolitan area network. As shown below, client devices converge at the corridor switch, and broadband Internet and IPTV traffic will be classified by assigning different VLANs. Broadband Internet users fall within VLAN 101-200, while IPTV users fall within VLAN 201-300.

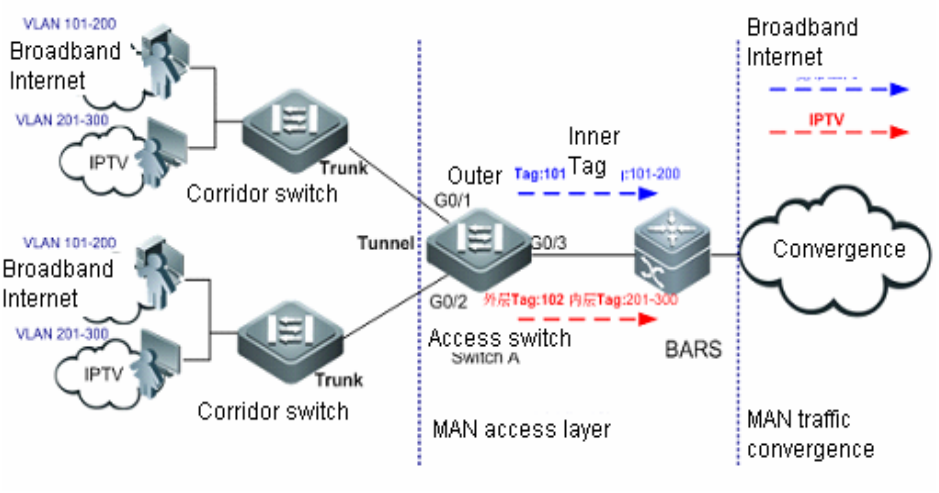


Figure 9 C-Tag based flexible QinQ to realize Internet access service

12.3.2.2 Application requirements

Broadband Internet and IPTV traffic shall be identified by VLAN ID, so as to apply different QoS service policies to different traffic.

12.3.2.3 Configuration tips

Configure C-Tag based flexible QinQ on MAN access layer switch's two interfaces (G0/1 and G0/2 of Switch A) connecting with the corridor convergence switches. The application requirements can be met by classifying service traffic as per inner VLAN Tag.

Flexible QinQ VLAN label planning for adding S-Tag on the basis of C-Tag traffic classification

Device	Service	Inner VLAN Tag	Outer VLAN Tag	Traffic classification rule
Switch A	Broadband Internet	101-200	101	C-Tag VLAN range
Switch A	IPTV	201-300	201	C-Tag VLAN range

Note

QinQ-enabled device will encapsulate the outer Tag of other VLAN for user packets and won't forward packets as per the original VLAN in the packets. Therefore, there is no need to create user's VLAN on the device.

12.3.2.4 Configuration Steps

- **Configure Switch A**

Step 1: Create provider VLAN 101 and VLAN 201 to distinguish the traffic of different services

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan 101
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 201
DES-7200(config-vlan)#exit
```

Step 2: On the downlink port of access switch, configure flexible QinQ for adding outer VLAN Tag on the basis of C-Tag

```
DES-7200(config)#interface range gigabitEthernet 0/1-2
DES-7200(config-if-range)# switchport mode dot1q-tunnel
```

! Configure Gi 0/1 and Gi 0/2 as Tunnel ports

```
DES-7200(config-if-range)# switchport dot1q-tunnel allowed vlan add untagged
101,201
```

! Add provider VLAN 101 and VLAN 201 into the allowed VLAN list of Tunnel port, and configure to strip the provider Tag when the peer packets return to the Tunnel port.

```
DES-7200(config-if-range)# dot1q outer-vid 101 register inner-vid 101-200
```

! Configure to add the tag of vlan 101 (S-tag) to vlan 101-200 (C-tag) data frames entering Tunnel port for transmission over the provider network

```
DES-7200(config-if-range)# dot1q outer-vid 201 register inner-vid 201-300
```

! Configure to add the tag of vlan 201 (S-tag) to vlan 201-300 (C-tag) data frames entering Tunnel port for transmission over the provider network.

Step 3: Configure Uplink port

```
DES-7200(config)# interface gigabitEthernet 0/3
DES-7200(config-if-GigabitEthernet 0/3)#switchport mode uplink
```

Note

Outer Tag VLAN (including Native VLAN) shall be allowed on Tunnel port, and packets of such VLAN shall be allowed to pass the Internet-accessing interface. In this example, the Native VLAN of Tunnel port is the default VLAN1, which is allowed by default.

12.3.2.5 Verification

Step 1: Verify whether the configurations are correct. Key points: whether the type of downlink interface is dot1q-tunnel, whether the outer Tag VLAN is included in the allowed VLAN list of the interface, whether the mapping policy on the interface is correct, and whether the uplink port has been properly configured.

```
DES-7200#show running-config interface gigabitEthernet 0/1

interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 101,201
 dot1q outer-vid 101 register inner-vid 101-200
 dot1q outer-vid 201 register inner-vid 201-300
 spanning-tree bpdufilter enable

        !
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 101,201
 dot1q outer-vid 101 register inner-vid 101-200
 dot1q outer-vid 201 register inner-vid 201-300
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/3
 switchport mode uplink
```

Step 2: Verify the QinQ configuration of respective ports again. Key points are the same as Step 1.

```
DES-7200#show interfaces dot1q-tunnel

========Interface Gi0/1========
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:

========Interface Gi0/2========
Native vlan: 1
Allowed vlan list:1, 101,201
Tagged vlan list:
```

Step 3: Verify the mapping rule for adding Tag on the basis of C-Tag. Key points: whether the mapping between inner VLAN tag and outer VLAN tag is correct.

```
DES-7200#show registration-table

Ports        Outer-VID   Inner-VID-list
------       ----------  --------------
Gi0/1        101         101-200
Gi0/1        201         201-300
Gi0/2        101         101-200
Gi0/2        201         201-300
```

12.3.3 ACL-based flexible QinQ to distinguish traffic

12.3.3.1 Topological diagram

The following figure shows the networking diagram for ACL-based flexible QinQ deployed on the metropolitan area network. The service provider provides broadband access and IPTV services to users. There are many out-of-date and low-end network access devices on user's network, making it impossible to effectively distinguish traffic according to VLAN ID. All types of services are carried in the same VLAN.

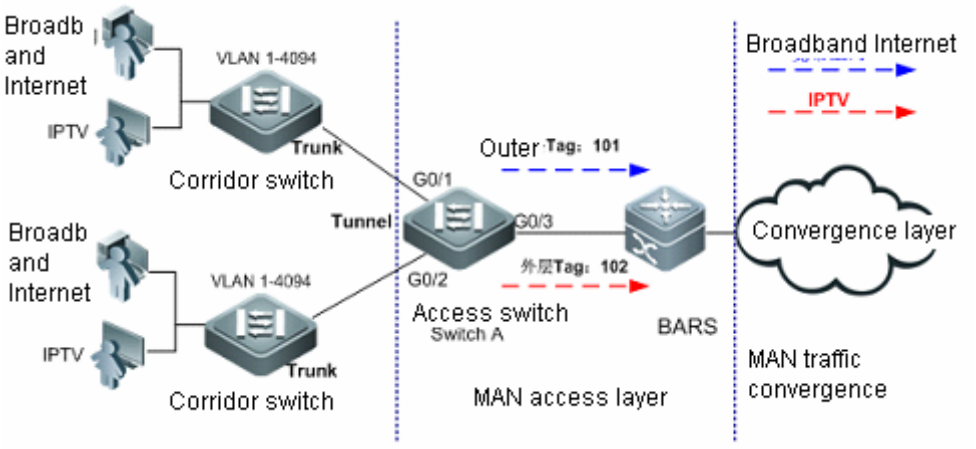


Figure 10 ACL-based flexible QinQ to realize Internet access service

12.3.3.2 Application requirements

Broadband Internet and IPTV traffic of downstream users shall be identified by protocol, so as to apply different QoS service policies to different traffic.

12.3.3.3 Configuration tips

Configure the ACL based flexible QinQ on MAN access layer switch's two interfaces (G0/1 and G0/2 of Switch A) connecting with the corridor convergence switches, so as to distinguish user traffic and meet the application requirements.

Generally, PPPOE dialing is used in broadband Internet service, with protocol number being 0x8863/0x8864 typically; IPoE is used in IPTV service, with protocol number being 0x0800 typically.

Flexible QinQ VLAN label planning for adding S-Tag on the basis of ACL traffic classification

Device	Service	Inner VLAN Tag	Outer VLAN Tag	Traffic classification rule
Switch A	Broadband (PPPoE)	1-4094	101	Protocol number: 0x8863/0x8864
Switch A	IPTV (IPoE)	1-4094	201	Protocol number: 0x0800

12.3.3.4 Configuration Steps

- **Configure Switch A**

Step 1: Create ACL for distinguishing traffic

```
DES-7200#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)# expert access-list extended acl1
```

! Matching protocol type 0x8863/Ox8864 of PPPOE

```
DES-7200(config-exp-nacl)# permit 0x8863 any any

DES-7200(config-exp-nacl)# permit 0x8864 any any

DES-7200(config-exp-nacl)#exit

DES-7200(config)# expert access-list extended acl2
```

! Matching protocol type 0x0800 of IPOE

```
DES-7200(config-exp-nacl)#permit 0x0800 any any
```

Step 2: Create provider VLAN 101 and VLAN 201 to distinguish the traffic of different users.

```
DES-7200#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)#vlan 101

DES-7200(config-vlan)#exit

DES-7200(config)#vlan 201

DES-7200(config-vlan)#exit
```

Note

QinQ-enabled device will encapsulate the outer Tag of other VLAN for user packets and won't forward packets as per the original VLAN in the packets. Therefore, there is no need to create user's VLAN on the device.

Step 3: On the downlink port of access switch, configure flexible QinQ for adding outer VLAN Tag on the basis of ACL

```
DES-7200(config)#interface range gigabitEthernet 0/1-2

DES-7200(config-if-range)# switchport mode dot1q-tunnel
```

! Configure Gi 0/1 and Gi 0/2 as Tunnel ports

```
DES-7200(config-if-range)#switchport dot1q-tunnel allowed vlan add untagged 101,201
```

! Add provider VLAN 101 and VLAN 201 into the allowed VLAN list of Tunnel port, and configure to strip the provider Tag when the peer packets return to the Tunnel port.

```
DES-7200(config-if-range)#traffic-redirect access-group acl1  nested-vlan 101 in
```

! Configure to add the tag of vlan 101 (S-tag) to data frames matching ACL1 and entering Tunnel port for transmission over the provider network

```
DES-7200(config-if-range)#traffic-redirect access-group acl2 nested-vlan 201 in
```

! Configure to add the tag of vlan 201 (S-tag) to data frames matching ACL2 and entering Tunnel port for transmission over the provider network

Step 4: Configure GigabitEthernet 0/3 as an Uplink port

```
DES-7200(config)# interface gigabitEthernet 0/3

DES-7200(config-if-GigabitEthernet 0/3)#switchport mode uplink
```

Note

Outer Tag VLAN (including Native VLAN) shall be allowed on Tunnel port, and packets of such VLAN shall be allowed to pass the Internet-accessing interface. In this example, the Native VLAN of Tunnel port is the default VLAN1, which is allowed by default.

12.3.3.5 Verification

Step 1: Verify whether the configurations of Tunnel port are correct. Key points: whether the interface type is dot1q-tunnel, whether the outer Tag VLAN is included in the allowed VLAN list of the interface, and whether the policy on the interface has been properly configured.

View the configurations on GigabitEthernet 0/1

```
DES-7200#show running-config interface gigabitEthernet 0/1

interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 101,201
 traffic-redirect access-group acl1 nested-vlan 101 in
 traffic-redirect access-group acl2 nested-vlan 201 in
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/2
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 101,201
 traffic-redirect access-group acl1 nested-vlan 101 in
 traffic-redirect access-group acl2 nested-vlan 201 in
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/3
 switchport mode uplink
```

Step 2: Verify the QinQ configuration of respective ports again. Key points are the same as Step 1.

```
DES-7200#show interfaces dot1q-tunnel

========Interface Gi0/1========
Native vlan: 1
Allowed vlan list:1,101,201
```

```
Tagged vlan list:

========Interface Gi0/2========
Native vlan: 1
Allowed vlan list:1,101,201
Tagged vlan list:
```

Step 3: Verify whether ACL configurations are correct. Key point: whether ACL entries are correct.

```
DES-7200#show access-lists

expert access-list extended acl1
 10 permit 0x8863 any any
 20 permit 0x8864 any any
```

! Match broadband service traffic

```
expert access-list extended acl2
 10 permit 0x800 any any
```

! Match IPTV service traffic

Step 4: Verify the mapping rule for adding Tag based on traffic. Key point: whether the mapping between inner VLAN tag and outer VLAN tag is correct.

```
DES-7200#show traffic-redirect
Ports      Type         VID    Match-filter
-------   ----------   -----   ------------
Gi0/1      Nested-vid   101      acl1
Gi0/1      Nested-vid   201      acl2
Gi0/2      Nested-vid   101      acl1
Gi0/2      Nested-vid   201      acl2
```

12.4 Typical BPDU Tunnel configuration example

12.4.1 Topological diagram

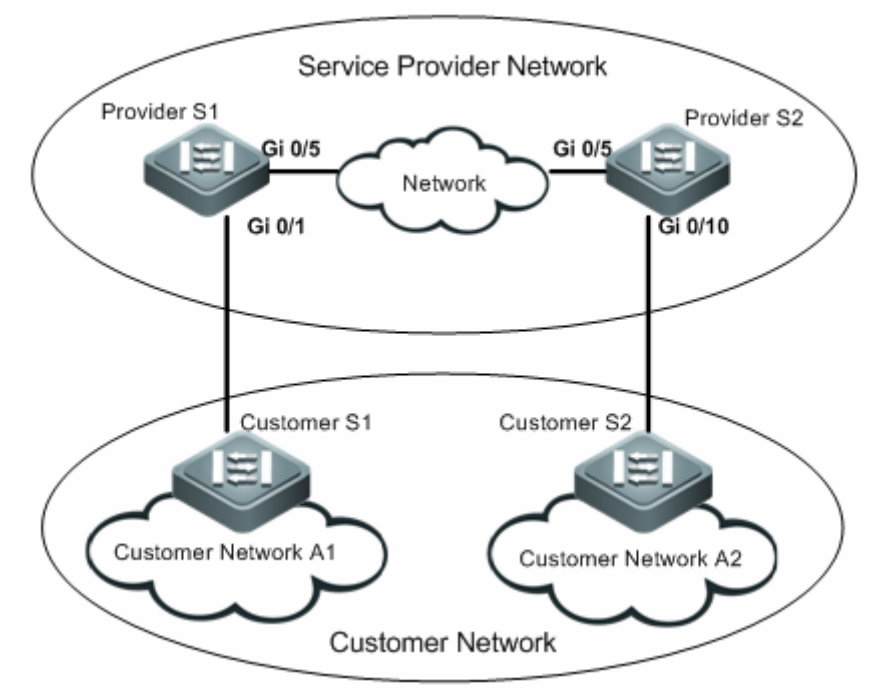


Figure 11 Topological diagram for BPDU Tunnel application

As shown above, the upper part is the provider network, and the lower part is the user network. The provider network includes edge devices of Provider S1 and Provider S2. Customer Network A1 and Customer Network A2 are two sites of the same user at different geographical locations. Customer S1 and Customer S2 are the access devices connecting user network with provider network, and access the provider network through Provider S1 and Provider S2 respectively.

12.4.2 Application requirements

1. Packets from user network are transmitted over provider network in VLAN200.

2. Customer Network A1 and Customer Network A2 at different geographical locations can participate in unified spanning tree calculation across the provider network without affecting the provider network.

12.4.3 Configuration tips

1. Enabling basic QinQ on the provider edge devices (Provider S1 and Provider S2) will meet the first need.

2. Enabling STP transparent transmission on provider edge devices (Provider S1 and Provider S2) will allow the provider network to transmit STP packets from user network through BPDU tunnel.

Note

In QinQ configuration model, when the service-network-connecting uplink port of edge device or the interconnecting ports of service provider devices are Trunk ports or Hybrid ports, please don't set the native vlan of trunk ports or hybrid ports to the default vlan of tunnel port, because packets leaving the trunk port or hybrid port will be stripped off the Tag with VID being its native vlan.

12.4.4 Configuration Steps

- **Configure Provider S1**

Step 1: Create provider VLAN 200

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan 200
DES-7200(config-vlan)#exit
```

Step 2: Enable basic QinQ on the interface connecting to the user network, and use VLAN 200 to transmit the traffic of user network through tunnel.

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#switchport mode dot1q-tunnel
DES-7200(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel native vlan
200
DES-7200(config-if-GigabitEthernet 0/1)#switchport dot1q-tunnel allowed
vlan add untagged 200
```

Step 3: Enable STP transparent transmission on the interface connecting to the user network.

```
DES-7200(config-if-GigabitEthernet 0/1)#l2protocol-tunnel stp enable
DES-7200(config-if-GigabitEthernet 0/1)#exit
```

Step 4: Enable global STP protocol transparent transmission.

```
DES-7200(config)#l2protocol-tunnel stp
```

Step 5: Configure Uplink port

```
DES-7200(config)# interface gigabitEthernet 0/5
DES-7200(config-if-GigabitEthernet 0/5)#switchport mode uplink
```

- **Configure Provider S2**

Configurations on Provider S2 are the same as those on Provider S1. Please refer to the configurations on Provider S1 given above.

12.4.5 Verification

Step 1: Verify the configurations of STP protocol transparent transmission. Key point: whether STP protocol transparent transmission has been enabled.

```
DES-7200#show l2protocol-tunnel stp

L2protocol-tunnel: Stp Enable
GigabitEthernet 0/1 l2protocol-tunnel stp enable
```

Step 2: Verify whether the tunnel ports have been properly configured. Key points: whether port type is dot1q-tunnel, whether the outer Tag VLAN is Native VLAN and is included in the allowed VLAN list of the port, and whether the uplink port on provider edge device is Uplink port.

```
DES-7200#show running-config
interface GigabitEthernet 0/1
 switchport mode dot1q-tunnel
 switchport dot1q-tunnel allowed vlan add untagged 200
 switchport dot1q-tunnel native vlan 200
 l2protocol-tunnel stp enable
 spanning-tree bpdufilter enable
!
interface GigabitEthernet 0/5
 switchport mode uplink
```

Steps to verify configurations on Provider S2 are the same as those on Provider S1. Please refer to the verification steps on Provider S1 given above.

DES-7200

IP Application Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)
Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 IP Address and Service Configuration

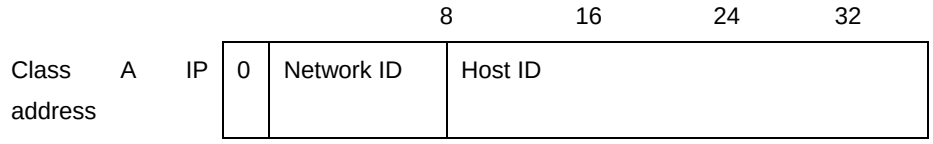
1.1 IP Address Configuration

1.1.1 IP Address Overview

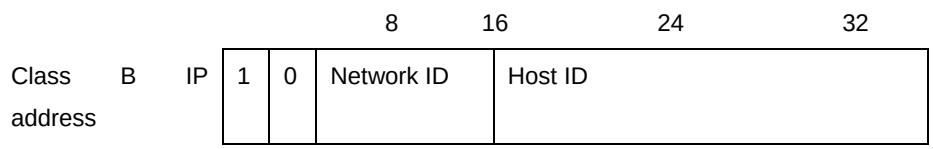
IP address is made up of 32 binary bits and expressed in the dotted decimal format for the convenience of writing and description. In the dotted decimal format, the 32 binary bits are broken into four octets (1 octet equals to 8 bits). Each octet is separated by a period (dot) in the range from 0 to 255. For example, 192.168.1.1 is an IP address in the dotted decimal format.

An IP address is an address that IP protocols use to connect one another. A 32-bit IP address consists of two parts: network address and local address. According to the first several bits of the network address of an IP address, an IP address is divided into four categories.

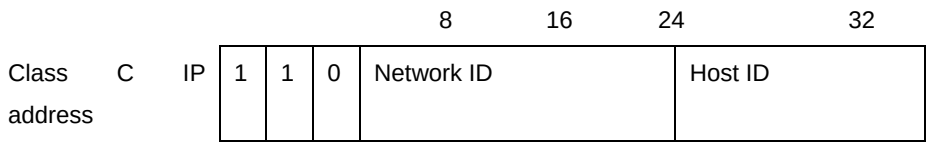
Class A: Total of 128 class-A IP addresses. The highest bit is 0 followed by seven bits identifying Network ID, and the remaining 24 bits identify Host ID.



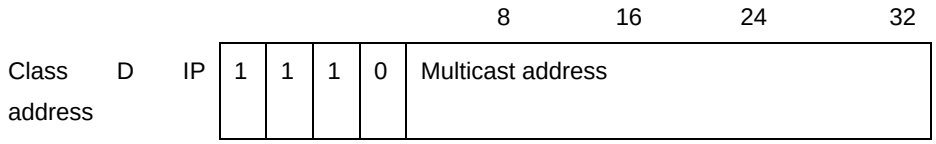
Class B: Total of 16,384 class B IP addresses. The highest two bits are 10 followed by 14 bits identifying Network ID, and the remaining 16 bits identify Host ID.



Class C: Totaol of 2,097,152 class C IP addresses. The highest three bits are 110 followed by 21 bits identifying Network ID, and the remaining eight addresses identify Host ID.



Class D: The highest four bits are 1110 and other bits are multicast IP address..



Note An IP address whose highest four bits are 1111 is prohibited. This type of IP address, also called Class E IP address, is reserved.

When you build up a network, you should execute IP addressing according to the real network environment. To make the network connect to the Internet, you need apply for IP addresses from a central authority, for example, the China Internet Network Information Center (CNNIC) in China. It is the Internet Corporation for Assigned Names and Numbers (ICANN) that is responsible for IP address allocation. However, a private network does not require the application of IP addresses. It is recommended to assign private IP addresses for them.

The following table lists those reserved and available addresses by class.

Class	Address Range	Status
Class A	0.0.0.0	Reserved
	1.0.0.0 to 126.0.0.0	Available
	127.0.0.0	Reserved
Class B	128.0.0.0 to191.254.0.0	Available
	191.255.0.0	Reserved
Class C	192.0.0.0	Reserved
	192.0.1.0 to 223.255.254.0	Available
	223.255.255.0	Reserved
Class D	224.0.0.0 to 239.255.255.255	Available
Class E	240.0.0.0 to 255.255.255.254	Reserved
	255.255.255.255	Multicast

There are three blocks of IP addresses reserved for private networks that are not used in the Internet. Address translation is required for a private network

using one of these IP addresses to access the Internet. The following table details these addresses, which are defined in RFC 1918.

Class	IP Address Range	Network Numbers
Class A	10.0.0.0 to 10.255.255.255	1
Class B	172.16.0.0 to 172.31.255.255	16
Class C	192.168.0.0 to 192.168.255.255	256

For the information on the assignment of IP address, TCP/UDP port and other codes, please refer to RFC 1166.

1.1.2 IP Address Configuration Task List

The IP address configuration task list includes the following tasks, only the first one is required, others are optional depending on your network requirements.

- Assigning IP Addresses to Network Interfaces (Required)
- Configuring Address Resolution Protocol (ARP) (Optional)
- Configuring IP address to WAN Address Translation (Optional)
- Disabling IP Routing (Optional)
- Handling Broadcast Packets (Optional)

1.1.2.1 Assigning IP Addresses to Network Interfaces

Only a host has an IP address configured can it receive and send IP packets. If an interface is configured with an IP address, this means that the interface supports running the IP protocol.

To assign an IP address to an interface, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip address** *ip-address mask*	Assign an IP address for the interface.
DES-7200(config-if)# **no ip address**	Remove the IP address configuration for the interface.

A 32-bit mask identifies the network part of an IP address. In a mask, the IP address bit corresponding to 1 represetns network ID and the IP address bit corresponding to 0 represents host ID. For example, the mask corresponding a Class A IP address is 255.0.0.0. You can partition a network into multiple

segments with a mask. The goal of network partition is to use some bits of the host address of an IP address as the network address to reduce hosts and increase networks. At this point, the mask is called subnet mask.

Note

Theoretically, any bit of the host address of an IP address can be used as the subnet mask. DES-7200 product only supports continuous subnet masks from left to right starting from the network ID.

The interface-related IP address configuration task list includes the following tasks, only the first one is required, others are optional depending on your network requirements.

- Assigning multiple IP addresses to an interface

1.1.2.1.1 Assigning multiple IP addresses to an interface

DES-7200 product supports assigning multiple IP addresses for an interface with one being the primary IP address and others being the secondary addresses. Theoretically, you can configure secondary addresses up your mind. A secondary IP address can reside in the same or different network with the primary IP address. The secondary IP address will be used frequently during the building of a network, for example, in the following cases:

- There may not enough host addresses for a network. For example, a LAN requires a Class C IP address to support up to 254 hosts. However, when there are more than 254 hosts in the LAN, another Class C IP address is necessary. Therefore, a host needs to connect two networks and thus needs configuring multiple IP addresses.
- Many older networks were built based on layer 2 bridges without partition. The use of secondary IP addresses makes them easy to upgrade to IP-based routing networks. An IP address is assigned for every device in a subnet.
- Two subnets of a network might otherwise be separated by another network. By creating a subnet in each separated subnets, you can connect the two separated subnets together by assigning secondary IP addresses. One subnet cannot appear on two or more interfaces in a device.

Note

Before configuring secondary IP addresses, you need to confirm that the primary IP address has been configured. All the devices in a network should have the same secondary IP address. If you assign a secondary IP address to a device but do not assign IP addresses for other devices, you can set it to the primary IP address for them.

To assign a secondary IP address to an interface, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip address** *ip-address mask* **Secondary**	Assign a secondary IP address to the interface.
DES-7200(config-if)# **no ip address** *ip-address* *mask* **secondary**	Remove the secondary IP address configuration for the interface.

1.1.2.2 Configuring Address Resolution Protocol (ARP)

Every device in a LAN has two addresses: local address and network address. Local address is contained in the header of the frames on the data link layer. Disputably, the correct term is data link layer address. Since this local address is handled in the MAC sub-layer of the data link layer, it is normally called MAC address representing an IP network device in a network. Network address represents a device in the Internet and indicates the network to which the device belongs.

For inter-communication, a device in a LAN must know the 48-bit MAC address of another device. The ARP can resolve the MAC address upon an IP address and the reversed ARP (RARP) can resolve the IP address upon a MAC address. You can resolve the MAC address in two ways: ARP and Proxy ARP. For the information on ARP, Proxy ARP and RARP, refer to RFC 826, RFC 1027, and RFC 903.

ARP binds the IP and MAC Address. It can resolve the MAC address upon an IP address. Then, the relationship between the IP address and the MAC address is stored in the ARP cache. With the MAC address, a device can encapsulate the frames of the data link layer and send them to the LAN in the Ethernet II-type by default. However the frames can also be encapsulated into other types of Ethernet frame (for example, SNAP).

The principle of RARP is similar to ARP. RARP resolves the IPaddress upon a MAC address. RARP is configured on non-disk workstation in general.

Normally, a device can work without any special address resolution configuration. DES-7200 product can manage address resolution by.

- Configuring ARP Statically
- Setting ARP Encapsulations
- Setting ARP Timeout

1.1.2.2.1 Configuring ARP Statically

The ARP offers dynamic IP address to MAC address mapping. It is not necessary to configure ARP statically in most cases. By configuring ARP Sstatically, DES-7200 product can respond to the ARP request from other IP addresses.

To configure static ARP, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **arp** *ip-address mac-address arp-type*	Define static ARP. Only arpa type is supported for arp-type.
DES-7200(config)# **no arp** *ip-address*	Remove static ARP

1.1.2.2.2 Setting ARP Encapsulations

So far DES-7200 products only support Ethernet II type ARP encapsulations, also known as ARPA keyword.

1.1.2.2.3 ARP Timeout Setting

ARP timeout takes effect for only the dynamically learned IP address to MAC address mapping. The shorter the timeout, the truer the mapping table saved in the ARP cache is , but the more network bandwidth the ARP occupies. Hence the advantages and disadvantages should be weighted. Generally it is not necessary to configure the ARP timeout time unless there is a special requirement.

To configure ARP timeout time, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **arp timeout** *seconds*	Configure the ARP timeout time in the range from 0 to 2147483, with 0 not being aged.
DES-7200(config-if)# **no arp timeout**	Remove the configuration.

By default, timeout time is 3600 seconds, that is, 1 hour.

1.1.2.3 Disabling IP Routing

IP routing feature is enabled by default. Do not execute this command unless you sure that IP routing is not needed. Disabling IP routing will make the equipment lose all the routes and the route forwarding function.

To disable IP routing, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **no ip routing**	Disable IP routing.
DES-7200(config)# **ip routing**	Enable IP routing

Note

The switch performs the checking of ip checksum towards the routing packets. If the ip checksum error occurs, the routing halts. To this end, the unicast packets will be discarded directly and the multicast packets will only be forwarded on Layer 2.

1.1.2.4 Handling Broadcast Packets

A broadcast packet is destined for all hosts in a physical network. DES-7200 product supports two kinds of broadcast packets: directed broadcast and flooding. A directed broadcast packet is sent to all the hosts in a specific network that the host IDs of their IP addresses are all set to 1. While a flooding broadcast packet is sent to all the hosts whose IP addresses are all set to 1. Broadcast packets are heavily used by some protocols, including the Internet protocol. Therefore, it is the basic responsibility for a network administrator to manage and control broadcast packets.

Forwarding flooding broadcast packets may make the network overburden and thus influencing network operation. This is known as broadcast storm. There are some ways to supress and restrict broadcast storm in the local network. However, layer 2 network devices like bridges and switches will forward and propagate broadcast storm.

The best solution to solve the broadcast storm problem is to specify a broadcast address for each network, that is, directed broadcast. This requires the IP protocol to use directed broadcast instead of flooding broadcast if possible.

For detailed description about broadcast, refer to RFC 919 and RFC 922.

To handle broadcast packets, perform the following tasks according to the network requirement.

- Enabling Directed Broadcast-to-Physical Broadcast Translation
- Establishing an IP Broadcast Address

1.1.2.4.1 Enabling Directed Broadcast-to-Physical Broadcast Translation

A directed broadcast IP packet is the one destined to the broadcast address of an IP subnet. For instance, the packet destined to 172.16.16.255 is a directed

broadcast packet. However, the node that generates this packet is not a member of the destination subnet.

Upon the receipt of directed broadcast IP packets, the device indirectly connecting the destination subnet will forward the packets in the same way as forwarding unicast packets. After the directed broadcast IP packets arrive the device directly connecting the subnet, the device transforms them into flooding broadcast IP packets (whose destination address is all 1s in general), and then send them to all the hosts within the subnet by means of broadcast on the link layer.

Enabling directed broadcast to physical broadcast translation on an interface allows the itnerface to forward the directed broadcast IP packets to the directly connected network. This command will only affect the transmission of the directed broadcast IP packets to the final destination subnet, not other directed broadcasts.

You can forward directed broadcast IP packets as required an interface by defining ACLs. Only those IP packets matching the ACLs are translated from directed broadcasts to physical broadcasts.

To configure the directed broadcast-to-physical broadcast translation, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip directed-broadcast** [*access-list-number*]	Enable directed broadcast to physical broadcast translation on the interface.
DES-7200(config-if)# **no ip directed-broadcast**	Disable the translation.

1.1.2.4.2 Establishing an IP Broadcast Address

Currently, the most popular way is the destination address consisting of all 1s (255.255.255.255). DES-7200 product can be configured to generate any form of IP broadcast address and receive any form of IP broadcast packets.

To set a broadcast IP address other than 255.255.255.255, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip broadcast-address** *ip-address*	Create a broadcast address.
DES-7200(config-if)# **no ip broadcast-address**	Remove the configuration.

1.1.3 Monitoring and Maintaining IP Address

To monitor and maintain your network, perform the tasks described in the following sections.

- Clearing Caches and Tables
- Displaying System and Network Status

1.1.3.1 Clearing Caches and Tables

You can remove all contents of a particular cache, table, or database, including:
1) Clearing ARP cache;

2) Clearing the hostname to IP address mapping table;

3) Clearing the routing tables.

Command	Function
DES-7200# **clear arp-cache**	Clear the ARP cache.
DES-7200# **clear ip route** {*network* [*mask*] | *}	Clear the routing table.

1.1.3.2 Displaying System and Network Status

You can show the contents of the IP routing table, cache, and database. Such information is very helpful in troubleshooting the network. You also can display information about reachability of local network and discover the routing path that the packets of your device are taking through the network.

To display system and network status, execute the following commands in the privileged mode :

Command	Function
DES-7200# **show arp**	Show the ARP table.
DES-7200# **show ip arp**	Show the IP ARP table.
DES-7200# **show ip interface** [*interface-type interface-number*]	Show the interface information.
DES-7200# **show ip route** [*network* [*mask*]]	Show the routing table.

Command	Function
DES-7200#**show ip route**	Show the brief information of the routing table.
DES-7200# **ping** *ip-address* [**length** *bytes*] [**ntimes** *times*] [**timeout** *seconds*]	Test network reachability.

1.1.4 IP Address Configuration Examples

This chapter provides some IP address configuration examples as follows:

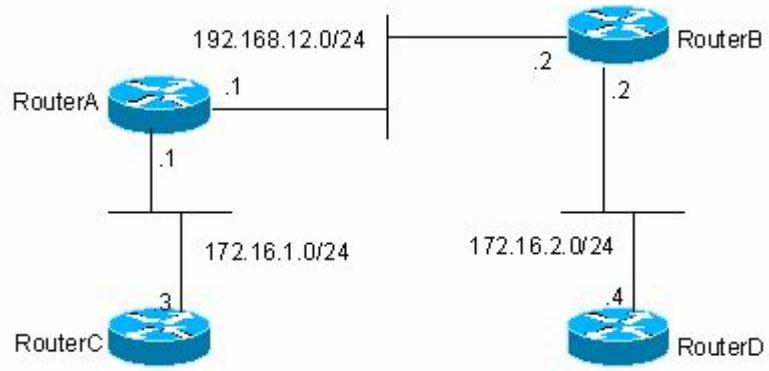
- Secondary IP Address Configuration Example

1.1.4.1 Secondary IP Address Configuration Example

Configuration requirements:

Figure 19-1 shows IP address assignment and network device connection.

Secondary IP address configuration example



Configure RIPv1. You can see the routes of 172.16.2.0/24 on router C and the routes of 172.16.1.0/24 on router D.

Configuration of the Routers:

RIPv1 does not support classless-based routes. This means masks are not carried with routing advertisement. 172.16.1.0/24 and 172.16.2.0/24 that belong to the same netowrk are separated by the Class C network 192.168.12.0/2. Generally, router C and router D cannot routes from each other. According to one feature of RIP, the mask of the route to be received should be set to the same value as that of the interface network if the route and the interface network belong to the same network. By configuring routers A and B, you can build a secondary netowrk 172.16.3.0/24 on the network 192.168.12.0/24 to link

the two separated subnets. The following presents a configuraiton description of routers A and B.

Router A:

```
interface FastEthernet 0/0
ip address 172.16.3.1 255.255.255.0 secondary
ip address 192.168.12.1 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.1.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

Router B:

```
interface FastEthernet 0/0
ip address 172.16.3.2 255.255.255.0 secondary
ip address 192.168.12.2 255.255.255.0
!
interface FastEthernet 0/1
ip address 172.16.2.1 255.255.255.0
!
router rip
network 172.16.0.0
network 192.168.12.0
```

1.2 IP Service Configuration

1.2.1 IP Service Configuration Task List

The IP service configuration includes the following optional configuration tasks. You can perform the task according to the requirements:

- Configuring the default gateway
- Managing IP connections

1.2.2 Managing IP Connections

The IP protocol stack offers a number of services to control and manage IP connections. Internet Control Message Protocol (ICMP) provides many of these services. Once a network problem occurs, a router or access server will send an ICMP message to the host or other rotuers. For detailed information on ICMP, see RFC 792.

To manage various aspects of IP connections, perform the optional tasks described in the following sections:

- Enabling ICMP Protocol Unreachable Messages
- Enabling ICMP Redirect Messages
- Enabling ICMP Mask Reply Messages
- Setting the IP MTU
- Configuring IP Source Routing

1.2.2.1 Enabling the ICMP Protocol Unreachable Message

When a router receives a non-broadcast packet destined to it, and this packet uses an IP protocol that it cannot handle, it will return an ICMP protocol unreachable message to the source address. Similarly, if the router is unable to forward the packet because it knows of no route to the destination address, it sends an ICMP host unreachable message. This feature is enabled by default.

To enable this service, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip unreachables**	Enable the ICMP protocol unreachable and host unreachable messages.
DES-7200(config-if)# **no ip unreachables**	Disable the ICMP protocol unreachable and host unreachable messages.

1.2.2.2 Enabling the ICMP Redirect Message

Routes are sometimes less than optimal. For example, it is possible for the device to be forced to resend a packet through the same interface on which it was received. If the device resends a packet through the same interface on which it was received, it sends an ICMP redirect message to the originator of the packet telling the originator that the gateway to this destination address is another device in the same subnet. Therefore the originator will transmit the packets based on the optimized path afterwards. This feature is enabled by default.

To enable the ICMP redirect message, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip redirects**	Enable the ICMP redirect message. It is enabled by default.

Command	Function
DES-7200(config-if)# **no ip redirects**	Disable the ICMP redirect message.

1.2.2.3 Enabling the ICMP Mask Reply Message

Occasionally, a network device needs to know the mask of a subnetwork in the Internet. To obtain this information, the device can send the ICMP mask request message. The receiving device will send the ICMP mask reply message. DES-7200 product can respond the ICMP mask request message. This function is enabled by default.

To enable the ICMP mask reply message, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip mask-reply**	Enable the ICMP mask reply message.
DES-7200(config-if)# **no ip mask-reply**	Disable the ICMP mask reply message.

1.2.2.4 Setting the IP MTU

All interfaces have a default MTU (Maximum Transmission Unit) value. All the packets which are larger than the MTU have to be fragmented before sending. Otherwise it is unable to be forwarded on the interface.

DES-7200 product allows you to adjust the MTU on an interface. Changing the MTU value can affect the IP MTU value, and the IP MTU value will be modified automatically to match the new MTU. However, changing the IP MTU value has no effect on the value of MTU.

The interfaces of a device in a physical network should have the same MTU for a protocol.

To set the IP MTU, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip mtu** *bytes*	Set the MTU in the range 68 to 1500 bytes.
DES-7200(config-if)# **no ip mtu**	Restore the setting to the default.

1.2.2.5 Configuring IP Source Routing

DES-7200 product supports IP source routing. Upon receiving an IP packet, the device will check its IP header like strict source route, loose source route and

recorded route, which are defined in RFC 791. If one of these options is enabled, the device performs appropriate action. Otherwise, it sends an ICMP error message to the source and then discards the packet. Our product supports IP source routing by default.

To enable IP source routing, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config)# **ip source-route**	Enable IP source routing.
DES-7200(config)# **no ip source-route**	Disable IP source routing.

Note

For DES-7200 series, due to the limitation of the hardware chip, the command **trap ip option packet** shall be used to notify the hardware of sending the packets with optional items to the software for handling.

2 IPv6 Configuration

2.1 IPv6 Overview

As the Internet is growing rapidly and the IPv4 address space is exhausting, the limitation of the IPv4 is more obvious. The research and practice of the next generation of the Internet Protocol becomes popular. Furthermore, the IPng workgroup of the IETF determines the protocol specification of IPng referred to as IPv6. Refer to RFC2460 for details.

Key Features of Ipv6:

- More Address Space

The length of address will be extended to 128 bits from the 32 bits of Ipv4. Namely, there are 2^128-1 addresses for IPv6. The IPv6 adopts the hierarchical address mode and supports multiple-level IP address assignment, for example, from the Internet backbone network to the internal subnet of enterprises.

- Simplified Format of Packet Header

The design principle of new IPv6 packet header is to minimize the overhead. For this reason, some non-critical fields and optional fields are removed from the packet header and placed into the extended packet header. The length of the IPv6 address is 4 times of IPv4 address; its packet header is only 2 times of IPv4 header. The improved IPv6 packet header is more efficient for forwarding, for instance, there is no checksum in the IPv6 packet header and it is not necessary for the IPv6 router to process the fragment during forwarding (the fragment is completed by the originator).

- High-efficient hierarchical Addressing and Routing Structure

The IPv6 adopts the aggregation mechanism and defines flexible hierarchical addressing and routing structure, and several networks at the same level is presented as a unified network prefix at the higher level of routers. So it obviously reduces the entries that the router must maintain and greatly minimizes the routing and storage overhead.

- Simple Management: Plug and Play

Simplify the management and maintenance of the network node by the implementation of a series of auto-discovery and auto-configuration functions. Such as the Neighbor Discovery, the MTU Discovery, the Router Advertisement, the Router Solicitation and

the Auto-configuration technologies provide related service for the plug and play. It should be mentioned that the IPv6 supports such address configuration methods as the stateful and the stateless. In the IPv4, the dynamical host configuration protocol (DHCP) implements the automatic setting of the host IP address and related configuration, while the IPv6 inherits this auto-configuration service of the IPv4 and refers to it as the Stateful Auto-configuration. Furthermore, the IPv6 also adopts an auto-configuration service, referred to as the Stateless Auto-configuration. During the stateless auto-configuration, the host obtains the local address of the link, the address prefix of local device and some other related configuration information automatically.

- Security

The IPSec is an optional extended protocol of the IPv4, while it is only a component of the IPv6 used to provide security. At present, the IPv6 implements the Authentication Header (AH) and Encapsulated Security Payload (ESP) mechanisms. Where, the former authenticates the integrity of the data and the source of the IP packet to ensure that the packet does come from the node marked by the source address, while the latter provides the data encryption function to implement the end-to-end encryption.

- More Excellent QoS Support

The new field in the IPv6 packet header defines how to identify and process the data flow. The Flow Label field in the IPv6 packet header is used to identify the data flow ID, by which the IPv6 allows users to put forward the requirement for the QoS of communication. The router can identify all packets of some specified data flow by this field and provide special processing for these packet on demand.

- Neighbor Nodes Interaction-specific New Protocol

The Neighbor Discovery Protocol of the IPv6 uses a series of IPv6 control information message (ICMPv6) to carry out the interactive management of the neighbor nodes (the nodes of the same link). The Neighbor Discovery Protocol and high-efficient multicast and unicast Neighbor Discovery message replace previous broadcast-based address resolution protocol (ARP) and the ICMPv4 router discovery message.

- Extensibility

The IPv6 provides powerful extensibility and the new features can be added to the extended packet header after the IPv6 packet header. Unlike the IPv4, the packet header can only support the option of up to 40 bytes, while the size of the IPv6 extended packet header is only limited by the maximum bytes of the whole IPv6 packet.

The IPv6 supports the following features:

- IPv6 Protocol
- IPv6 Address Format
- Type of IPv6 Address

- ICMPv6
- IPv6 Neighbor Discovery
- Path MTU Discovery
- ICMPv6 Redirection
- Address Conflict Detection
- IPv6 Stateless Auto-configuration
- IPv6 Address Configuration
- IPv6 Route Forwarding (supporting static route configuration)
- Configuration of various IPv6 parameters
- Diagnosis Tool **Ping IPv6**

2.1.1 IPv6 Address Format

The basic format of an IPv6 address is X : X : X : X : X : X : X : X, where X is a 4 hex integers (16 bits). Each digit contains 4 bits of information, each integer contains 4 hex digits and each address contains 8 integers, so it is total for 128 bits. Some legal IPv6 addresses are as follows:

2001:ABCD:1234:5678:AAAA:BBBB:1200:2100

800 : 0 : 0 :0 : 0 : 0 : 0 : 1

1080 : 0 : 0 : 0 : 8 : 800 : 200C : 417A

These integers are hex integers, where A to F denote 10 to 15 respectively. Each integer in the address must be denoted and the starting 0 needs not be denoted. Some IPv6 address may contain a series of 0s (such as the examples 2 and 3). Once this condition occurs, the ": :" is allowed to denote this series of 0s. Namely, the address 800:0:0:0:0:0:0:1 can be denoted as: 800 :: 1.

These two colons denote that this address can be extended to the complete 128-bit address. In this way, the 16-bit group can be replaced with two colons only when they are all 0s and the two colons can only present for one time.

In the mixture environment of IPv4 and IPv6, there is a mixture denotation method. The lowest 32 bits in an IPv6 address can be used to denote an IPv4 address. The address can be expressed in a mixture mode, i.e., X: X : X : X : X : X : d . d . d . d. Where, the X denotes a 16-bit integer, while d denotes an 8-bit decimal integer. For instance, the address 0 : 0 : 0 : 0 : 0 : 0 : 192 .168 . 20 : 1 is a legal IPv6 address. After the abbreviated expression method is used, this address can be denoted as follows: : : 192.168. 20. 1. One of the typical example is the IPv4-compatible IPv6 address, which is expressed in the "::A.B.C.D" mode, i.e., "::1.1.1.1"; the other typical example is the IPv4-mapped IPv6 address, which is expressed in the "::FFFF:A.B.C.D" and used to invert the IPv6 address to the IPv6 address, i.e., map the IPv4 address"1.1.1.1" to the IPv6 address"::FFFF:1.1.1.1".

For the IPv6 address is divided into two parts such as the subnet prefix and the interface identifier, it can be denoted as an address with additional numeric value by the method like the CIDR address. Where, this numeric value indicates how many bits represent the network part (the network prefix). Namely the IPv6 node address indicates the length of the prefix, and the length is differentiated from the IPv6 address by the slash. For instance: 12AB::CD30:0:0:0:0/60,The length of the prefix used for routing in this address is 60 bits.

2.1.2 Type of IPv6 Address

In RFC4291, there are the following three defined types of IPv6 addresses:

- Unicast: Identifier of a single interface. The packet to be sent to a unicast address will be transmitted to the interface identified by this address.
- Anycast: Identifiers of a set of interfaces. The packet to be sent to an anycast address will be transmitted to one of the interfaces identified by this address (select the nearest one according to the routing protocol).
- Multicast: Identifiers of a set of interfaces (In general, they are of different nodes). The packet to be sent to a Multicast address will be transmitted to all the interfaces which are added to this multicast address.

Caution

The broadcast address is not defined in the IPv6.

The following will introduce these types of addresses one-by-one:

2.1.2.1 Unicast Addresses

The unicast address is divided into unspecified address, loopback address, link-level local address, site-level local address and global unicast address. Now the site-level local address has been repealled, the unicast addresses excepting for the unspecified address, loopback address and thhe link-level local address are all global unicast addresses.

1. Unspecified Address

The unspecified address is 0:0:0:0:0:0:0:0, generally abbreviated as ::.

(1) If there is no unicast address when the host is rebooting, use the unspecified address as the source address, send the router request and obtain the prefix information from the gateway to auto-generate the unicast address.

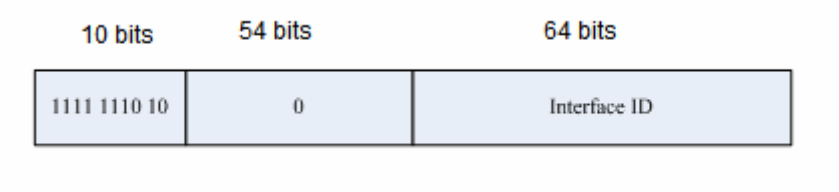
(2) When configuring the IPv6 address for the host, check whether the IPv6 address conflicts with the address for other hosts in the same network segment or not. If so, use the unspecified address as the source address to send the neighbor request message.

2. Loopback Address

The loopback address is 0:0:0:0:0:0:0:1, abbreviated as ::1, which is equal to the IPv4 address 127.0.0.1 and used when the node sends the packets to itself.

3. Link-level Local Address

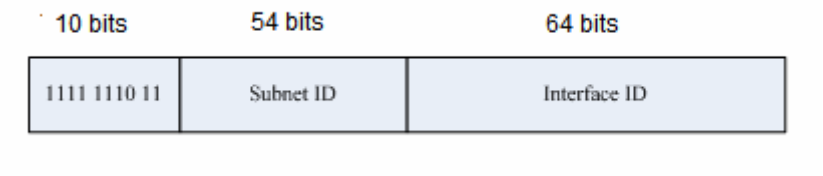
The format of link-level local address:



The link-level local address is used to number the host on the single network link. The address of former 10-bit identification for the prefix is the link-level local address. The router will not forward the message of the source address or the destination address with the link-level local address forever. The intermediate 54-bit of this address is 0. The latter 64 indicates the interface identifier, this part allows the single network to connect to up to 2^{64}-1 hosts.

4. Site-level Local Address

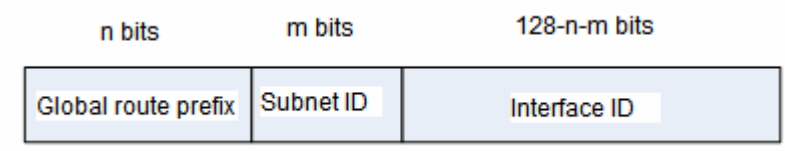
The format of site-level local address:



The site-level local address can be taken to transmit the data within the site, and the router will not forward the message of the source address or the destination address with the site-level local address to Internet. Namely, such packet route can only be forwarded within the site, but cannot be forwarded to out of the site. Suppose that the site is the LAN for a company, the site-level local address is similar to the IPv4 private address, i.e., 192.168.0.0/16. The RFC3879 has repealled the site-level local address.

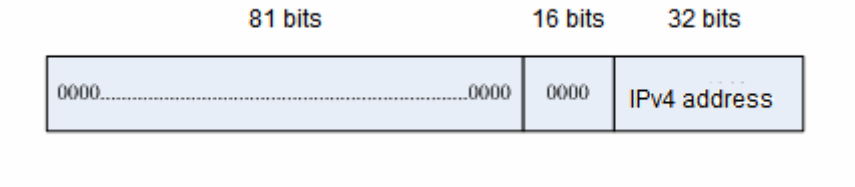
5. Global Unicast Address

The format of global unicast address:

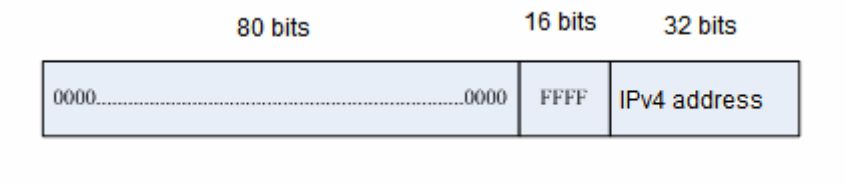


One class of the global unicast address is the IPv6 address embedded with IPv4 address, which is used to interconnect the IPv4 nodes and the IPv6 nodes and divided into IPv4-compatible IPv6 address and the IPv4-mapped IPv6 address.

The format of IPv4-compatible IPv6 address:



The format of IPv4-mapped IPv6 address:



The IPv4-compatible IPv6 address is mainly used to the automatic tunneling, which supports both the IPv4 and IPv6. The IPv4-compatible IPv6 address will transmit the IPv6 packet via the IPv4 router in the tunneling way. Now the IPv4-compatible IPv6 address has been repealled. The IPv6 address of an IPv4 mapping is used to access the nodes that only support IPv4 by IPv6 nodes. For example, when one IPv6 application of the IPv4/IPv6 host requests the resolution of a host name (the host only supports IPv4), the name server will internally generate the IPv6 addresses of the IPv4 mapping dynamically and return them to the IPv6 application.

2.1.2.2 Multicast Addresses

The format of the IPv6 multicast address is shown as follows:

```
|    8     |  4 |  4 |                   112 bits                   |
+----------+----+----+----------------------------------------------+
|11111111|flgs|scop|                   group ID                     |
+----------+----+----+----------------------------------------------+
```

The first byte of the address format is full 1, which denote a multicast address.

- Flag field:

It consists of 4 bits.At present, only the fourth bit is specified. The bit is used to indicate whether the address is a known multicast address specified by Internet Number Constitution or a temporary multicast address used in a specific condition. If this flag

bit is 0, it indicates this address is a known multicast address. If this bit is 1, it indicates that this address is a temporary one. Other 3 flag bits are reserved for future use.

- Range field:

Composed of 4 bits and used to denote the range of multicast. Namely, whether the multicast group contains the local node, the local link and the local site or any position nodes in the IPv6 global address space.

- Group Identifier field:

112 bits long and used to identify a multicast group. Depending on whether a multicast address is temporary or known and the range of the address, a multicast identifier can denote different groups.

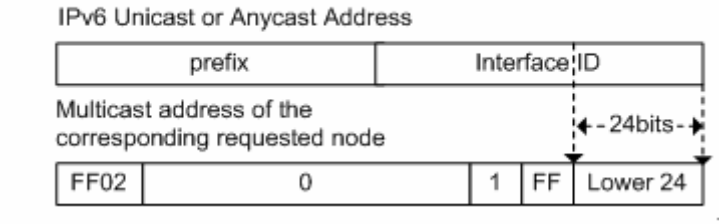
The multicast address of the IPv6 is this type of address taking FF00::/8 as the prefix One multicast address of an IPv6 usually identifies the interfaces of a serial of different nodes. When one message is sent to one multicast address, this message will be distributed to the interfaces of each node with this multicast address. One node (host or router) should add the following multicast:

- The multicast address of all nodes for the local link is FF02::1
- The prefix of the multicast address for the solicited node is FF02:0:0:0:0:1:FF00:0000/104

If they are routers, it is necessary to add the multicast address FF02::2 of all routers for the local link.

The multicast address of the solicited node corresponds to the IPv6 unicast and anycast address, so it is necessary for the IPv6 node to add corresponding multicast address of the solicited node for each configured unicast address and anycast address. The prefix of the multicast address for the solicited node is FF02:0:0:0:0:1:FF00:0000/104, another 24 bits are comprised of the unicast address or the lower 24 bits of the anycast address, for instance, the multicast address of the solicited node corresponding to the FE80::2AA:FF:FE21:1234 is FF02::1:FF21:1234,

The multicast address of solicited node is usually used to the neighbor solicitation (NS) message. The format of the solicited node is shown as follows:



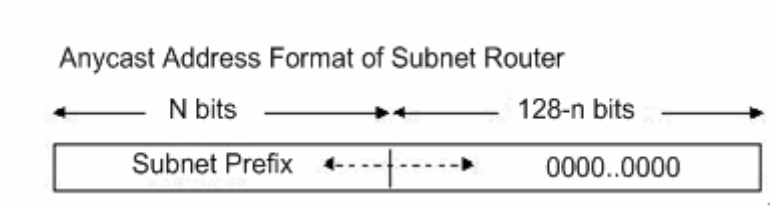
2.1.2.3 Anycast Addresses

The anycast address is similar with the multicast address as more than one node shares an anycast address. The difference is that only one node expects to receive the data packet of the anycast address, while all nodes of the multicast address members expect to receive all packets sending to this address. The anycast address is assigned to normal IPv6 unicast address space, so the anycast address cannot be differentiated from the unicast address from the style. For this reason, each member of all anycast addresses has to be configured explicitly to identify the anycast address.

Caution The anycast address can only be assigned to the router, but cannot be assigned to the host. Furthermore, the anycast address cannot be taken as the source address of the message.

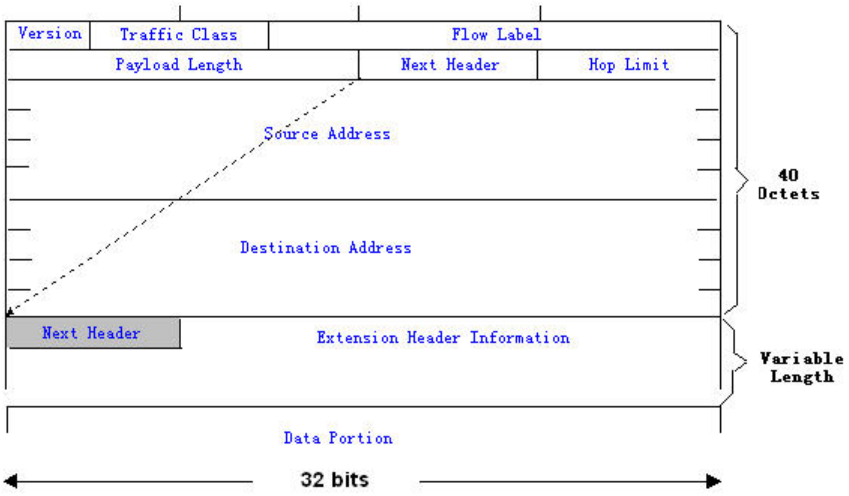
The RFC2373 predefines an anycast address, referred to as the anycast address of the subnet router. The following diagram shows the anycast address format of the subnet router, which consists of the subnet prefix followed by a series of 0s (as the interface identifier).

Where, the subnet prefix identifies a specified link (subnet) and the packet to be sent to the anycast address of the subnet router will be distributed to a router of this subnet. The anycast address of the subnet router is usually used for some node which needs to communicate with one router of the remote subnet.



2.1.3 IPv6 Packet Header Structure

The format of the IPv6 packet header is shown as the figure below:



The IPv4 packet header takes 4 bytes as the unit; the IPv6 packet header takes 8 bytes as the unit and the total length of the packet header is 40 bytes. In the IPv6 packet header, the following fields are defined:

- Version:

The length is 4 bits. For IPv6, the field must be 6.

- Traffic Class:

The length is 8 bits. It indicates a type of service provided to the packey and is equal to the “TOS” in the IPv4.

- Flow Label:

The length is 20 bits used to identify the packets of the same service flow. One node can be taken as the sending source of several service flows. Flow label and source node IP address identify a service flow uniquely.

- Payload Length:

The length is 16 bits, including the byte length of payload and the length of various IPv6 extension options (if any). In other words, it includes the length of an IPv6 packet except for the IPv6 header itself.

- Next Header:

This field indicates the protocol type in the header field following the IPv6 header. Similar to the IPv4 protocol field, the Next Header field can be used to indicate whether the upper level is TCP or UDP. It can also be used to indicate whether an extended IPv6 header exists.

- Hop Limit:

The length is 8 bits. When one router forwards the packet for one time, this field will reduce 1. If this field is 0, this packet will be discarded. It is similar to the life span field in the IPv4 packet header.

- Source Address (Source Address):

The length is 128 bits. It indicates the sender address of an IPv6 packet.

- Destination Address (Destination Address):

The length is 128 bits. It indicates the receiver address of an IPv6 packet.

At present, the following extended headers are defined for the IPv6:

- Hop-by-Hop Options:

This extended header must directly follow an IPv6 header. It contains the option data that must be checked by each node along the path.

- Routing Header (Routing (Type 0)):

This extended header indicates the nodes that a packet will go through before reaching the destination. It contains the address table of various nodes that the packet goes through. The initial destination address of the IPv6 header is the first one of a series of addresses in the route header, other than the final destination address of the packet. After receiving this packet, the node of this address will process the IPv6 header and the routing header, and send the packet to the second address of the routing header list. It repeats this step until the packet reaches the final destination.

- Fragment Header (Fragment):

This extended header is used to fragment the packets longer than the MTU of the path between the source node and destination node.

- Destination Option Header (Destination Options):

This extended header replaces the IPv4 option field. At present, the only defined destination option is to fill the option with an integer multiple of 64 bits (8 bytes) when necessary. This extended header can be used to carry the information checked by the destination node.

- Upper-layer Extended Header (Upper-layer header):

It indicates the the upper layer transmission protocol, such as TCP(6) and UDP(17).

Furthermore, the extended header of the Authentication and the Encapsulating Security Payload will be described in the IPSec section. At present, the IPv6 implemented by us cannot support the IPSec.

2.1.4 IPv6 Path MTU Discovery

As with the path MTU discovery of the IPv4, the path MTU discovery of the IPv6 allows one host to discover and adjust the size of the MTU in the data transmission path.

Furthermore, when the data packet to be sent is larger than the MTU of the data transmission path, the host will fragment the packets by itself. This behavior makes it not necessary for the router to process the fragment, and thus save resources and improve the efficiency of the IPv6 network.

Caution

The minimum link MTU is 68 bytes in the IPv4, indicating that the links along the path over which the packets are transmitted should support at least the link MTU of 68 bytes. The minimum link MTU is 1280 bytes in the IPv6. It is strongly recommended to use the link MTU of 1500 bytes for the link in the IPv6.

2.1.5 IPv6 Neighbor Discovery

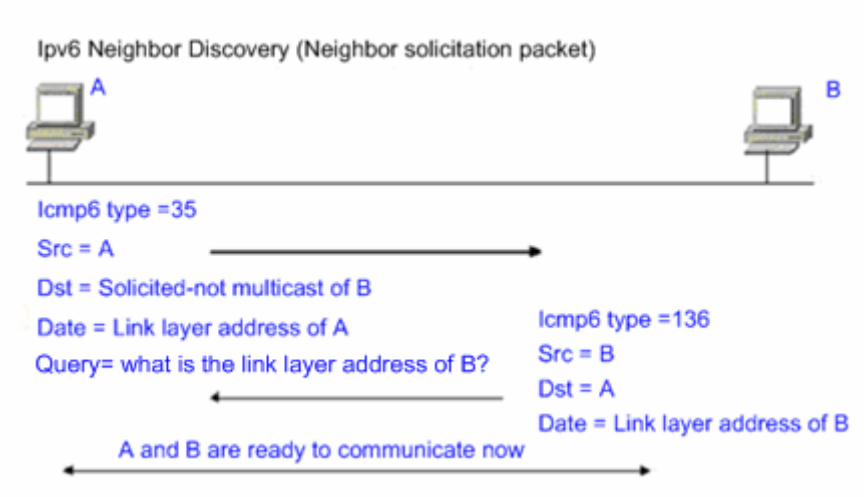
The main functions of the IPv6 Neighbor discovery protocol include Router Discovery, Prefix Discovery, Parameter Discovery, Address Auto-configuration, Address Resolution(ARP), Next-hop Confirmation, Neighbor Unreachability Check, Address Conflict Check and Redirection. Neighbor discovery defines 5 types of ICMP message, which are Router Solicitation(ICMP type133), Router Advertisement(ICMP type134), Neighbor Solicitation or ARP request (ICMP type135), Neighbor Advertisement or APR response(ICMP type136) and ICMP redirection message(ICMP type137).

The following describes the neighbor discovery function in detail:

2.1.5.1 Address Resolution

A node must get the link layer address of another node before communicating with it. At this time, it should send the neighbor solicitation (NS) message to the solicitated multicast address of the IPv6 address of the destination node. The NS message also contains the link layer address of itself. After receiving this NS message, the destination node responds with a message, referred to as neighbor advertisement (NA), with its link layer address. After receiving the response message, the source node can communicate with the destination node.

The following is the neighbor solicitation procedure:



2.1.5.2 Neighbor Unreachability Detection

Enabling the Neighbor Unreachability Detection function to send the IPv6 unicast packet to the neighbor whose reachable time expires.

Neighbor Unreachability Detection and sending the IPv6 packet to the neighbor can be co-processed. During the detection, it continues to forward the IPv6 packet to the neighbor.

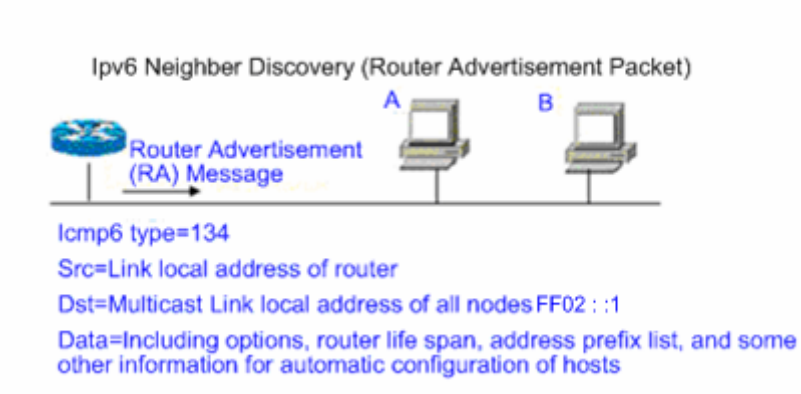
2.1.5.3 Address Conflict Detection

After configuring the IPv6 address to the host, enabling the address conflict detection function to check whether the IPv6 address in the link is sole or not.

2.1.5.4 Router, Prefix and Parameter Advertisement

The router sends the Router Advertisement (RA) to all the local nodes of the link periodically.

The following figure shows the process of sending the Router Advertisement (RA):



In general, the Router Advertisement (RA) contains the contents below:

- One or more IPv6 address prefixes used for the on-link confirmation or the stateless address auto-configuration.
- Effective period of the IPv6 address prefix.
- Usage of the host auto-configuration (Stateful or stateless).
- Information for the default router (namely, determine whether this router is taken as the default router. If yes, it will announce the time as the default router itself).
- Other information for configuration such as the hop limit, the MTU and the neighbor solicitation retransmission interval.

The Router Advertisement (RA) is also used to respond to the Router Solicitation (RS) message sent by the host. The Router Solicitation (RS) message allows the host to obtain the auto-configuration information immediately without waiting for the router to send the Router Advertisement (RA). If there is no unicast address when the host is activated, the Router Solicitation (RS) message sent by the host will use the unassigned address (0:0:0:0:0:0:0:0) as the source address of the solicitation message. Otherwise, the existing unicast address is taken as the source address, while the Router Solicitation (RS) message uses the multicast address (FF02::2) of all routers for the local link as the destination address. As the response router solicitation (RS) message, the Router Advertisement (RA) message will use the source address of the solicitation message as the destination address (if the source address is the unassigned address, it will use the multicast address FF02::1) of all nodes for the local link.

The following parameters can be configured in the Router Advertisement (RA) message:

Ra-interval: Interval of sending the Router Advertisement (RA).

Ra-lifetime: Router lifetime, namely whether the device is acted as the default router of the local link and the time as this role.

Prefix: IPv6 address prefix of the local link, which can be used for the on-link confirmation or the stateless address auto-configuration, including the configuration of other parameters for the prefix.

Rs-initerval: Interval of sending the neighbor solicitation message.

Reachabletime: Time maintained after considering the neighbor reachable.

We configure the above parameters in the IPv6 interface property.

Caution

1. By default, no Router Advertisement (RA) message is sent actively on the interface. To do so, you can use the command **no ipv6 nd suppress-ra** in the interface configuration mode.
2. In order to make the stateless address auto-configuration of the node work normally, the length of the prefix for the router advertisement (RA) message should be 64 bits.

2.1.5.5 Redirection

After receiving the IPv6 packets, the router discovers the better next-hop and sends the ICMP redirection message to notify the host of the better next-hop. Next time the host sends the IPv6 packets to the better next-hop directly.

2.2 IPv6 Configuration

The following will introduce the configuration of various function modules of the IPv6 respectively:

2.2.1 Configuring IPv6 Address

This section describes how to configure an IPv6 address on an interface. By default, no IPv6 address is configured.

Caution

Once an interface is created and its link status is UP, the system will automatically generate the local link address for the interface. At present, the IPv6 doesn't support anycast address.

To configure an IPv6 address, execute the following commands in the global configuration mode:

Command	Meaning
DES-7200#**configure terminal**	Enter the global configuration mode.
DES-7200(config)#**interface** *interface-id*	Enter the interface configuration mode. Note that the **no switchport** command shall be used to switchover the layer-2 port to the layer-3 interface.
DES-7200(config-if)#**ipv6 enable**	Enable the IPv6 protocol on an interface. If this command is not run, the system automatically enables the IPv6 protocol when you configure an IPv6 address for an interface.
DES-7200(config-if)#**ipv6 address** *ipv6-address/prefix-length* DES-7200(config-if)#**ipv6 address** *ipv6-prefix/prefix-length* [**eui-64**]	Configure the IPv6 unicast address for this interface. The key word **Eui-64** indicates the generated IPv6 address consists of the configured address prefix and the 64-bit interface ID. Note: Whether the key word **eui-64** is used, it is necessary to enter the complete address format to delete an IPv6 address (Prefix + interface ID/prefix length). When you configure an IPv6 address on an interface, then the IPv6 protocol is automatically enabled on the interface. Even if you use **no ipv6 enable**, you cannot disable the IPv6 protocol.
DES-7200(config-if)#**end**	Return to the privileged EXEC mode.
DES-7200#**show ipv6 interface** *interface-id*	View the IPv6 interface information.
DES-7200#**copy running-config startup-config**	Save the configuration.

Use the **no ipv6 address** *ipv6-prefixIprefix-length* **[eui-64]** command to delete the configured IPv6 address.

The following is an example of the configuration of the IPv6 address:

```
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address fec0:0:0:1::1/64
```

```
DES-7200(config-if)# end
DES-7200(config-if)# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:00:00:00:00:01
INET6: fe80::200:ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

2.2.2 Configuring ICMPv6 Redirection

This section will describe how to configure the ICMPv6 redirection function on the interface. By default, the redirection function of the IPv6 on the interface is enabled. The router needs to send the redirection message to the source during packet forwarding in the following cases:

- The destination address of the message is not a multicast address;
- The destination address of the message is not the router itself;
- The output interface of the next hop determined by the device for this message is the same as the interface this message received, namely, the next hop and the originator is of the same link;
- The node identified by the source IP address of the packet is a neighbor of the local router. Namely, this node exists in the router's neighbor table.

Caution The router other than the host can generate the redirection message, and the router will not update its routing table when it receives the redirection message.

To enable redirection on the interface, execute the following commands in the global configuration mode:

Command	Meaning
DES-7200#**configure terminal**	Enter the global configuration mode.
DES-7200(config)#**interface** *interface-id*	Enter the interface configuration mode. Note that the **no switchport** command shall be used to switchover the layer-2 port to the layer-3 interface.
DES-7200(config-if)#**ipv6 redirects**	Enable the IPv6 redirection function.
DES-7200(config-if)#**end**	Return to the privileged EXEC mode.
DES-7200#**show ipv6 interface** *interface-id*	Show the interface configuration.
DES-7200#**copy running-config startup-config**	Save the configuration.

Use the **no ipv6 redirects** command to disable the redirection function. The following is an example to configure the redirection function:

```
DES-7200(config)# interface vlan 1
DES-7200 (config-if)# ipv6 redirects
DES-7200 (config-if)# end
DES-7200 # show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
```

```
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

2.2.3 Configuring Static Neighbor

This section will describe how to configure a static neighbor. By default, the static neighbor is not configured. In general, a neighbor learns and maintains its status by the Neighbor Discovery Protocol (NDP) dynamically. Moreover, you can configure the static neighbor manually.

To configure the static neighbor, execute the following commands in the global configuration mode.

Command	Meaning
DES-7200#**configure terminal**	Enter the global configuration mode.
DES-7200(config)#**ipv6 neighbor** *ipv6-address interface-id hardware-address*	Configure a static neighbor on the interface.
DES-7200(config)#**end**	Return to the privileged EXEC mode.
DES-7200#**show ipv6 neighbors**	View the neighbor list.
DES-7200#**copy running-config startup-config**	Save the configuration.

Use the **no ipv6 neighbor** command to delete the specified neighbor. The following is an example to configure a static neighbor on SVI 1:

```
DES-7200(config)# ipv6 neighbor fec0:0:0:1::100 vlan 1 00d0.f811.1234
DES-7200 (config)# end
DES-7200# show ipv6 neighbors verbose fec0:0:0:1::100
IPv6 Address       Linklayer Addr   Interface
fec0:0:0:1::100    00d0.f811.1234   vlan 1
State: REACH/H Age: - asked: 0
```

2.2.4 Configuring Address Conflict Detection

This section describes how to configure address conflict detection times. Address conflict detection is mandatory to assign unicast addresses to interfaces. The goal is to

dectect the uniqueness of an address. The address conflict detection should be carried out for the manual configuration address, the stateless auto-configuration address or the statefull auto-configuration address. However, it is not necessary to carry out the address conflict detection under the following two conditions:

- The management prohibits the address conflict detection, namely, the number of the neighbor solicitation messages sent for the address conflict detection is set to 0.
- The configured anycast address can not be applied to the address conflict detection.

Furthermore, if the address conflict detection function is not disabled on the interface, the system will enable the address conflict detection process for the configured address when the interface changes to the Up status from the Down status.

The following is the configuration procedure of the quantity of the neighbor solicitation message sent for the address conflict detection:

Command	Meaning
DES-7200#**configure terminal**	Enter the global configuration mode.
DES-7200(config)#**interface** *interface-id*	Enter the interface configuration mode. Note that the **no switchport** command shall be used to switchover the layer-2 port to the layer-3 interface.
DES-7200(config-if)#**ipv6 nd dad attempts** *attempts*	The quantity of the neighbor solicitation message sent for the address conflict detection. When it is configured to 0, any neighbor solicitation message is denied. Enable the address conflict detection function on the interface.
DES-7200(config-if)#**end**	Return to the privileged mode.
DES-7200#**show ipv6 interface vlan** *1*	View the IPv6 information on the interface.
DES-7200#**copy running-config startup-config**	Save the configuration.

Use the **no ipv6 nd dad attempts** command to restore the default value. The following is an example to configure the times of the neighbor solicitation (NS) message sent for the address conflict detection on the SVI1:

```
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 nd dad attempts 3
DES-7200(config-if)# end
DES-7200# show ipv6 interface vlan 1
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 nd dad attempts 3
DES-7200(config-if)# end
DES-7200# show ipv6 interface vlan 1
Interface vlan 1 is Up, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:0:0:1::1 , subnet is fec0:0:0:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 3
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

2.2.5 Configuring Other Interface Parameters

The IPv6 parameters on an interface fall into 2 parts, one is used to control the behavior of the router itself, the other is used to control the contents of the router advertisement (RA) sent by the router to determine what action should be taken by the host when it receives this router advertisement (RA).

The following will introduce these commands one by one:

Command	Meaning
DES-7200#**configure terminal**	Enter the global configuration mode.

Command	Meaning
DES-7200(config)#**interface** *interface-id*	Enter the interface configuration mode. Note that the **no switchport** command shall be used to switchover the layer-2 port to the layer-3 interface.
DES-7200(config-if)#**ipv6 enable**	Enable the IPv6 function.
DES-7200(config-if)#**ipv6 nd ns-interval** *milliseconds*	(Optional) Define the retransmission interval of the neighbor solicitation message, in ms, the default value is 1000ms.
DES-7200(config-if)#**ipv6 nd reachable-time** *milliseconds*	(Optional) Define the time when the neighbor is considered to be reachable, in ms, the default value is 30000ms. Note: as specified in RFC4861, the reachable time of a neighbor should be increased or decreased at random on the basis of the configured time in the range of 0.5 to 1.5 of the configured time.
DES-7200(config-if)#**ipv6 nd prefix** *ipv6-prefix/prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise**]]	(Optional) Set the address prefix to be advertised in the router advertisement (RA) message.
DES-7200(config-if)#**ipv6 nd ra-lifetime** *seconds*	(Optional) Set the TTL of the router in the router advertisement (RA) message, namely the time as the default router. 0, indicates that the router will not act as the default router of the direct-connected network. The default value is 1800s.

Command	Meaning
DES-7200(config-if)#**ipv6 nd ra-interval** {*seconds* **min-max** *min_value max_value*}	(Optional) Set the time interval for the router to send the router advertisement (RA) message periodically, in second, and the default value is 200s. With the **min-max** specified, the actual interval of the message sending is a random value between the minimum and maximum value. Without the **min-max** specified, the actual interval of the message sending is approximately 1.2/0.8*the configured value.
DES-7200(config-if)#**ipv6 nd managed-config-flag**	(Optional) Set the "managed address configuration" flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain the address when it receives this router advertisement (RA). By default, the flag bit is not configured for the router advertisement (RA) message.
DES-7200(config-if)#**ipv6 nd other-config-flag**	(Optional) Set the "other stateful configuration" flag bit of the router advertisement (RA) message, and determine whether the host will use the stateful auto-configuration to obtain other information other than the address when it receives this router advertisement (RA). By default, the flag bit is not configured for the router advertisement (RA) message.
DES-7200(config-if)#**ipv6 nd suppress-ra**	(Optional) Set whether suppress the router advertisement (RA) message in this interface. By default, the flag bit is not configured for the router advertisement (RA) message.
DES-7200(config-if)#**end**	Return to the privileged EXEC mode.
DES-7200#**show ipv6 interface** [*interface-id*] [**ra-info**]	Show the ipv6 interface of the interface or the information of RA sent by this interface.

Command	Meaning
DES-7200#**copy running-config startup-config**	(Optional) Save the configuration.

The **no** command of above commands can be used to restore the default value. For details, refer to *IPv6 Command Reference*.

2.3 IPv6 Monitoring and Maintenance

It is mainly used to provide related command to show some internal information of the IPv6 protocol, such as the ipv6 information, the neighbor table and the route table information of the interface.

Command	Meaning
Show ipv6 interface [*interface-id*] [**ra-info**]	Show the IPv6 information of the interface.
Show ipv6 neighbors [**verbose**] [*interface-id*] [*ipv6-address*]	Show the neighbor information.
Show ipv6 route [**static**] [**local**] [**connected**]	Show the information of the IPv6 routing table.

1. View the IPv6 information of an interface.

```
DES-7200# show ipv6 interface
interface vlan 1 is Down, ifindex: 2001
address(es):
Mac Address: 00:d0:f8:00:00:01
INET6: fe80::2d0:f8ff:fe00:1 , subnet is fe80::/64
INET6: fec0:1:1:1::1 , subnet is fec0:1:1:1::/64
Joined group address(es):
ff01:1::1
ff02:1::1
ff02:1::2
ff02:1::1:ff00:1
MTU is 1500 bytes
ICMP error messages limited to one every 10 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
```

```
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

2. View the information of the router advertisement (RA) message to be sent of an interface

```
DES-7200# show ipv6 interface ra-info
vlan 1: DOWN
RA timer is stopped
waits: 0, initcount: 3
statistics: RA(out/in/inconsistent): 4/0/0, RS(input): 0
Link-layer address: 00:00:00:00:00:01
Physical MTU: 1500
ND router advertisements live for 1800 seconds
ND router advertisements are sent every 200 seconds<240--160>
Flags: !M!O, Adv MTU: 1500
ND advertised reachable time is 0 milliseconds
ND advertised retransmit time is 0 milliseconds
ND advertised CurHopLimit is 64
Prefixes: (total: 1)
fec0:1:1:1::/64(Def, Auto, vltime: 2592000, pltime: 604800, flags: LA)
```

3. View the neighbor table information of the IPv6.

```
DES-7200# show ipv6 neighbors
IPv6 Address               Linklayer Addr  Interface
fe80::200:ff:fe00:1      0000.0000.0001 vlan 1
State: REACH/H Age: - asked: 0
fec0:1:1:1::1              0000.0000.0001 vlan 1
State: REACH/H Age: - asked: 0
```

3 IPv6 Tunnel Configuration

3.1 Overview

The IPv6 is designed to inherit and replace the IPv4. However, the evolution from the IPv4 to the IPv6 is a gradual process. Therefore, it is inevitable that these two protocols coexist for a period before the IPv6 completely replaces the IPv4. At the beginning of this transition stage, IPv4 networks are still main networks. IPv6 networks are similar to isolated islands in IPv4 networks. The problems about transition can be divided into the following two types:

1. Communications among isolated IPv6 networks via IPv4 networks
2. Communications between IPv6 networks and IPv4 networks

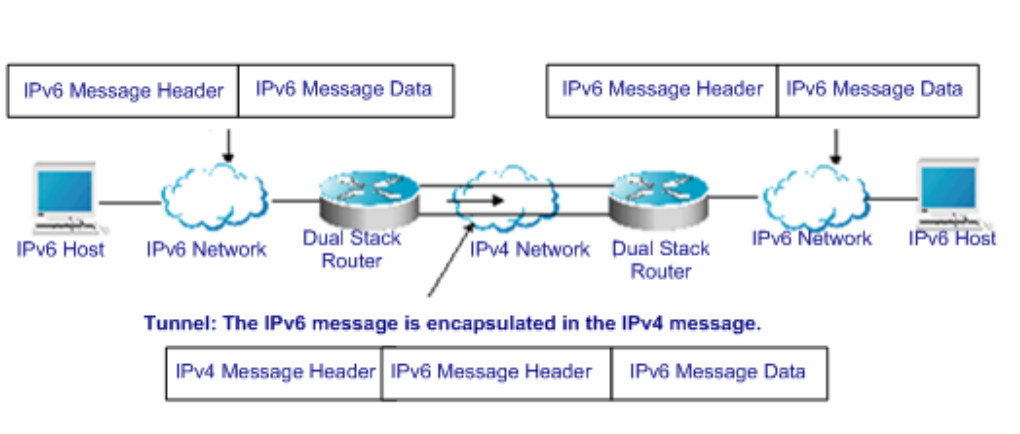
This article discusses the tunnel technology that is used to solve problem 1. The solution to problem2 is NAT-PT (Network Address Translation-Protocol Translation), which is not covered in this article.

The IPv6 tunnel technology encapsulates IPv6 messages in IPv4 messages. In this way, IPv6 protocol packets can communicate with each other via IPv4 networks. Therefore, with the IPv6 tunnel technology, isolated IPv6 networks can communicate one another via existing IPv4 networks, avoiding any modification and upgrade to existing IPv4 networks. An IPv6 tunnel can be configured between Area Border Routers or between an Area Border Router and the host. However, all the nodes at the two ends of the tunnel must support the IPv4 and IPv6 protocol stacks. At present, our company supports the following tunnel technologies:

Tunnel Type	Reference
Manually Config Tunnel	RFC2893
Intra-Site Automatic Tunnel Addressing Protocol(ISATAP)	draft-ietf-ngtrans-isatap-22

Caution Interconnecting the isolated IPv6 networks through the IPv6 tunnel technology is not the ultimate IPv6 network architecture. Instead, it is a transitional technology.

The model using the tunnel technology is shown in the following figure:



The features of various tunnels are respectively introduced below.

3.1.1 Manually Configured IPv6 Tunnel

One manually configured tunnel is similar to one permanent link set up between two IPv6 domains via the backbone network of the IPv4. It is applicable for the relatively fixed connections that have a higher demand on security between two Area Border Routers or between an Area Border Router and a host.

On a tunnel interface, you must manually configure the IPv6 address, source IPv4 address (tunnel source) and destination IPv4 address (tunnel destination) of the tunnel. The nodes at the two end of the tunnel must support the IPv6 and IPv4 protocol stacks. In practical application, tunnels are always manually configured in pairs. You can think it as a point-to-point tunnel.

3.1.2 ISATAP Automatic unnel

Intra-site Automatic Tunnel Addressing Protocol (ISATAP) is a type of IPv6 tunnel technology by which an intra-site IPv6 architecture takes an IPv4 network as one nonbroadcast multi-access (NBMA) link layer, namely taking an IPv4 network as the virtual link layer of the IPv6.

ISATAP is applicable for the case where the pure IPv6 network inside a site is not ready for use yet and an IPv6 message need be transferred internally in the site. For example, a few of IPv6 hosts for test need communicate one another inside the site.

By an ISATAP tunnel, the IPv4/IPv6 dual stack hosts on a same virtual link can communicate one another inside the site.

On the ISATAP site, the ISATAP router provides standard router advertisement message, allowing the ISATAP host to be automatically configured inside the site. At the same time, the ISATAP router performs the function that an intra-site ISATAP host and external IPv6 host forward messages.

The IPv6 address prefix used by ISATAP can be any legal 64-bit prefix for IPv6 unicast, including the global address prefix, local link prefix and local site prefix. The IPv4 address is placed as the ending 32 bits of the IPv6 address, allowing a tunnel to be automatically built.

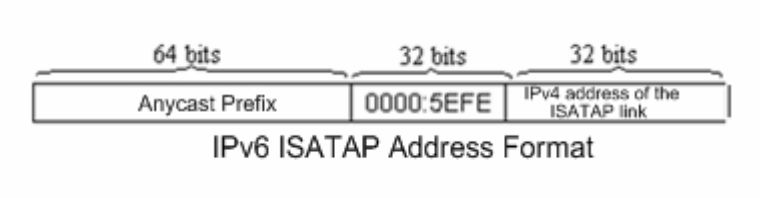
It is very possible that ISATAP is used with other transition technologies.

- ISATAP interface identifier

The unicast address used by ISATAP is in the form of a 64-bit IPv6 prefix plus a 64-bit interface identifier. The 64-bit interface identifier is generated in the revised EUI-64 address form. Where, the value of the first 32 bits of the interface identifier is **0000:5EFE**, an interface identifier of ISATAP.

- ISATAP address structure

An ISATAP address refers to the unicast address containing an ISATAP interface identifier in its interface identifier. An ISATAP address structure is shown in the following figure:



IPv6 ISATAP Address Format

The above figure shows that the interface identifier contains an IPv4 address. The address is the IPv4 address of a dual stack host and will be used when an automatic tunnel is automatically built.

For example, the IPv6 prefix is 2001::/64 and the embedded IPv4 address is 192.168.1.1. In the ISATAP address, the IPv4 address is denoted as the hexadecimal numeral of C0A8:0101. Therefore, its corresponding ISATAP address is as follows:

2001::0000:5EFE:C0A8:0101

3.2 IPv6 Tunnel Configuration

3.2.1 Manually Configuring IPv6 Tunnels

This section explains how to configure tunnels manually.

To configure a tunnel manually, configure an IPv6 address on the tunnel interface and manually configure the IPv4 addresses of the source port and destination port of the tunnel. Then, configure the hosts or routers at the two ends of the tunnel to ensure that they support the dual stacks (the IPv6 and IPv4 protocol stacks).

Caution

Do not configure tunnels manually with the same Tunnel Source and Tunnel Destination.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip
ipv6 enable
tunnel source {ip-address | type num}
tunnel destination ip-address
end
```

To configure an IPv6 tunnel manually, execute the following commands in the global configuration mode:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.
tunnel mode ipv6ip	Set the tunnel type to manually configured tunnel.
ipv6 enable	Enable the IPv6 function on the interface. You can also configure the IPv6 address to directly enable the IPv6 function on the interface.
tunnel source {*ip-address* | *type num*	Specify the IPv4 source address or referenced source interface number of a tunnel. Note: If you specify an interface, then the IPv4 address must have been configured on the interface.

Command	Meaning
tunnel destination *ip address*	Specify the destination address of a tunnel.
end	Return to the privileged mode.
copy running-config startup-config	Save the configuration.

Refer to the section *Verifying and Mmonitoring IPv6 Tunnel Configuration* to check the operation of the tunnel.

3.2.2 Configuring ISATAP Tunnel

This section introduces how to configure an ISATAP device.

On an ISATAP tunnel interface, the configuration of an ISATAP IPv6 address and the advertisement configuration of a prefix is same to that of a normal IPv6 interface. However, the address configured for an ISATAP tunnel interface must be a revised EUI-64 address. The reason is that the last 32 bits of the interface identifier in the IPv6 address are composed of the IPv4 address of the interface referenced by the tunnel source address. Refer to the above chapters and sections for the information about ISATAP address formats.

Caution

A device supports multiple ISATAP tunnels. However, the source of each ISATAP tunnel must be different.

Otherwise, there is no way to know which ISATAP tunnel a received ISATAP tunnel message belongs to.

Brief steps

```
config terminal
interface tunnel tunnel-num
tunnel mode ipv6ip isatap
ipv6 address ipv6-prefix/prefix-length eui-64
tunnel source interface-type num
no ipv6 nd suppress-ra
end
```

To configure an ISATAP tunnel, execute the following commands in the global configuration mode:

Command	Meaning
configure terminal	Enter the global configuration mode.
interface tunnel *tunnel-num*	Specify a tunnel interface number to create a tunnel interface and enter the interface configuration mode.

Command	Meaning
tunnel mode ipv6ip isatap	Set the tunnel type to ISATAP tunnel.
ipv6 address ipv6-prefix/prefix-length eui-64	Configure the IPv6 ISATAP address. Be sure to specify to use the **eui-64** keyword. In this way, the ISATAP address will be automatically generated. The address configured on an ISATAP interface must be an ISATAP address.
tunnel source type *num*	Specify the source interface number referenced by a tunnel. On the referenced interface, the IPv4 address must have been configured.
no ipv6 nd suppress-ra	By default, it is disabled to send router advertisement messages on an interface. Use the command to enable the function, allowing the ISATAP host to be automatically configured.
End	Return to the privileged EXEC mode.
copy running-config startup-config	Save the configuration.

Refer to the section *Verifying and Mmonitoring IPv6 Tunnel Configuration* to check the operation of the tunnel.

3.3 Verifying and Monitoring IPv6 Tunnel Configuration

This section introduces how to verify the configuration and operation of an IPv6 tunnel.

Brief steps

```
enable
show interface tunnel number
show ipv6 interface tunnel mumber
ping protocol destination
show ip route
show ipv6 route
```

To verify the configuration and operation of a tunnel, execute the following commands in the privileged mode:

Command	Meaning
enable	Enter the privileged configuration mode.

Command	Meaning
show interface tunnel *tunnel-num*	View the information of a tunnel interface.
show ipv6 interface tunnel *tunnel-num*	View the IPv6 information of a tunnel interface.
ping protocol destination	Check the basic connectivity of a network.
show ip route	View the IPv4 routing table.
show ipv6 route	View the IPv6 router table.

1. View the information of a tunnel interface.

```
DES-7200# show interface tunnel 1
Tunnel 1 is up, line protocol is Up
Hardware is Tunnel, Encapsulation TUNNEL
Tunnel source 192.168.5.215 , destination 192.168.5.204
Tunnel protocol/transport IPv6/IP
Tunnel TTL is 9
Tunnel source do conformance check set
Tunnel source do ingress filter set
Tunnel destination do safety check not set
Tunnel disable receive packet not set
```

2. View the IPv6 information of a tunnel interface.

```
DES-7200# show ipv6 interface tunnel 1
interface Tunnel 1 is Up, ifindex: 6354
address(es):
Mac Address: N/A
INET6: fe80::3d9a:1601 , subnet is fe80::/64
Joined group address(es):
ff02::2
ff01::1
ff02::1
ff02::1:ff9a:1601
INET6: 3ffe:4:0:1::1 , subnet is 3ffe:4:0:1::/64
Joined group address(es):
ff02::2
ff01::1
ff02::1
ff02::1:ff00:1
MTU is 1480 bytes
ICMP error messages limited to one every 100 milliseconds
ICMP redirects are enabled
ND DAD is enabled, number of DAD attempts: 1
ND reachable time is 30000 milliseconds
ND advertised reachable time is 0 milliseconds
ND retransmit interval is 1000 milliseconds
```

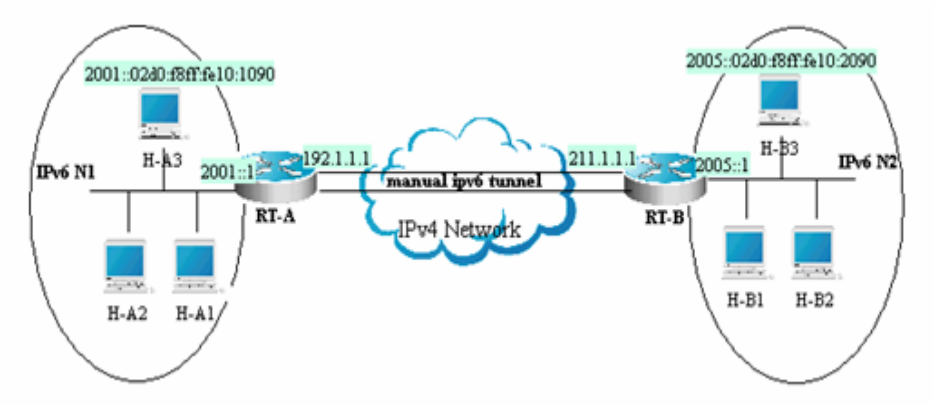
```
ND advertised retransmit interval is 0 milliseconds
ND router advertisements are sent every 200 seconds<240--160>
ND router advertisements live for 1800 seconds
```

3.4 IPv6 Tunnel Configuration Instances

The following sections introduce IPv6 tunnel configuration instances.

- Manual IPv6 Tunnel Configuration
- ISATAP Tunnel Configuration

3.4.1 Manual IPv6 Tunnel Configuration



As shown in the above figure, IPv6 networks N1 and N2 are isolated by the IPv4 network. Now, the two networks are interconnected by configuring a tunnel manually. For example, the H-A3 host in N1 can access the H-B3 host in N2.

In the figure, RT-A and RT-B are routers that support the IPv4 and IPv6 protocol stacks. Tunnel configuration occurs on the Area Border Routers (RT-A and RT-B) in N1 and N2. Note that the tunnel must be configured manually in pairs, that is, on RT-A and RT-B.

The following presents the tunnel configuration on routers:

Prerequisite: Suppose the routes of IPv4 are connected. In the following content, no more route configuration condition about IPv4 is listed.

RT-A configuration

#Connect the interfaces of the IPv4 network

```
interface FastEthernet 2/1
no switchport
ip address 192.1.1.1 255.255.255.0
```

#Connect the interfaces of the IPv6 network

```
interface FastEthernet 2/2
no switchport
ipv6 address 2001::1/64
no ipv6 nd suppress-ra  (optional)
```

#Configure manual tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 211.1.1.1
```

#Configure the route to the tunnel

```
ipv6 route 2005::/64 tunnel 1
```

RT-B configuration

#Connect the interfaces of the IPv4 network

```
interface FastEthernet 2/1
no switchport
ip address 211.1.1.1 255.255.255.0
```

Connect the interfaces of the IPv6 network

```
interface FastEthernet 2/2
no switchport
ipv6 address 2005::1/64
no ipv6 nd suppress-ra  (optional)
```

#Configure the manual tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip
ipv6 enable
tunnel source FastEthernet 2/1
tunnel destination 192.1.1.1
```

#Configure the route to the tunnel

```
ipv6 route 2001::/64 tunnel 1
```

3.4.2 Manual IPv6 tunnel Configuration for Supporting Multicast

Assuming that the network topology is shown in Fig 4. On the basis of the previous example, the additional support to PIM SMv6 multicast shall be provided. Detailed configurations related to multicast are shown below:

- RT-A

Globally enable multicast

```
ipv6 multicast-routing
```

Enable PIM SMv6 on the interface

```
interface Tunnel 1
IPv6 pim sparse-mode
```

- RT-B

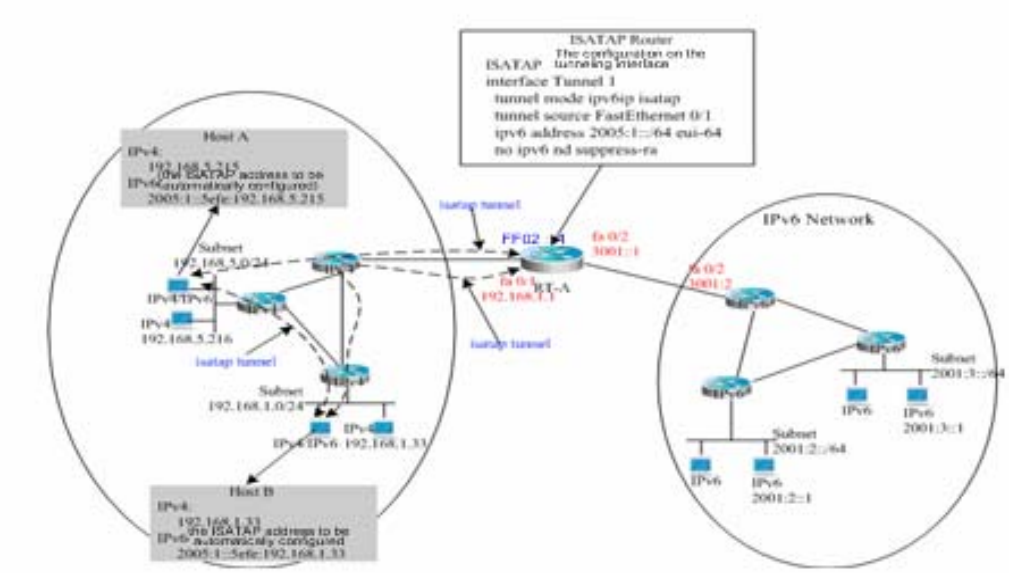
Globally enable multicast

```
ipv6 multicast-routing
```

Enable PIM SMv6 on the interface

```
interface Tunnel 1
IPv6 pim sparse-mode
```

3.4.3 ISATAP Tunnel Configuration



The above figure is one typical topology using an ISATAP tunnel. The ISATAP tunnel is used to communicate between isolated IPv4/IPv6 dual stack hosts inside the IPv4 site. The ISATAP router has the two following functions inside the ISATAP site:

- Receive a router request message from the ISATAP host inside the site and then respond with a router advertisement message for the ISATAP host inside the site to be automatically configured.
- Be responsible for the message forwarding function of the ISATAP host inside the site and the IPv6 host outside the site.

In the above figure, when Host A and Host B send the router solicitation message to ISATAP Router, ISATAP Router will respond with a router advertisement message. After receiving the message, the hosts will automatically perform self-configuration and generate their own ISATAP addresses respectively. Then, the IPv6 communication between Host A and Host B will be done via the ISATAP tunnel. When Host A or Host B need communicate with the IPv6 host outside the site, Host A sends the message to the ISATAP router RT-A via the ISATAP tunnel and then RT-A forwards the message to the IPv6 network.

In the above figure, ISATAP Router (RT-A) is configured as follows:

Connect the interfaces of the IPv4 network

```
interface FastEthernet 0/1
no switchport
ip address 192.168.1.1 255.255.255.0
```

Configure the ISATAP tunnel interface

```
interface Tunnel 1
tunnel mode ipv6ip isatap
tunnel source FastEthernet 0/1
ipv6 address 2005:1::/64 eui-64
no ipv6 nd suppress-ra
```

Connect the interfaces of the IPv6 network

```
interface FastEthernet  0/2
no switchport
ipv6 address 3001::1/64
```

Configure the route to the IPv6 network

```
ipv6 route 2001::/64 3001::2
```

4 DHCP Configuration

4.1 Introduction to DHCP

The DHCP (Dynamic Host Configuration Protocol), specified in RFC 2131, provides configuration parameters for hosts over the Internet. The DHCP works in the client/server mode. The DHCP server assigns IP addresses for the hosts dynamically and provides configuration parameters.

The DHCP assigns IP address in three ways:

1. Assign IP addresses automatically. The DHCP server assigns permanent IP addresses to the clients;

2. Assign IP addresses dynamically. The DHCP server assigns IP addresses that will expire after a period of time to the clients (or the clients can release the addresses by themselves);

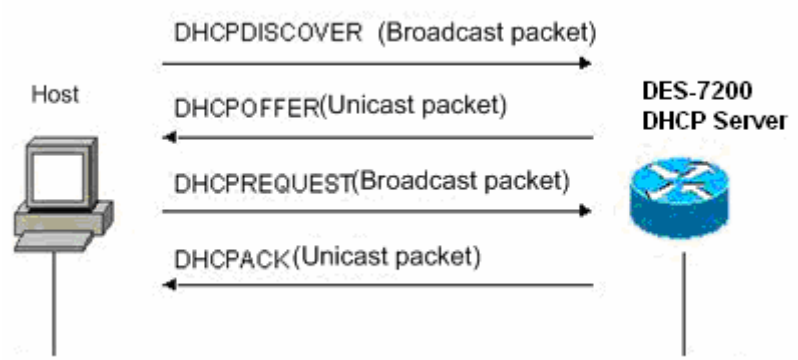
3. Configure IP addresses manually. Network administrators specify IP addresses and send the specified IP addresses to the clients through the DHCP.

Among the above mentioned three methods, only dynamic assignment allows reuse of the IP address that the client does not need any more.

The format of DHCP message is based on that of BOOTP (Bootstrap Protocol) message. Hence, it is necessary for the device to be able to act as the BOOTP relay agent and interact with the BOOTP client and the DHCP server. The function of BOOTP relay agent eliminates the need of deploying a DHCP server in every physical network. The DHCP is detailed in RFC 951 and RFC 1542.

4.2 Introduction to the DHCP Server

As specified in RFC2131, the DHCP server of DES-7200 is implemented to assign and manage IP addresses for the DHCP clients. The DHCP operation process is shown in the following figure.



Process of requesting an IP address:

1. The host broadcasts a DHCPDISCOVER packet in the network to locate the DHCP server;

2. The DHCP server sends a DHCPOFFER packet in unicast form to the host, including IP address, MAC address, domain name and address lease period;

3. The host sends a DHCPREQUEST packet in broadcast form to formally request the server to assign the provided IP address;

4. The DHCP server sends a DHCPACK packet in unicast form to the host to confirm the request.

Note

The DHCP client may receive the DHCPOFFER packets from multiple DHCP servers, and accept any DHCPOFFER packet. However, the DHCP client usually accepts the first received DHCPOFFER packet only. The address specified in the DHCPOFFER packet from the DHCP server is not necessarily the finally assigned address. Generally, the DHCP server reserves this address until the client sends a formal request.

The goal of broadcasting the DHCPREQUEST packet is to let all the DHCP servers that send the DHCPOFFER packet receive this packet and then release the IP address specified in the DHCPOFFER packet.

If the DHCPOFFER packet sent to the DHCP client contains invalid parameters, the DHCP client sends the DHCPDECLINE packet to refuse the assigned configuration.

During negotiation, if the DHCP client does not respond to the DHCPOFFER packet in time, the DHCP server will send the DHCPNAK packet to the DHCP client, initiating the address request process again.

The advantages of using the DHCP server of DES-7200 for network construction are:

- Decrease network access cost. Generally, dynamic address assignment costs less than static address assignment.
- Simplify configuration tasks and reduce network construction cost. Dynamic address assignment significantly simplifies equipment configuration, and even reduces deployment cost if devices are deployed in the places where there are no professionals.
- Centralized management. During configuration management on several subnets, any configuration parameter can be changed simply by modifying and updating configurations in the DHCP server.

4.3 Introduction to the DHCP Client

The DHCP client can obtain IP addresses and other configuration parameters from the DHCP server automatically. The DHCP client brings the following advantages:

- Save device configuration and deployment time.
- Reduce the possibility of configuration errors.
- Centrally manage IP address assignment.

Caution

The DHCP Client are supported on the Ethernet interface, FR, PPP, HDLC interfaces.

4.4 Introduction to the DHCP Relay Agent

The DHCP relay agent forwards DHCP packets between the DHCP server and the DHCP clients. When the DHCP clients and the server are not located in the same subnet, a DHCP relay agent must be available for forwarding the DHCP request and response messages. Data forwarding by the DHCP relay agent is different from general forwarding. In general forwarding, IP packets are unaltered and the transmission is transparent. However, upon receiving a DHCP message, the DHCP relay agent regenerates and forwards a DHCP message.

From the perspective of the DHCP client, the DHCP relay agent works like a DHCP server. From the perspective of the DHCP server, the DHCP relay agent works like a DHCP client.

4.5 Configuring DHCP

To configure DHCP, perform the following tasks, of which the first three tasks are mandatory.

- Enabling the DHCP Server and the DHCP Relay Agent (required)
- Configuring DHCP Excluded Addresses (required)
- Configuring DHCP Address Pool (required)
- Binding Address Manually (optional)
- Configuring the Ping Times (optional)
- Configuring Ping Packet Timeout (optional)
- Ethernet interface DHCP client configuration (optional)
- DHCP Client Configuration in PPP Encapsulation link (optional)
- DHCP Client Configuration in FR Encapsulation link (optional)
- DHCP Client Configuration in HDLC Encapsulation link (optional)

4.5.1 Enabling the DHCP Server and the DHCP Relay Agent

To enable the DHCP server and the DHCP relay agent, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **service dhcp**	Enable the DHCP server and the DHCP relay agent.
DES-7200(config)# **no service dhcp**	Disable the DHCP server and the DHCP relay agent.

Note

By default, in v10.1 and later, the command **service dhcp** can be used for both DHCP server and DHCP relay, which are two mutually-exclusive functions. The switchover of those two functions depends on whether the DHCP address pool is configured or not.

However, for the product in the version prior to v10.1(excluding v10.1), the command **service dhcp** is not supported by both DHCP server and DHCP relay. You can use the command **service dhcp** to enable the DHCP service or the DHCP server.

For some product in v10.1 and later, DHCP may conflict with some functions. For the details, see the prompting message of specific product.

4.5.2 Configuring DHCP Excluded Addresses

Unless configured particularly, the DHCP server tries to assign all the subnet addresses defined in the address pool to the DHCP clients. If you want to reserve some addresses, such as those that have been assigned to servers or devices, you must define clearly that these addresses cannot be assigned to the DHCP clients.

To configure the addresses that cannot be assigned to the DHCP clients, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp excluded-address low-ip-address** [**high-ip-address**]	Define a range of IP addresses that the DHCP server will not assign to the DHCP clients.
DES-7200(config)# **no ip dhcp excluded-address low-ip-address** [**high-ip-address**]	Remove the configuration.

A good practice in configuring the DHCP server is to prohibit the DHCP server from assigning any address that has been assigned specifically. This provides two advantages: 1) No address conflict will occur; 2) When DHCP assigns addresses, the time for detection is shortened and thus DHCP will perform assignment more efficiently.

4.5.3 Configuring DHCP Address Pool

Both DHCP Address assignment and DHCP parameters sent to the client should be defined in the DHCP address pool. If no DHCP address pool is configured, addresses cannot be assigned to the DHCP clients even though the DHCP server has been enabled. However, if the DHCP server has been enabled, the DHCP relay agent is always working regardless of the DHCP address pool.

You can give a meaningful name that can be memorized easily to the DHCP address pool. The name of address pool contains characters and digits. DES-7200 product allows you to define multiple address pools. The IP address of the DHCP relay agent in the DHCP request packet is used to determine which address pool is used for address assignment.

- If the DHCP request packet does not contain the IP address of the DHCP relay agent, the address that is in the same subnet or network as the IP address of the interface that receives the DHCP request packet is assigned

to the DHCP client. If no address pool is defined for this network segment, address assignment fails.

- If the DHCP request packet contains the IP address of the DHCP relay agent, the address that is in the same subnet or network as this address is assigned to the DHCP client. If no address pool is defined for this network segment, address assignment fails.

To configure a DHCP address pool, perform the following tasks as appropriate, of which the first three tasks are mandatory:

- Configure an address pool name and enter its configuration mode (required)
- Configure a subnet and its mask for the address pool (required)
- Configure the default gateway for the DHCP client (required)
- Configure the address lease period (optional)
- Configure the domain name of the DHCP client (optional)
- Configuring the domain name server (optional)
- Configure the NetBIOS WINS server (optional)
- Configure the NetBIOS node type for the DHCP client (optional)

4.5.3.1 Configuring an Address Pool Name and Enter Its Configuration Mode

To configure an address pool name and enter the address pool configuration mode, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp pool** *dhcp-pool*	Configuring an address pool name and enter the address pool configuration mode

The address pool configuration mode is shown as “DES-7200(dhcp-config)#”.

4.5.3.2 Configuring the Boot File for the DHCP Client

The boot image file is the one used when the client starts. The boot image file is often the operation system to be downloaded by the DHCP client.

To configure the boot file for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7200 (dhcp-config)# **bootfile** *filename*	Configure the name of the boot file for the DHCP client.

4.5.3.3 Configuring the Default Gateway for the DHCP Client

The IP address of the default gateway must be in the same network as the IP address of the DHCP client.

To configure the default gateway for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **default-router** *address* [*address2…address8*]	Configure the default gateway.

4.5.3.4 Configuring the Address Lease Period

The lease for the address that the DHCP server assigns to the client is one day by default. The client should request to renew when the lease period is going to expire. Otherwise, it cannot use this address when the lease period expires.

To configure the address lease period, execute the following command in the address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **lease** {*days* [*hours*] [*minutes*] | **infinite**}	Configure the address lease period.

4.5.3.5 Configuring the Domain Name of the DHCP Client

The domain name of the DHCP client can be specified. In this way, the domain name suffix will be automatically added to the incomplete host name to form a complete host name when the DHCP client accesses the network resources using the host name.

To configure the domain name of the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **domain-name** *domain*	Configure the domain name.

4.5.3.6 Configuring the Domain Name Server

A DNS server should be specified for domain name resolution when the DHCP client accesses the network resources using a host name.

To configure a domain name server for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **dns-server** *address* [*address2…address8*]	Configure a DNS server.

4.5.3.7 Configuring the NetBIOS WINS Server

WINS is a domain name resolution service from Microsoft that the TCP/IP network uses to resolve a NetNBIOS name to an IP addresses. The WINS server runs in Windows NT. After started, the WINS server will receive a registration request from the WINS client. When the WINS client is being shut down, it will send a name release message to the WINS server to guarantee the consistency of available computers between the WINS database and the network.

To configure a NetBIOS WINS server for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **netbios-name-server** *address* [*address2…address8*]	Configure a DNS server.

4.5.3.8 Configuring the NetBIOS Node Type for the DHCP Client

There are four types of NetBIOS nodes for Microsoft DHCP client:

1. Broadcast. The NetBIOS name is resolved in the broadcast mode;
2. Peer-to-peer. The WINS server is asked directly to resolve the NetBIOS name;
3. Mixed. First, the name is resolved in the broadcast mode, and then the WINS server is connected to resolve the name;
4. Hybrid. First the WINS server is asked directly to resolve the NetBIOS name. If there is no response, the NetBIOS name is resolved in the broadcast mode.

By default, the Windows operation systems support broadcast or hybrid type NetBIOS nodes. If no WINS server is configured, the node is of broadcast type. If a WINS server is configured, the node is of hybrid type.

To configure the NetBIOS node type for the DHCP client, execute the following command in the address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **netbios-node-type** *type*	Configure the NetBIOS node type.

4.5.3.9 Configuring the Network Number and Mask of the DHCP Address Pool

To configure dynamic address binding, you must configure the subnet and its mask for the new address pool. A DHCP address pool provides the DHCP server with an address space that can be assigned to clients. All the addresses in the address pool are available for the DHCP clients unless address exclusion is configured. The DHCP server assigns the addresses in the address pool in sequence. If an address already exists in the binding table or this address is detected to be already present in this network segment, the DHCP server will check the next address until it assigns a valid address.

To configure the subnet and its mask of the DHCP address pool, execute the following commands in the address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **network** *network-number mask*	Configure the network number and mask of the DHCP address pool.

Caution

For the DHCP dynamic address pool of DES-7200 products, addresses are assigned based on the physical address and ID of a DHCP client. This means there should not be two leases for the same DHCP client in the DHCP dynamic address pool. If path redundancy occurs between the DHCP client and the DHCP server (the DHCP client can reach the DHCP server by the direct path or relay path), the DHCP server may fail to assign addresses.

To solve this problem, administrators should avoid path redundancy between the DHCP clients and the DHCP sever in other ways like adjusting physical links or network paths.

4.5.3.10 Configuring DHCP Address Pool to Allocate Address as per Option82

Generally, the DHCP relay agent will insert an option of "Option 82" to carry relevant information about the client during the process of packet forwarding (such as the VLAN to which the client belongs, slot number, port number or user's 1X class). Upon receipt of such packets, the DHCP server will allocate addresses according to the specific information about clients by analyzing Option 82 information. For example, Option 82 can be utilized to allocate a certain range of IP addresses to clients belonging to a certain VLAN or user class. This feature can be used when it is needed to allocate a specific range of IP addresses according to user's network allocation information (such as VLAN, slot number or port number) or user's priority.

Each DHCP address pool can allocate addresses using Option 82 information. Option 82 information will be matched and classified, and we can specify the allocable address range for the corresponding class. One DHCP address pool can be associated with multiple classes, and different address ranges can be specified for each class.

During the process of address allocation, we can first determine the allocable address pool according to the network segment to which the client belongs, and then further determine its CLASS according to Option 82 information, so as to allocate IP address from the address range corresponding to the CLASS. When a request packet matches multiple classes in the address pool, address will be allocated from the address ranges corresponding to these classes in the order that the classes are configured in the address pool. If the class has not allocable address, the address range for next matching class will be used, and the like. Each class corresponds to one address range, and the addresses must be allocated from low to high. Multiple classes can be configured with the same address range. If the class associated with the address pool is specified but the corresponding network scope is not configured, then the default address range of this class shall be same as that of the address pool to which this class belongs.

To configure the CLASS associated with address pool and the address range corresponding to the class, execute the following commands in address pool configuration mode:

Command	Function
DES-7200(dhcp-config)# **class** *class-name*	Configure the name of associated class, and enter the class configuration mode of address pool.

Command	Function
DES-7200(config-dhcp-pool-class)# **address range** *low-ip-address high-ip-address*	Configure the corresponding address range.

Caution

1. When the class configured cannot be found in global class, a global class will be created automatically;
2. The associated class configured in the address pool may conflict with the static manual binding, and therefore must not be configured at the same time.
3. Up to 5 classes can be configured for each address pool.

4.5.4 Configuring Class

4.5.4.1 Configuring Option82 Matching Information for CLASS

The specific Option82 matching information corresponding to each CLASS can be configured after entering CLASS configuration mode in global mode. One CLASS can match multiple Option 82 information, and it is considered matched if the packet matches any information. If no matching information is configured for CLASS, then this CLASS can match any request packets carrying Option 82 information. The address can only be allocated from the corresponding address pool after the request packet matches a specific CLASS.

To configure global CLASS and the Option 82 information corresponding to the CLASS, execute the following commands in global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp class** *class-name*	Configure CLASS name and enter global CLASS configuration mode.
DES-7200(config-dhcp-class)# **relay agent information**	Enter Option 82 matching information configuration mode.

Command	Function
DES-7200(config-dhcp-class-relayinfo)# **relay-information hex** *aabb.ccdd.eeff…* [*****]	Configure specific Option 82 matching information. 1. Aabb.ccdd.eeff.. is a hexadecimal number 2. * means imperfect matching mode. It is considered matched if the information before * is matched.

Caution

1. Global CLASS can have up to 20 matches.

4.5.4.2 Configuring Remark Information for CLASS

To configure remark information to describe the meaning of CLASS, execute the following commands in global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp class** *class-name*	Configure CLASS name and enter CLASS configuration mode.
DES-7200(config-dhcp-class)#**remark** *used in #1 building*	Configure remark information.

4.5.4.3 Configuring whether or not to use CLASS Allocation

To configure address allocation using CLASS, execute the following commands in global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp use class**	Configure address allocation using CLASS.

Caution This command is enabled by default. Execute NO command to disable address allocation using CLASS.

4.5.5 Configuring Binding Database Storage

4.5.5.1 Configuring to periodically Save Binding Database into FLASH

To avoid the loss of binding database (lease information) on DHCP server due to power failure or reboot of device, you can configure the delay time to write the database into FLASH. The time is 0 by default, namely the database will be written into FLASH at variable intervals.

To periodically write the binding database into the FLASH, execute the following command in global configuration mode:

Command	Function
DES-7200(config)# [**no**] **ip dhcp database write-delay** [*time*]	Configure DHCP delay time to write into FLASH. *time*：600s--86400s (default: 0)

Caution Since frequent FLASH reading and writing will shorten the service life of FLASH, we shall pay attention to the delay time configured. Short delay time will enable efficient storage of device information, while long delay time can reduce the frequency of FLASH reading and writing, thus providing a longer service life.

4.5.5.2 Configuring to manually Save Binding Database into FLASH

To avoid the loss of DHCP binding database (lease information) due to power failure or reboot of device, you can also manually write the existing binding database information into the FLASH as needed besides configuring the delay time for FLASH writing.

To manually write the binding database into the FLASH, execute the following command in global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp database write-to-flash**	Write DHCP binding database information into the FLASH

4.5.6 Manual Address Binding

Address binding refers to the IP address to MAC address mapping for the DHCP clients. You can bind addresses in two ways.

- Manual binding: Configure the static IP address to MAC address mapping for the DHCP client on the DHCP server manually. Manual binding actually offers a special address pool;
- Dynamic binding: Upon receiving a DHCP request from the DHCP client, the DHCP server dynamically assigns an IP address from the DHCP address pool to the DHCP client, and thus mapping the IP address to the MAC address for the DHCP client.

To define manual address binding, you first need to define a host address pool for each manual binding, and then define the IP address and hardware address (MAC address) or ID for the DHCP client. Generally, a client ID instead of a MAC address, is defined for the Microsoft clients. The client ID contains media type and MAC address. For the codes of media types, refer to Address Resolution Protocol Parameters in RFC 1700. The code of Ethernet type is “01”.

To configure the manual address binding, execute the following commands in the address pool configuration mode:

Command	Function
DES-7200(config)# **ip dhcp pool** *name*	Define the name of the DHCP address pool and enter the DHCP configuration mode.
DES-7200(dhcp-config)# **host** *address*	Define an IP address for the DHCP client.
DES-7200(dhcp-config)# **hardware-address** *hardware-address type* DES-7200(dhcp-config)# **client-identifier** unique-identifier	Define a hardware address for the DHCP client, such as aabb.bbbb.bb88 Define an ID for the DHCP client, such as 01aa.bbbb.bbbb.88

Command	Function
DES-7200(dhcp-config)# **client-name** *name*	(Optional) Define the client name using standard ASCII characters. Don't include domain name in the client name. For example, if you define the mary host name, do not define as mary.rg.com

4.5.7 Configuring Ping Times

By default, when trying to assign an IP address from the DHCP address pool to a DHCP client , the DHCP server will ping the IP address twice (one packet for each time). If there is no response, the DHCP server considers this address an idle address and assigns it to the DHCP client. If there is a response, the DHCP server considers that this address is in use and tries to assign another address to the DHCP client until an address is assigned successfully.

To configure the number of Ping packets, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp ping** *packets number*	Configure the number of Ping packets before the DHCP server assigns an address. If it is set to 0, the Ping operation is not performed. The default value is 2.

4.5.8 Configuring Ping Packet Timeout

By default, the DHCP server considers the IP address inexistent if it has not received a response within 500 milliseconds after pinging an IP address. You can adjust the Ping packet timeout.

To configure the Ping packet timeout, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp ping timeout** *milliseconds*	Configure the Ping packet timeout for the DHCP server. The default value is 500ms.

4.5.9 Configuring the DHCP Client on the Ethernet Interface

DES-7200 products support obtaining the IP address dynamicaly assigned by the DHCP server on an Ethernet interface.

To configure the DHCP client on the Ethernet port, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

4.5.10 Configuring the DHCP Client in the PPP Encapsulation Link

DES-7200 products support obtaining the IP address dynamicaly assigned by the DHCP server on a PPP encapsulation interface.

To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

4.5.11 Configuring the DHCP Client in the FR Encapsulation Link

DES-7200 products support obtaining the IP address dynamicaly assigned by the DHCP server on an FR encapsulation interface.

To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

4.5.12 Configuring the DHCP Client in the HDLC Encapsulation Link

DES-7200 products support obtaining the IP address dynamicaly assigned by the DHCP server on an HDLC encapsulation interface.

To configure the DHCP client, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip address dhcp**	Obtain an IP address through DHCP.

Note For some product in v10.1, DHCP client supports obtaining the IP address assigned by the DHCP server in the point-to-point link of PPP, HDLC, FR encapsulation.

4.6 Monitoring and Maintaining Information

4.6.1 Monitoring and Maintaining the DHCP Server

Three types of commands are available for monitoring and maintaining the DHCP server:

1. Clear commands, used to clear such information as DHCP address binding, address conflict and server statistics;
2. Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and fix faults;
3. Show commands, used to show information about DHCP.

DES-7200 products provide three clear commands. To clear information, execute the following commands in the command execution mode:

Command	Function
DES-7200# **clear ip dhcp binding** { *address* | ***** }	Clear the DHCP address binding information.
DES-7200# **clear ip dhcp conflict** { *address* | *}	Clear the DHCP address conflict information.

Command	Function
DES-7200# **clear ip dhcp server statistics**	Clear the DHCP server statistics.

To debug the DHCP server, execute the following command in the command execution mode:

Command	Function
DES-7200# **debug ip dhcp server** [events | packet]	Debug the DHCP server.

To show the working status of the DHCP server, execute the following commands in the command execution mode:

Command	Function
DES-7200# **show ip dhcp binding** [*address*]	Show the DHCP address binding information.
DES-7200# **show ip dhcp conflict**	Show the DHCP address conflict information.
DES-7200# **show ip dhcp server statistics**	Show the DHCP server statistics.

4.6.2 Monitoring and Maintaining the DHCP Client

There are two types of commands for monitoring and maintaining the DHCP client. The following operations can be performed on the DHCP client:

Debug commands, used to output necessary debugging information. Such commands are mainly used to diagnose and clear faults.

Show commands, used to show information about DHCP.

To debug the DHCP client, execute the following command in the command execution mode:

Command	Function
DES-7200# **debug ip dhcp client**	Debug the DHCP client.

To show information about the lease that the DHCP client obtains, execute the following command in the command execution mode:

Command	Function

Command	Function
DES-7200# **show dhcp lease**	Show the information about DHCP lease.

Note For some product in v10.1, DHCP client supports obtaining the IP address assigned by the DHCP server in the point-to-point link of PPP, HDLC, FR encapsulation.

4.7 Example of Configuring Address Pool to Support Option82

In the following example, an address pool of "net82" is defined; the address pool is in the network segment of 172.16.1.0/24, and the associated classes include class1, class2, class3 and class4. Class1 will allocate addresses from the range of 172.16.1.1-172.16.1.8; class2 will allocate addresses from the range of 172.16.1.9-172.16.1.18; class3 will allocate addresses from the range of 172.16.1.19-172.16.1.28; class4 has no defined address range, and will allocate addresses from the range of entire network segment. Configure class1 to match Option 82 information of 0100002120, class2 to match 0106020145, class3 to match 06020506*, and class4 to match any information.

```
!
ip dhcp class class1
 relay agent information
    relay-information hex 0100002120
!
ip dhcp class class2
 relay agent information
    relay-information hex 0106020145
!
ip dhcp class class3
 relay agent information
    relay-information hex 06020506*
!
ip dhcp class class4
!
ip dhcp pool net82
network 172.16.1.0 255.255.255.0
class class1
```

```
address range 172.16.1.1 172.16.1.8
class class2
address range 172.16.1.9 172.16.1.18
class class3
address range 172.16.1.19 172.16.1.28
class class4
```

4.8 Typical DHCP Configuration Example

4.8.1.1 Topological Diagram

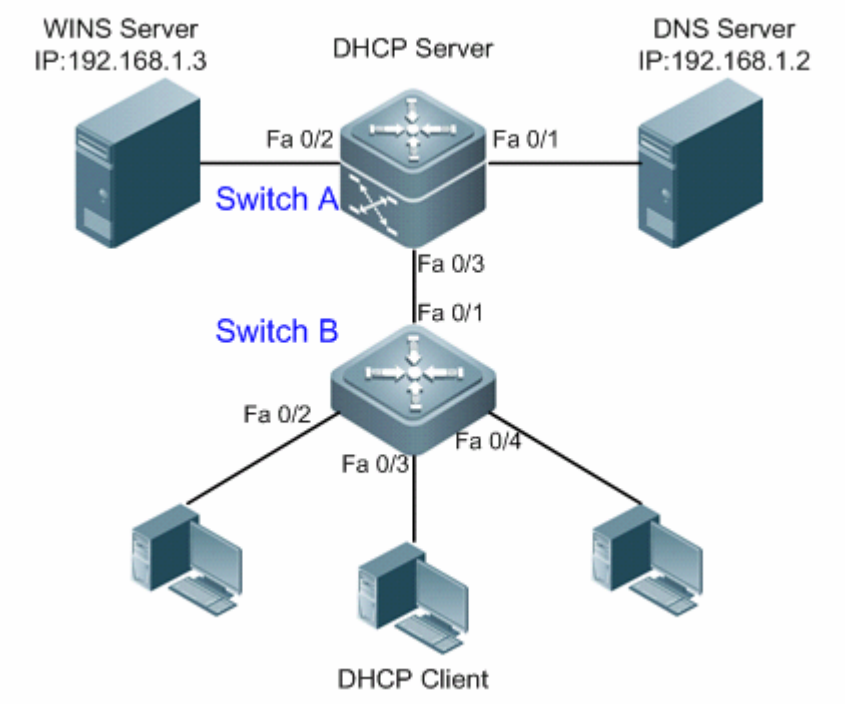


Fig 2 Diagram of DHCP example

4.8.1.2 Application Requirements

Switch A can serve as a DHCP Sever to allocate dynamic IP addresses to one part of clients and fixed IP addresses to another part of clients.

DNS Server can provide domain name resolution service for the IP addresses allocated by DHCP server to clients, namely the clients can access network resources via host names. WINS Server can translate host names into IP addresses for hosts communicating through NETBIOS protocol.

4.8.1.3 Configuration Tips

1. Enable DHCP server on Switch A and create an address pool to configure dynamic IP address allocation. Meanwhile, create an address pool to bind IP address manually.

2. Specify the address of Domain Name Server (addresses of DNS Server and WINS Server in this example) and domain name of client in the corresponding address pool.

Note

This example only illustrates the configuration of DHCP Server related features on Switch A. As for Switch B, all access users will belong to VLAN 1 by default. Access PC will obtain a dynamically allocated IP address. If you are in need of other applications, please refer to the relevant configurations.

4.8.1.4 Configuration Steps

Step 1: On Switch A, create a new DHCP address pool and configure dynamic IP address allocation.

! Configure the name of address pool as "dynamic" and enter DHCP configuration mode.

```
SwitchA #configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA (config)#ip dhcp pool dynamic
```

! In DHCP configuration mode, configure an IP address network allocable to clients and configure the default gateway of this network segment.

```
SwitchA (dhcp-config)#network 192.168.1.0 255.255.255.0
SwitchA (dhcp-config)#default-router 192.168.1.1 255.255.255.0
```

Step 2: Specify the DNS Server of "dynamic" address pool and configure the domain name of client.

! Assuming that the IP address of DNS Server is 192.168.1.2; configure Domain Name Server in the address pool and configure the domain name of client as DES-7200.com.

```
SwitchA (dhcp-config)#dns-server 192.168.1.2
SwitchA (dhcp-config)#domain-name DES-7200.com
```

Step 3: Specify the WINS Server of "dynamic" address pool and configure the NetBIOS node type of client.

! Assuming that the IP address of WIN Server is 192.168.1.3; configure NetBIOS WINS server in the address pool and configure the NetBIOS node type as Hybrid.

```
SwitchA(dhcp-config)#netbios-name-server 192.168.1.3
SwitchA(dhcp-config)#netbios-node-type h-node
```

Step 4: Configure excluded addresses in global mode.

! As shown above, IP addresses of 192.168.1.1, 192.168.1.2 and 192.168.1.3 have been allocated to the gateway, DNS server and WINS server. By configuring excluded addresses, these addresses won't be allocated to clients.

```
SwitchA (dhcp-config)#exit
SwitchA (config)#ip dhcp excluded-address 192.168.1.1 192.168.1.3
```

Step 5: Create another address pool and manually bind the IP address.

! Configure the name of address pool as "static" and enter DHCP configuration mode.

```
SwitchA (config)#ip dhcp pool static
```

! Manually bind the IP address of 192.168.1.4/24 to the MAC address of 0013.2049.9014, with client name being "admin". Note: The identifier for identifying the client shall indicate the network media type ("01" for Ethernet), namely the identifier of the client corresponding to the manually bound MAC address shall be 0100.1320.4990.14.

```
SwitchA (dhcp-config)#host 192.168.1.4 255.255.255.0
SwitchA (dhcp-config)#client-identifier 0100.1320.4990.14
SwitchA (dhcp-config)#client-name admin
```

Step 6: Specify the gateway address corresponding to the "static" address pool.

! Configure gateway address as 192.168.1.1/24.

```
SwitchA (dhcp-config)#default-router 192.168.1.1 255.255.255.0
```

Step 7: Specify the DNS Server of "static" address pool and configure the domain name of client.

! Assuming that the IP address of DNS Server is 192.168.1.2; configure Domain Name Server in the address pool and configure the domain name of client as DES-7200.com.

```
SwitchA (dhcp-config)#dns-server 192.168.1.2
SwitchA (dhcp-config)#domain-name DES-7200.com
```

Step 8: Specify the WINS Server of "static" address pool and configure the NetBIOS node type of client.

! Assuming that the IP address of WIN Server is 192.168.1.3; configure NetBIOS WINS server in the address pool and configure the NetBIOS node type as Hybrid.

```
SwitchA(dhcp-config)#netbios-name-server 192.168.1.3
```

```
SwitchA(dhcp-config)#netbios-node-type h-node
SwitchA(dhcp-config)#exit
```

Step 9: Configure the SVI interface of client.

! By default, all access clients belong to VLAN 1; configure the SVI of VLAN 1 as 192.168.1.1/24.

```
SwitchA(config)#interface vlan 1
SwitchA(config-if)#ip address 192.168.1.1 255.255.255.0
```

Step 10: Enable DHCP Server on Switch A.

```
SwitchA(dhcp-config)#exit
SwitchA(config)#service dhcp
```

4.8.1.5 Verification

Step 1: Display the configurations of Switch A.

```
SwitchA#show running-config
!
service dhcp
!
ip dhcp excluded-address 192.168.1.1 192.168.1.3
!
ip dhcp pool dynamic
 netbios-node-type n-node
 netbios-name-server 192.168.1.3
 domain-name DES-7200.com
 network 192.168.1.0 255.255.255.0
 dns-server 192.168.1.2
 default-router 192.168.1.1 255.255.255.0
!
ip dhcp pool static
 client-name admin
 client-identifier 0100.1320.4990.14
 host 192.168.1.10 255.255.255.0
 netbios-node-type n-node
 netbios-name-server 192.168.1.3
 domain-name DES-7200.com
 dns-server 192.168.1.2
 default-router 192.168.1.1 255.255.255.0
!
interface VLAN 1
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
```

Step 2: Connect two PCs to Switch B, with the MAC address of one PC being 0013.2049.9014. View the IP address allocated by DHCP Server on Switch A.

```
SwitchA#show ip dhcp binding
IP address Client-Identifier/ Lease expiration Type Hardware address
192.168.1.4 0100.e04c.70b7.e2 000 days 23 hours 48 mins Automatic
192.168.1.10 0100.1320.4990.14  Infinite      Manual
```

5 DHCP Relay Configuration

5.1 Overview

5.1.1 Understanding DHCP

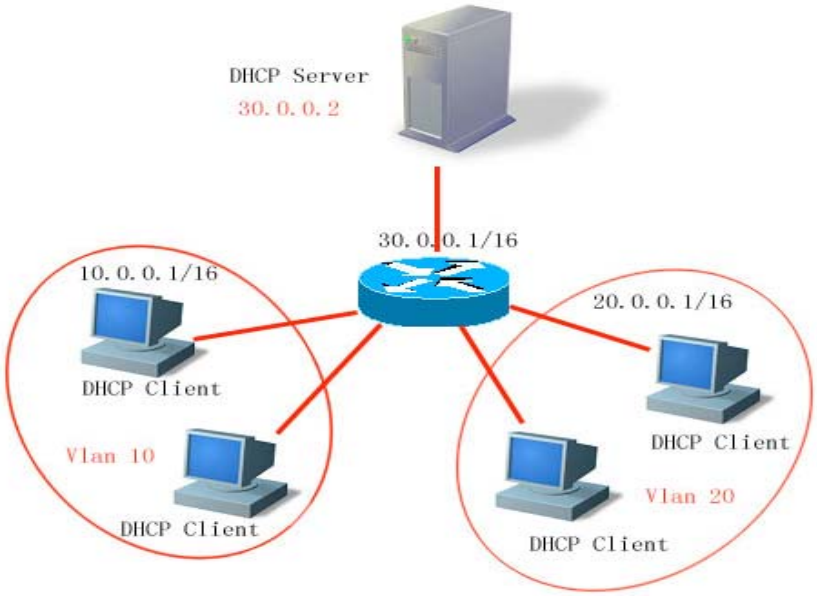
The DHCP protocol is widely used to dynamically allocate the reusable network resources, for example, IP address.

The DHCP Client sends the DHCP DISCOVER packet in broadcast form to the DHCP Server. After the DHCP Server receives the DHCP DISCOVER packet, it allocates resources such as IP address to the the DHCP Client according to the appropriate policy, and sends the DHCP OFFER packet. After the DHCP Client receives the DHCP OFFER packet, it checks if the resources are available. If resources are available, it sends the DHCP REQUEST packet. If not, it sends the DHCP DISCOVER packet. When the DHCP server receives the DHCP REQUEST packet, it checks if the IP addresses (or other limited resources) can be allocated. If yes, it sends the DHCP ACK packet. If not, it sends the DHCP NAK packet. When the DHCP Client receives the DHCP ACK packet, it starts to use the resources allocated by the DHCP server. If it receives the DHCP NAK packet, it may re-send the DHCP DISCOVER packet to request another IP address.

5.1.2 Understanding the DHCP Relay Agent

The destination IP address of DHCP REQUEST packet is 255.255.255.255. This type of packets is only forwarded inside the subnet and is not to be forwarded by the devices. For dynamic IP address allocation across network segments, the DHCP Relay Agent is created. It encapsulates the received DHCP REQUEST packet into unicast IP packets and forwards it to the DHCP server. At the same time, it forwards the received DHCP response pacekt to the DHCP Client. In this way, the DHCP Relay Agent works as a transit station responsible for communicating with the DHCP Clients and the DHCP Server on

different network segments. Therefore, one DHCP Server in a LAN can implement the dynamic IP management for all network segments, that is, a dynamic DHCP IP management in the Client - Relay Agent - Server mode.



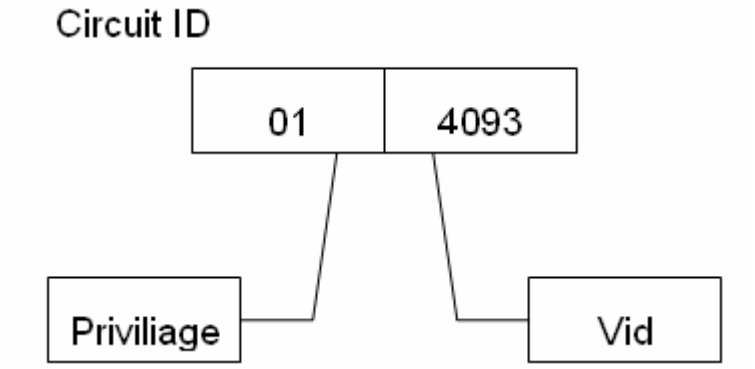
VLAN 10 and VLAN 20 correspond with the 10.0.0.1/16 and 20.0.0.1/16 networks respectively, while the DHCP Server is located on the 30.0.0.1/16 network. To have a dynamic IP management on the 10.0.0.1/16 and 20.0.0.1/16 networks through the DHCP Server at 30.0.0.2, just enable the DHCP Relay Agent on the device that functions as the gateway, and specify the IP address of the DHCP Server to 30.0.0.2.

5.1.3 Understanding DHCP Relay Agent Information(option 82)

As specified in RFC3046, when a relay device performs DHCP relay, the network information of the DHCP client can be indicated in detail by adding an option, so that the DHCP server can assign users with IP addresses for different privileges. RFC3046 specifies that the option is numbered 82, so it is also called option82. This option can be divided into several sub-options. Currently, the sub-options in frequent use are Circuit ID and Remote ID. DES-7200 provides two types of relay agent information. One is the relay agent information option dot1x that is combined with the 802.1x application scheme, the other is relay agent information option82 that is combined with the port VID, slot, port and

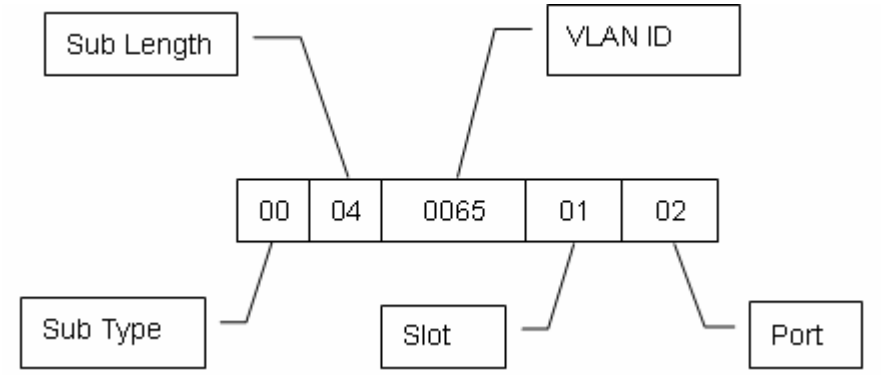
MAC address. Depicted below are the contents in the option, format, and typical application schemes when the two schemes are used:

1. relay agent information option dot1x: This application scheme requires 802.1x authentication. The device ‘s IP privilege combiens with the ID of VLAN to which the DHCP client belongs to form the Circuit ID sub-option. When DHCP relay is uploaded to the DHCP server, combined with the configuration of the DHCP server, the DHCP relay agent can assign IP addresses with different privileges to the users with different privileges. The Circuit ID is in the following format, where the **privilege** and **vid** fields respectively have two bytes:

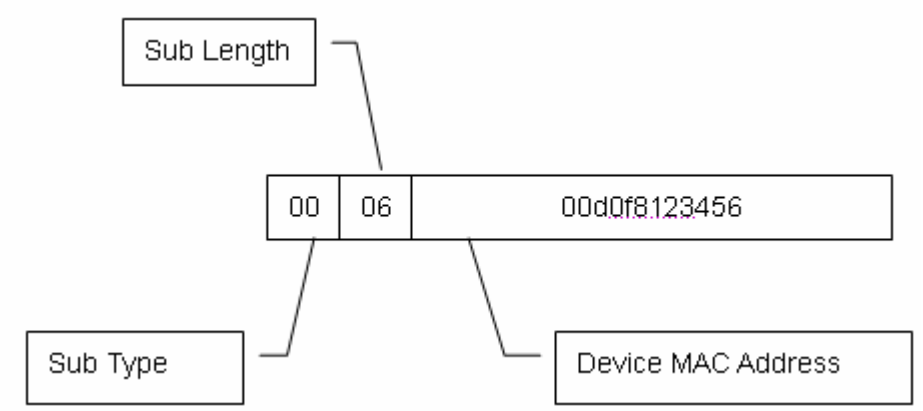


2. relay agent information option82: This option can be used without running other protocol modules. During DHCP relay, the device forms option82 information according to the port that receives the DHCP request message and the physical IP address of the device itself, and uploads the option82 information to the DHCP server. The option is in the following format:

Agent Circuit ID



Agent Remote ID



5.1.4 Understanding DHCP relay Check Server-id Function

When the DHCP is used, generally multiple DHCP servers are configured for a network for the purpose of backup, so that the network will continue to work even if a server fails. During the four interaction processes of DHCP acquisition, a DHCP server has been selected when the DHCP client sends the DHCP request message. Here, the DHCP request message includes the optional server-id. In some particular application circumstances, we need to enable this option for relay in order to reduce loads on the network server. In this way, the DHCP request message is only sent to the specified DHCP server, instead of to every configured DHCP server. This is the DHCP check server-id function.

5.2 Configuring DHCP

5.2.1 Configuring the DHCP Relay Agent

To configure the DHCP relay agent, execute the following commands in the global configurtion mode:

Command	Function
DES-7200 (config)# **service dhcp**	Enable the DHCP agent.
DES-7200(config)# **no service dhcp**	Disable the DHCP agent.

5.2.2 Configuring the IP Address of the DHCP Server

After you have configured the IP address of the DHCP Server, the DHCP request message received by the device will be forwarded to it. At the same

time, the DHCP response message received from the DHCP server will also be forwarded to the DHCP Client.

The IP address of the DHCP server can either be configured globally or on the layer 3 interface. Up to 20 IP addresses can be configured for the DHCP server in every mode. When the DHCP request message is received from an interface, the DHCP server of the interface is first used. If no DHCP server is configured on the interface, the DHCP server globally configured will be used.

The DHCP supports vrf-based relay function by adding the vtf parameter to the IP address of the DHCP server.

To configure the IP address of the DHCP server, exeute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip helper-address** [**vrf** {*vrf-name*} **| global**] *A.B.C.D*	Configure the IP address of the DHCP server globally.
DES-7200(config-if)# **ip helper-address** [**vrf** {*vrf-name*} **| global**] *A.B.C.D*	Configure the IP address of the DHCP server on the interface. This command must be set on the layer-3 interface.
DES-7200(config)# **no IP helper-address** [**vrf** {*vrf-name*} **| global**] *A.B.C.D*	Delete the globally configured IP address of the DHCP server.
DES-7200(config-if)# **no IP helper-address** [**vrf** {*vrf-name*} **| global**] *A.B.C.D*	Delete the IP address of the DHCP server configured on the interface.

5.2.3 Configuring DHCP option dot1x

Description in Understanding the DHCP Relay Agent Information shows that we can configure **ip dhcp relay information option dot1x** to enable the **option dot1x** function of the DHCP relay when you need to assign the IP addresses with different privileges to the users of different privileges. When this function is enabled, the device will work with 802.1x to add corresponding option information to the DHCP server when it relays. This function should be used with the dot1x function.

To configure DHCP option dot1x, execute the following commands in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **ip dhcp relay information option dot1x**	Enable the DHCP option dot1x function.
DES-7200(config)# **no ip dhcp relay information option dot1x**	Disable the DHCP option dot1x function.

5.2.4 Configuring DHCP option dot1x access-group

In the option dot1x application scheme, the device needs to restrict the unauthorized IP address or the IP address with low privilege to access certain IP addresses, and restrict the access between users with low privileges. To do so, configure the command **ip dhcp relay information option dot1x access-group** *acl-name*. Here the ACL defined by *acl-name* must be configured in advance. It is used to filter some contents and prohibit unauthorized users from accessing each other. In addition, ACL associated here is applied to all the ports on the device. This ACL has not default ACE and is not conflicted with ACLs associated with other interfaces. For example:

Assign a type of IP addresses for all the unauthorized users, namely 192.168.3.2-192.168.3.254, 192.168.4.2-192.168.4.254, and 192.168.5.2-192.168.5.254. 192.168.3.1, 192.168.4.1, and 192.168.5.1 are gateway addresses that are not assigned to users. In this way, an unauthorized user uses one of the 192.168.3.x-5.x addresses to access the Web portal for downloading client software. Therefore, the device should be configured as follows:

```
DES-7200# config
DES-7200(config)# ip access-list extended DenyAccessEachOtherOfUnauthrize
DES-7200(config-ext-nacl)# permit ip any host 192.168.3.1    //Packet that
can be sent to the gateway
DES-7200(config-ext-nacl)# permit ip any host 192.168.4.1
DES-7200(config-ext-nacl)# permit ip any host 192.168.5.1
DES-7200(config-ext-nacl)# permit ip host 192.168.3.1 any
```

//Permit the packets whose source IP address is the gateway.

```
DES-7200(config-ext-nacl)# permit ip host 192.168.4.1 any
DES-7200(config-ext-nacl)# permit ip host 192.168.5.1 any
DES-7200(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.3.0
0.0.0.255
```

//Prohibit unauthorized users from accessing each other

```
DES-7200(config-ext-nacl)# deny ip 192.168.3.0  0.0.0.255  192.168.4.0
0.0.0.255
```

```
DES-7200(config-ext-nacl)# deny ip 192.168.3.0 0.0.0.255 192.168.5.0
0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.4.0
0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.4.0 0.0.0.255 192.168.5.0
0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.5.0
0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.3.0
0.0.0.255
DES-7200(config-ext-nacl)# deny ip 192.168.5.0 0.0.0.255 192.168.4.0
0.0.0.255
DES-7200(config-ext-nacl)# exit
```

Then, apply the command to the global interfaces using the **ip dhcp relay information option dot1x access-group** *DenyAccessEachOtherOfUnauthrize* command.

To configure **DHCP option dot1x access-group**, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp relay information option dot1x access-group** *acl-name*	Enable DHCP option dot1x acl.
DES-7200(config)# **no ip dhcp relay information option dot1x access-group** *acl-name*	Disable DHCP option dot1x acl.

5.2.5 Configuring DHCP option 82

When the **ip dhcp relay information option82** command is configured, the device adds **option** in the format as described in Understanding **DHCP Relay Agent Information** to the DHCP server during DHCP relay.

To configure DHCP option82, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp relay information option82**	Enable the DHCP option82 function.
DES-7200(config)# **no ip dhcp relay information option82**	Disable the DHCP option82 function.

5.2.6 Configuring DHCP option VPN

To enable DHCP Relay in the MPLS VRF environment, execute the **ip dhcp relay information option vpn** command in the global configuration mode by setting VPN-ID, Subnet-Selection and Server-id Override options.

The VPN-ID option carried with the DHCP request message indicates the VPN (VRF environment) from which the DHCP Request message comes. The DHCP response message from the DHCP server to the DHCP relay also carries with VPN-ID based on which the DHCP relay forwards the DHCP response message to the right VRF.

In traditional process of DHCP relay, the gateway address field of the DHCP message indicates the subnet where the DHCP client locates in and the communication address of the DHCP Server and the DHCP relay. In multi-VRF environment, however, the IP address of the interface through which the DHCP relay connects to the DHCP Server belogns to the global routing table. The gateway address field of the DHCP message from the DHCP relay to the DHCP Server indicates the communication address of the DHCP Server and the DHCP relay. The Subnet-Selection option carries with the IP address of the interface through which the DHCP relay connects to the DHCP Server to notify the DHCP server of the subnet where the DHCP client locates in.

In the MPLS VPN environment, the DHCP client cannot send RENEW and RELEASE messages from the VRF to which it belongs to the global DHCP Server. The Server-id-Override option carries with the IP address of the VRF interface through which the DHCP relay connects to the DHCP Server. For the DHCP response message from the DHCP Server to the DHCP relay, the Server-id-Override option is used to override the Server ID address field. As a result, the DHCP client sends RENEW and RELEASE messages to the corresponding DHCP Relay which then forwards the messages to the DHCP Server.

Command	Function
DES-7200(config)# **ip dhcp relay information option vpn**	Enable the DHCP Aware VRF function.
DES-7200(config)# **no ip dhcp relay information option vpn**	Disable the DHCP Aware VRF function.

5.2.7 Configuring DHCP relay check server-id

After the **ip dhcp relay check** *server-id* command is configured, the device resolves DHCP SERVER-ID option upon receiving DHCP relay. If this option is set, the DHCP request message is sent to this server only, instead of other configured servers.

To configure **DHCP relay check** *server-id* function, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip dhcp relay check** *server-id*	Enable the DHCP relay check server-di function.
DES-7200(config)# **no ip dhcp relay check** *server-id*	Disable the DHCP relay check server-id function.

5.2.8 Configuring DHCP Relay Suppression

After the **ip dhcp relay suppression** command is configured, the port will not relay the DHCP request broadcast packet by transforming it into the unicast form. However, it will not suppress the normal forwarding of broadcast packets received.

To configure DHCP relay suppression, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip dhcp relay Suppression**	Enable the DHCP relay suppression function.
DES-7200(config-if)# **no ip dhcp relay Suppression**	Disable the DHCP relay suppression function.

5.2.9 DHCP Configuration Example

The following commands enable the DHCP relay function and add two groups of IP addresses of the DHCP server:

```
DES-7200# configure terminal
DES-7200(config)# service dhcp                    //Enable the dhcp relay function
DES-7200(config)# ip helper-address 192.18.100.1   //Add an IP address globally
```

```
DES-7200(config)# ip helper-address192.18.100.2     //Add an IP address
globally
DES-7200(config)# interface GigabitEthernet 0/3
DES-7200(config-if)# ip helper-address 192.18.200.1 //Add an IP address on
the interface
DES-7200(config-if)# ip helper-address 192.18.200.2 // Add an IP address on
the interface
DES-7200(config-if)# end
```

5.3 Other Precausions on DHCP Relay Configuration

For layer 2 network devices, you must enable at least one of the option dot1x, dynamic address binding and option82 functions when the cross-management vlan relay function is required. Otherwise, only the relay function of management VLAN can be enabled for the layer 2 device.

5.3.1 Precautions on DHCP option dot1x Configuration

1. This command works only when the configuration related to AAA/802.1x is correct.
2. When this scheme is adopted, the IP authorization of the DHCP mode of 802.1x should be enabled.
3. This command cannot be used together with command **dhcp option82** because they are conflicted.
4. When the IP authorization of the DHCP mode of 802.1x is enabled, the MAC address and the IP address will also be bound. Therefore, IP authorization and DHCP dynamic binding function cannot be enabled at the same time.

5.3.2 Precautions on DHCP option82 Configuration

The DHCP option82 function and the **dhcp option dot1x** function cannot be used at the same time because they are conflicted.

5.4 Showing DHCP Configuration

Show the DHCP configuration using the **show running-config** command in the privileged mode.

```
DES-7200# show running-config
Building configuration...
Current configuration : 1464 bytes
version DNOS 10.1.00(1), Release(11758)(Fri Mar 30 12:53:11 CST 2007 -nprd
hostname DES-7200
vlan 1
ip helper-address 192.18.100.1
ip helper-address 192.18.100.2
ip dhcp relay information option dot1x
interface GigabitEthernet 0/1
interface GigabitEthernet 0/2
interface GigabitEthernet 0/3
no switchport
ip helper-address 192.168.200.1
ip helper-address 192.168.200.2
interface VLAN 1
ip address 192.168.193.91 255.255.255.0
line con 0
exec-timeout 0 0
line vty 0
exec-timeout 0 0
login
password 7 0137
line vty 1 2
login
password 7 0137
line vty 3 4
login
end
```

5.5 Typical DHCP Relay Configuration Example

5.5.1 Topological Diagram

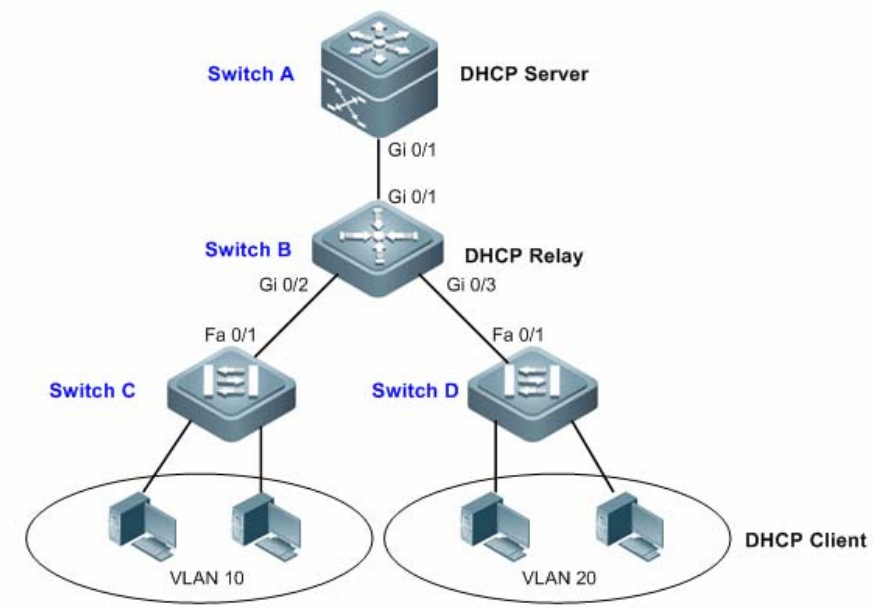


Diagram for DHCP Relay configuration

5.5.2 Application Requirements

As shown above, Switch C and Switch D are access devices connecting with PC users belonging to VLAN 10 and VLAN 20. Switch B is the gateway device, while Switch A is the core routing device. The following requirements must be met:

- Switch A can serve as DHCP Server allocating dynamic IP addresses to VLAN users.
- The users connecting to Switch C and Switch D can acquire dynamic IP addresses across the network segment.

5.5.3 Configuration Tips

1. Configuring DHCP Server: On Switch A, create DHCP address pools for users from VLAN 10 and VLAN 20 respectively, and enable DHCP Server (relevant configurations of DHCP Server can be found in "DHCP Configuration").

2. Configuring DHCP Relay: On Switch B, configure the address of DHCP Server (configure the address of DHCP Server as 10.1.1.2/24) and enable DHCP Server.

Note

On Switch C and Switch D, configure the VLAN to which the corresponding ports belong, and the access PC can acquire dynamic IP address once connected.

5.5.4 Configuration Steps

Step 1: Configure DHCP Server.

! In global mode, create a DHCP address pool named "vlan10" on Switch A, with corresponding IP network segment being 192.168.1.0/24 and the address of network gateway being 192.168.1.1.

```
SwitchA(config)#ip dhcp pool vlan10
SwitchA(dhcp-config)#network 192.168.1.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.1.1
SwitchA(dhcp-config)#exit
```

! Create an address pool named "vlan20", with IP network segment being 192.168.2.0/24 and gateway address being 192.168.2.1.

```
SwitchA(config)#ip dhcp pool vlan20
SwitchA(dhcp-config)#network 192.168.2.0 255.255.255.0
SwitchA(dhcp-config)#default-router 192.168.2.1
SwitchA(dhcp-config)#exit
```

! In global configuration mode, configure 192.168.1.1 and 192.168.2.1 as the excluded addresses, so as to avoid the conflict between allocated IP address and gateway address.

```
SwitchA(config)#ip dhcp excluded-address 192.168.1.1
SwitchA(config)#ip dhcp excluded-address 192.168.2.1
```

! Enable DHCP Server.

```
SwitchA(config)#service dhcp
```

Step 2: Configure layer-3 communication between Switch A and Switch B.

! On Switch A, configure port Gi 0/1 as the Route Port, with corresponding IP address being 10.1.1.2/24.

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

! On Switch B, configure port Gi 0/1 as the Route Port, with corresponding IP address being 10.1.1.3/24.

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if)#no switchport
SwitchB(config-if)#ip address 10.1.1.3 255.255.255.0
SwitchB(config-if)#exit
```

! Configure default route on Switch A

```
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 10.1.1.3
```

Step 3: Configure the gateway for access users.

! On Switch B, configure the SVI of VLAN 10 to 192.168.1.1/24.

```
SwitchB(config)#vlan 10
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 10
SwitchB(config-if)#ip address 192.168.1.1 255.255.255.0
SwitchB(config-if)#exit
```

! Configure the SVI of VLAN 20 to 192.168.2.1/24.

```
SwitchB(config)#vlan 20
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 20
SwitchB(config-if)#ip address 192.168.2.1 255.255.255.0
SwitchB(config-if)#exit
```

Step 4: Configure DHCP Relay.

! On Switch B, globally configure the address of DHCP server as 10.1.1.2 and enable DHCP Server.

```
SwitchB(config)#ip helper-address 10.1.1.2
SwitchB(config)#service dhcp
```

Step 5: Configure layer-2 communication between Switch B and Switch C/D.

! On Switch B, configure ports Gi 0/2 and Gi 0/3 as the Trunk Port.

```
SwitchB(config)#interface range gigabitEthernet 0/2-3
SwitchB(config-if-range)#switchport mode trunk
```

! Configure port Fa 0/1 of Switch C and Switch D as the Trunk Port.

5.5.5 Verification

Step 1: Display configurations of respective devices.

! Configurations of Switch A

```
SwitchA#show running-config
!
service dhcp
```

```
!
ip dhcp excluded-address 192.168.1.1
ip dhcp excluded-address 192.168.2.1
!
ip dhcp pool vlan10
 network 192.168.1.0 255.255.255.0
 default-router 192.168.1.1
!
ip dhcp pool vlan20
 network 192.168.2.0 255.255.255.0
 default-router 192.168.2.1
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
ip route 0.0.0.0 0.0.0.0 10.1.1.3
!
```

! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.3 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface GigabitEthernet 0/3
 switchport mode trunk
!
interface VLAN 10
 no ip proxy-arp
```

```
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.2.1 255.255.255.0
!
```

Step 2: Connect two PCs with the ports belonging to VLAN 10 and VLAN 20 and verify dynamic IP address allocation.

```
SwitchA#show ip dhcp binding
IP address Client-Identifier/ Lease expiration  Type Hardware address
192.168.1.2 0100.1320.4990.14 000 days 23 hours 59 mins  Automatic
192.168.2.2 0100.e04c.70b7.e2 000 days 23 hours 59 mins  Automatic
```

5.6 Typical Option dot1x Configuration Example

5.6.1 Topological Diagram

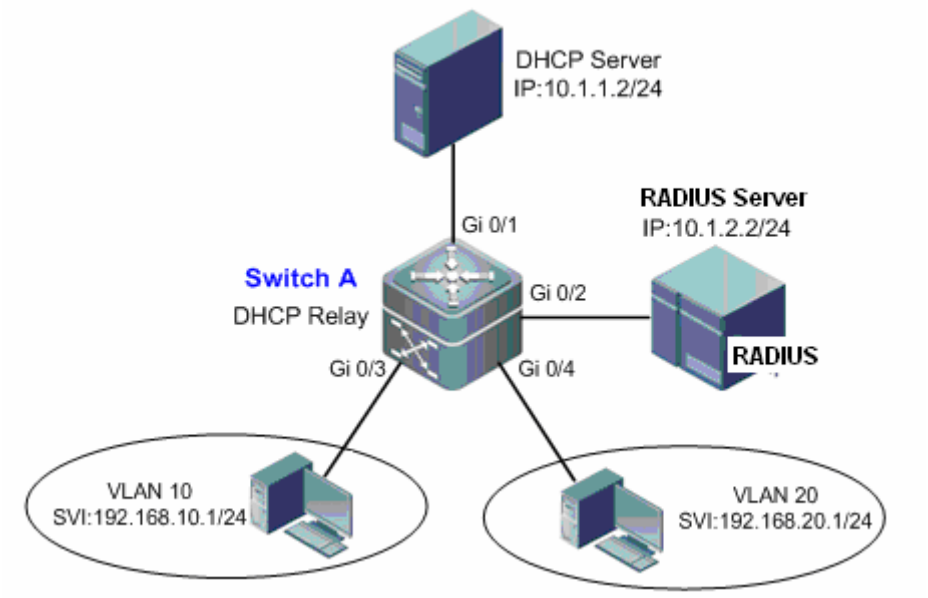


Diagram for DHCP Option Dot1x

5.6.2 Application Requirements

- Switch A is a layer-3 device allowing route communication between different network segments.

- Access users belonging to different VLANs access Internet after Dot1x authentication, and RADIUS Server assigns different access privileges to different users.
- DHCP Server can allocate IP addresses to users according to the privilege of authenticated user.

5.6.3 Configuration Tips

1. Configure basic DHCP Relay: On Switch A, configure the address of DHCP Server (10.1.1.2/24) and enable DHCP Server. After configuration, the user can acquire dynamic IP address across the network segment.

2. Configure 802.1X authentication: On Switch A, enable 802.1X authentication and set the user ports to controlled ports (Gi 0/3 and Gi 0/4). After configuration, the user will need to pass Dot1x authentication before accessing Internet.

3. Configure the assignment of privilege-based IP address: On Switch A, enable DHCP Option dot1x and configure IP authorization mode as DHCP Server mode. After configuration, the DHCP Server can allocate IP addresses according to user's privilege.

Note

1. Relevant configurations of 802.1X are detailed in "802.1X Configuration"
2. The realization of this example also needs the configuration of RADIUS Server and DHCP Server. For relevant details, please refer to the relevant documents.

5.6.4 Configuration Steps

Configure Switch A

Step 1: Configure the address of user gateway and the address of server interface.

! Configure the VLANs corresponding to Gi 0/3 and Gi 0/4 and configure the SVI corresponding to each VLAN.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-if-GigabitEthernet 0/3)#switchport access vlan 10
DES-7200(config-if-GigabitEthernet 0/3)#exit
DES-7200(config)#interface gigabitEthernet 0/4
DES-7200(config-if-GigabitEthernet 0/4)#switchport access vlan 20
DES-7200(config-if-GigabitEthernet 0/4)#exit
```

```
DES-7200(config)#interface vlan 10
DES-7200(config-if-VLAN 10)#ip address 192.168.10.1 255.255.255.0
DES-7200(config-if-VLAN 10)#exit
DES-7200(config)#interface vlan 20
DES-7200(config-if-VLAN 20)#ip address 192.168.20.1 255.255.255.0
DES-7200(config-if-VLAN 20)#exit
```

! Configure the interface address of DHCP Server and RADIUS Server.

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#no switchport
DES-7200(config-if-GigabitEthernet 0/1)#ip address 10.1.1.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 0/1)#exit
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
DES-7200(config-if-GigabitEthernet 0/2)#ip address 10.1.2.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 0/2)#exit
```

Step 2: Configure relevant features of DHCP Relay.

! Configure the address of DHCP server as 10.1.1.2/24 and enable DHCP service.

```
DES-7200(config)#ip helper-address 10.1.1.2
DES-7200(config)#service dhcp
```

! Enable DHCP Option dot1x.

```
DES-7200(config)#ip dhcp relay information option dot1x
```

Step 3: Configure 802.1X relevant features.

! Enable AAA and configure the address of Radius Server as 10.1.2.2/24; configure Radius Key as "DES-7200".

```
DES-7200(config)#aaa new-model
DES-7200(config)#radius-server host 10.1.2.2
DES-7200(config)#radius-server key DES-7200
```

! Create Dot1x authentication method list named "d1x" and configure Dot1x to apply such authentication method list.

```
DES-7200(config)#aaa authentication dot1x d1x group radius
DES-7200(config)#dot1x authentication d1x
```

! Configure ports Gi 0/3 and Gi 0/4 as controlled ports.

```
DES-7200(config)#interface range gigabitEthernet 0/3-4
DES-7200(config-if-range)#dot1x port-control auto
DES-7200(config-if-range)#exit
```

! Configure IP authorization mode as DHCP Server mode.

```
DES-7200(config)#aaa authorization ip-auth-mode dhcp-server
```

5.6.5 Verification

Step 1: Display configurations of respective devices.

! Configurations of Switch A

```
DES-7200#show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode dhcp-server
aaa authentication dot1x d1x group radius
!
vlan 10
!
vlan 20
!
service dhcp
ip helper-address 10.1.1.2
!
ip dhcp relay information option dot1x
!
radius-server host 10.1.2.2
radius-server key DES-7200
!
dot1x authentication d1x
interface GigabitEthernet 0/1
 no switchport
 no ip proxy-arp
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet 0/2
 no switchport
 no ip proxy-arp
 ip address 10.1.2.1 255.255.255.0
!
interface GigabitEthernet 0/3
 switchport access vlan 10
 dot1x port-control auto
!
interface GigabitEthernet 0/4
 switchport access vlan 20
 dot1x port-control auto
```

```
!
interface VLAN 10
 no ip proxy-arp
 ip address 192.168.10.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 192.168.20.1 255.255.255.0
!
```

6 UDP-Helper Configuration

6.1 UDP-Helper Configuration

6.1.1 UDP-Helper Overview

The main function of UDP-Helper is to implement the relay and forward of UDP broadcast packets. By configuring the destination server for the UDP broadcast packets to be forwarded, the UDP-Helper can convert the UDP broadcast packets into the unicast packets and then send them to the specified destination server. The UDP-Helper acts like a relay.

Once enabled, the UDP-Helper will check to see whether the destination UDP port number of the received broadcast packets matches the port number to be forwarded. If so, it modifies the destination IP address of packets as the IP address of the specified destination server, and send the packets to the destination server in unicast form.

When the UDP-Helper is enabled, the broadcast messages from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

Note

The relay of BOOTP/DHCP broadcast packet is implemented through the UDP Port 67 and 68 by the DHCP Relay module; therefore, the two ports can not be configured as the relay port of UDP-Helper.

6.2 Configuring UDP-Helper

6.2.1 Default UDP-Helper Configuration

Default UDP-Helper configuration

Attribute	Default value

Attribute	Default value
Relay and forwarding	Disabled
UDP port for relay and forwarding	When the UDP-Helper is enabled, the UDP broadcast packets from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.
Destination server for delay and forward	None

6.2.2 Enable the Relay and Forward Function of the UDP-Helper

Command	Function
DES-7200(config)# **udp-helper Enable**	Enable the relay and forward function of UDP broadcast packets. This function is disabled by default.

The **no udp-helper enable** command is used to disable the relay and forward funciton of the UDP-Helper.

Note

1. The relay and forwarding function is disabled by default.
2. When the UDP-Helper is enabled, the broadcast packets from UDP Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.
3. When the UDP-Helper is disabled, all of the configured UDP ports including the default ports are cancelled.

6.2.3 Configuring the Destination Server for Relay and Forwarding

Command	Function
DES-7200(config-if)# **ip helper-address** *IP-address*	Configure the destination server to which the UDP broadcast packets are relayed and forwarded. By default, it is not configured.

The **no ip helper-address** command can be used to remove the destination server for relay and forwarding.

Note

1. At most 20 destination servers can be configured for an interface.
2. If the destination server for relay and forwarding is configured on a specified interface, when the UDP-Helper is enabled, the broadcast packets of the specified UDP port received from this interface will be sent to the destination server configured for this interface in unicast form.

6.2.4 Configuring the UDP Port for Relay and Forwarding

Command	Function
DES-7200(config)# **ip forward-protocol udp** *ID*	Configure the UDP port for relay and forwarding. If only the UDP parameter is specified, the default port will be used for relay and forwarding; otherwise, the port can be configured upon necessary. When the UDP-Helper is enabled, the broadcast packets from Ports 69, 53, 37, 137, 138 and 49 are relayed and forwarded by default.

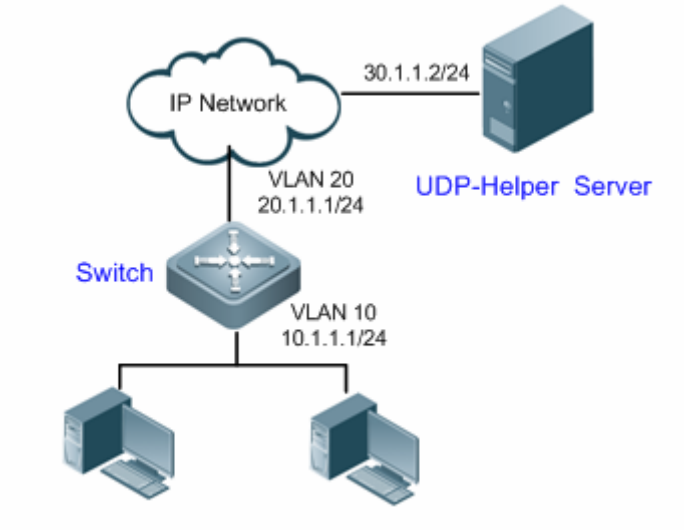
The **no ip forward-protocol udp port** command can be used to disable the UDP port for relay and forwarding.

Note

- Only when the function of delay and forwarding is enabled for the UDP-Helper and the destination server is configured for the relay and forwarding, can the UDP port be configured for relay and forwarding. Otherwise, the error prompts will appear.
- When the relay and forwarding function of the UDP-Helper is enabled, the function of forwarding the broadcast UDP packets from the default ports 69, 53, 37, 137, 138 and 49 will be enabled right now without any configuration.
- At most 256 UDP ports are supported for relay and forwading by the switch.
- Two ways can be used to configure the default ports, for example, the **ip forward-protocol udp domain** and **ip forward-protocol udp** *53* commands do the same thing.

6.3 UDP-Help Configuration Example

6.3.1 Topology Diagram



Networking diagram for UDP-Helper configuration

6.3.2 Application Requirements

It is required that the switch shall be able to forward UDP broadcast packets with destination port being 1000 to the specified UDP-Helper server (with server IP being 30.1.1.2/24).

6.3.3 Configuration Tips

Steps to configure UDP-Helper relay forwarding feature on the device:

1. Enable UDP-Helper relay forwarding
2. Configure the destination server of UDP-Helper relay forwarding
3. Configure the destination port number of UDP broadcast packets for relay forwarding (in this example, UDP broadcast packets with destination port being 1000 are subject to relay forwarding; meanwhile, the device will by default forward UDP broadcast packets containing destination port numbers of 69, 53, 37, 137, 138 and 49).

Note

- UDP port for relay forwarding can only be configured after UDP-Helper relay forwarding is enabled and the destination server is configured, or else the error message will be displayed.
- After enabling UDP relay forwarding, the device will immediately forward UDP broadcast packets containing the default port numbers of 69, 53, 37, 137, 138 and 49 without further configuration.

6.3.4 Configuration Steps

Before configuring relevant features of UDP-Helper, please make sure the route from switch to network segment of UDP-Helper server is reachable. The IP addresses configured on respective interfaces are shown in the topological diagram. Here we will introduce how to configure relevant features of UDP-Helper.

Step 1: Enable UDP-Helper relay forwarding on the Switch

```
DES-7200(config)#udp-helper enable
```

Step 2: Configure the IP address for the destination server of UDP-Helper relay forwarding as 30.1.1.2 on SVI 10.

```
DES-7200(config)#vlan 10
DES-7200(config-vlan)#exit
DES-7200(config)#interface vlan 10
DES-7200(config-if-VLAN 10)#ip address 10.1.1.1 255.255.255.0
DES-7200(config-if-VLAN 10)# ip helper-address 30.1.1.2
DES-7200(config-if-VLAN 10)#exit
```

Step 3: Configure the Switch to forward UDP broadcast packets carrying the destination port number of 1000.

```
DES-7200(config)#ip forward-protocol udp 1000
```

6.3.5 Verify Configurations

- Display configurations of the switch. Key points: whether relay forwarding is enabled or not; IP address of relay server; destination port number carried in UPD broadcast packets requiring relay forwarding.

```
DES-7200#show run
!
udp-helper enable
!
```

```
vlan 10
!
ip forward-protocol udp 1000
!
interface VLAN 10
 no ip proxy-arp
 ip helper-address 30.1.1.2
 ip address 10.1.1.1 255.255.255.0
!
interface VLAN 20
 no ip proxy-arp
 ip address 20.1.1.1 255.255.255.0
!
```

- Verify whether relay forwarding has taken effect.

Step 1: Send UDP broadcast packets carrying the destination port number of 999

PC1 sends a UDP broadcast packet with the following format:

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:999
```

PC2 acts as UDP-Helper server. Such packet is not received on PC2.

Step 2: Send UDP broadcast packets carrying the destination port number of 1000.

PC1 sends a UDP broadcast packet with the following format:

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:1000
```

PC2 acts as UDP-Helper server. Such packet is received on PC2. The destination IP address of packet is 30.1.1.2, and the data contained are the same as the packets sent.

Step 3: Send UDP broadcast packets with destination port number being 69, 53, 37, 137, 138 or 49.

PC1 sends a UDP broadcast packet with the following format (taking destination port number of 69 as the example):

```
Src_mac:0000.0000.0001
Dst_mac:0xFFFFFFFFFFFF
Src_ip:1.0.0.3
Dst_ip:255.255.255.255
Dst_port:69
```

PC2 acts as UDP-Helper. Such packet is received on PC2. The destination IP address of packet is 30.1.1.2, and the data contained are the same as the packets sent.

From the above verification output, we can learn that the switch has successfully forwarded UDP broadcast packets with user-defined destination port number (destination port number 1000 and default numbers of 69, 53, 37, 137, 138, and 49) to the specified UDP-Helper server.

7 DHCPv6 Server Configuration

7.1 Introduction to DHCPv6 Server

7.1.1 Overview of DHCPv6 Server

Along with the development of IPv6 network, IPv6-based network is being applied more and more widely. In IPv6 network, the 128-bit IPv6 addresses are usually written in hexadecimal format. This feature has made manual address assignment very difficult, as the format of IPv6 address doesn't look intuitive. Therefore, the automatic assignment of IPv6 addresses has become an important part of network planning. In order to facilitate address assignment without manual intervention or with minimum manual intervention, several methods and technologies have been developed for address assignment and parameter configuration of IPv6 hosts. Here are several methods for IPv6 address assignment:

1. Manual assignment

IPv6 address can be configured manually. This method is applicable to the configuration of routing interface and static network parameters. Of course, manual assignment may easily go wrong during the handling of hexadecimal 128-bit IPv6 addresses.

2. Stateless address auto-configuration

Stateless Address Auto-configuration is best suited for address assignment of IPv6 nodes without any manual intervention. To apply this method on an IPv6 node, this node must be connected to at least one IPv6 router through the network. The IPv6 router will be configured by the administrator and send Router Advertisement messages on the link. These messages will be received by local IPv6 nodes, which will automatically complete the configuration of IPv6 address and routing parameters without manual intervention.

3. Stateful DHCPv6

The DHCPv6 protocol (Dynamic Host Configuration Protocol for IPv6) as defined in RFC3315 allows the DHCP Server to send configuration parameters such as IPv6 address to IPv6 nodes, and also allows flexible assignment and reuse of network addresses.

4. DHCPv6-PD

The DHCPv6-PD (DHCPv6 Prefix Delegation) as defined in RFC3633 is an extension of DHCPv6. In typical DHCPv6 application, DHCPv6 Server will assign stateful IPv6 address to a DHCPv6 Client. As an extended feature, DHCPv6-PD Server can assign a complete subnetwork and other network and interface parameters to DHCPv6-PD Client through Prefix Delegation message.

5. Stateless DHCPv6

Stateless DHCPv6 integrates the features of stateless address auto-configuration and stateful DHCPv6. The device can use stateless address auto-configuration to acquire IPv6 address, and utilize DHCPv6 to acquire more parameters in the mean time. These parameters cannot be provided through stateless address auto-configuration. The device may use such information to complete all configurations.

Note	Under certain circumstances, in network planning, the aforementioned IPv6 address and parameter allocation methods can be used simultaneously.

DES-7200 DHCPv6 Server supports the assignment of IPv6 address and prefix. IPv6 address assignment refers to the auto-configuration of IPv6 address for DHCPv6 Client, while prefix assignment allows flexible site-level auto-configuration to control the site address space. Network terminals such as PC can combine stateless auto-configuration or stateful auto-configuration to achieve the auto-configuration of address and other network parameters. DES-7200 DHCPv6 Server also supports DHCPv6-PD Server expansion (hereafter referred to as DHCPv6 Server).

7.1.2 Basic Concepts of DHCPv6 Server

7.1.2.1 DUID

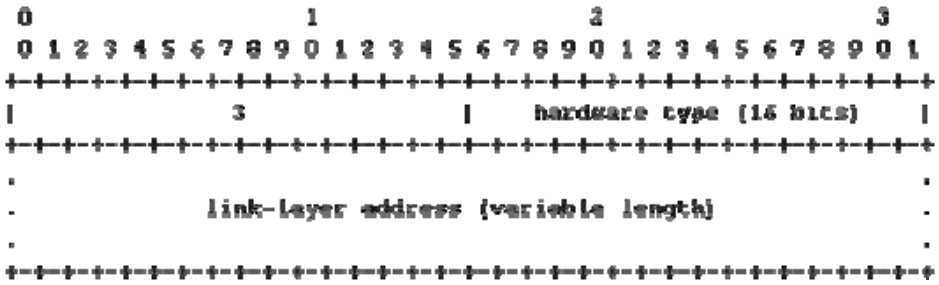
DUID refer to DHCP Unique Identifier. As clearly defined in RFC3315, each DHCPv6 device (including client, relay and server) must have a unique DHCPv6 identifier for mutual authentication during the exchange of DHCPv6 messages. Furthermore, DUID cannot be used for other purposes. For all DHCPv6 devices, DUID must not be reused and shall be stable to any device (i.e., the DUID of a device must not be changed due to the replacement of certain part). The length of a DUID must not exceed 128-byte, and there are three types of DUIDs:

1. DUID-LLT: DUID Based on Link-Layer address plus Time;

2. DUID-EN: DUID Assigned by Vendor Based on Enterprise Number；

3. DUID-LL: Link-Layer address, DUID-LL;

DES-7200 DHCPv6 devices currently adopt DUID-LL, the structure of which is shown below:



The value of DUID type is 0x0003 (DUID-LL); the value of Hardware type is 0x0001 (Ethernet); the value of Link layer address will be the MAC address of device.

7.1.2.2 DHCPv6 address assignment

Different from DHCPv4, the DHCPv6 Server assigns an Identity Association (IA) to the client instead of a single address, and each IA consists of the unique identifier of IAID (Identity association identifier), which is generated by DHCPv6 Client and associated with each IA. The IA and Client jointly establish the one-to-one corresponding relationship. Each IA contains multiple addresses, and the Client may assign the addresses of IA to other interfaces of the device. The addresses contained in IA can be divided into the following three categories:

1. NA: Non-temporary Addresses, the unique address in the world;
2. TA: Temporary Addresses (no related applications);
3. PD: Prefix Delegation, prefix space;

Therefore, given the difference in the addresses of IA, IA can be divided into IA_NA, IA_TA and IA_PD (IA-Type). DES-7200 DHCPv6 Server supports the assignment of IA_NA and IA_PD (no support to IA_TA).

7.1.2.3 DHCPv6 bindings

DHCPv6 Bindings are a group of manageable address information structures based on Identity Association (IA) and can be identified by both Server and Client. The binding data on Server will record the IA assigned to each Client and other

configuration information. Each Client can apply for multiple bindings. The binding data on Server are organized in the form of binding table and indexed by DUID, IA-Type and IAID.

7.1.2.4 Type of DHCPv6 messages

According to RFC3315, DHCPv6 uses UDP 546 and 547 ports to exchange messages: the DHCPv6 Client uses Port 546 to receive messages, while the DHCPv6 Server and Relay will use Port 547 to receive messages. The type of messages that can be exchanged between DHCPv6 Server, Client and Relay are shown below (as per RFC3315):

1. Type of messages sent from Client to Server include: Solicit, Request, Confirm, Renew, Rebind, Release, Decline, Information-request;

2. Type of messages sent from Server to Client include: Advertise, Reply, Reconfigure;

3. Type of messages sent from Relay to Relay to Server include: Relay-forward;

4. Type of messages sent from Server or Relay to Relay include: Relay-reply;

During message exchange, in order to simplify the exchange flow, not all types of messages will be used. Instead, flexible control can be realized through the DHCPv6 options carried by messages, and the data transmitted by messages will also change according to different options. The types and roles of DHCPv6 messages are similar to that of DHCPv4 messages. Although DHCPv6 messages have made some changes for the new network and flow, certain types of messages are still related. The comparison between DHCPv6 messages and DHCPv4 messages is shown below:

DHCPv6 messages	DHCPv4 messages
Solicit (1)	DHCPDISCOVER
Advertise (2)	DHCPOFFER
Request (3), Renew (5), Rebind (6)	DHCPREQUEST
Reply (7)	DHCPACK / DHCPNAK
Release (8)	DHCPRELEASE
Information-request (11)	DHCPINFORM
Decline (9)	DHCPDECLINE
Confirm (4)	NA
Reconfigure (10)	DHCPFORCERENEW

Relay-forward (12), Relay-reply (13)	NA

Caution	DES-7200 DHCPv6 Server doesn't support Reconfigure message. DHCPv4 related contents are detailed in the section of "DHCP configuration".

7.1.3 Operating principle of DHCPv6 Server

The application model of DHCPv6 basically follows the framework of DHCPv4, and is composed of Server, Client and Relay. The configuration parameters are obtained through the interaction between Client and Server, while the Relay can transparently link the Client with Server outside the local link. The message interaction and parameter maintenance basically follow the practices of DHCPv4, but DHCPv6 has modified the message structure and flow handling according to the new network. Comparing with DHCPv4, DHCPv6 has the following features:

1. DHCPv6 adopts a new message structure and has made huge modifications to the original DHCPv4 message by removing the optional parameters in the header of DHCPv4 messages and preserving few fields to be used in all interactions. Other optional fields are all encapsulated in the option field of messages.

2. DHCPv6 adopts the new address parameters. As mentioned above, in DHCPv6, the address field is deleted from the fixed header of DHCPv4 messages, and the entire address parameter and relevant time parameter are encapsulated in the IA option. Each DHCPv6 Client is associated with one IA, and each IA can contain multiple addresses and relevant time information. The corresponding IA can be generated in accordance with the type of address, such as IA_NA, IA_TA and IA_PD.

3. DHCPv6 has introduced the new server-side identifier for clients, namely DUID.

4. DHCPv6 supports stateless DHCPv6 auto-configuration. During the auto-configuration of network nodes, the address configuration is independent from parameter configuration, and each corresponding configuration can be acquired via the DHCP approach, that means the network node can acquire other non-address parameters from the DHCPv6 server. Compared with the allocation scheme of DHCPv4, this is a critical change.

5. DHCPv6 supports prefix-based allocation. Apart from IPv6 address, network prefix can also be allocated via DHCPv6.

The basic application model of DHCPv6 is shown in the following figure:

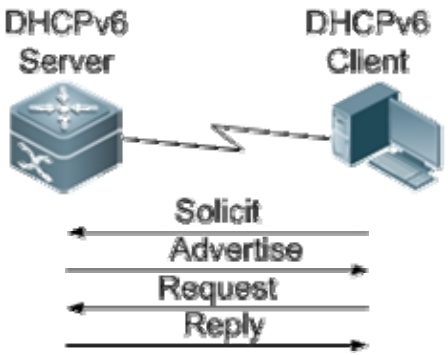


Fig 1. Typical DHCPv6 address assignment

The above figure is a typical process of DHCPv6 address assignment:

1. DHCPv6 Client sends a multicast Solicit message with destination address being FF02::1:2 and destination UDP port being 547 to the local link, and this message will be received by all DHCPv6 Servers and DHCPv6 Relays on the local link. Multicast is used instead of broadcast because broadcast has been abolished in the IPv6 network.

2. After receiving the multicast Solicit message, the DHCPv6 Server will reply with a unicast Advertise message.

3. After selecting the Server, the DHCPv6 Client will send a multicast Request message with destination address being FF02::1:2 and destination UDP port being 547 to the local link.

4. After receiving the Request message, DHCPv6 Server will send a unicast Reply message to complete the configuration process.

As mentioned above, such a 4-message DHCPv6 interaction is very similar to the 4-message interaction in DHCPv4 (Discover - Offer - Request - Reply). By utilizing the option of Rapid Commit, the 4-message interaction can be simplified into 2-message interaction (Solicit - Reply). If the Client includes this option in the Solicit message, the Server will send Reply message after receiving the corresponding message, as shown below:

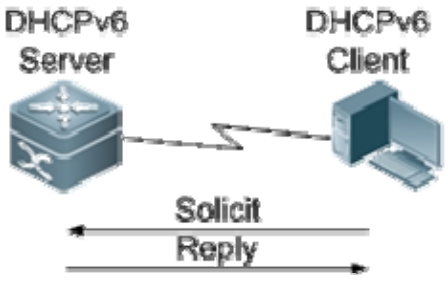


Fig 2. Simplified 2-message interaction

Between Server and Client, the Relay can be introduced to complete the address assignment between Client and Server. The Solicit message sent by the Client to the Server will be wholly encapsulated in the Relay-forward message as an option. The Server will decode the solicit information contained in the incoming message and encapsulate the reply information in the Relay option of Relay-reply message, and then send the Relay-reply message to the Relay, which will decode the reply information and forward to the Client, as shown below:

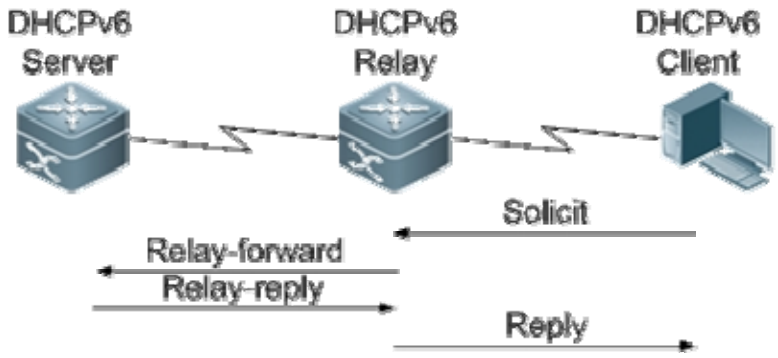


Fig 3. Interaction between Server, Relay and Client

In case the network connection of Client has changed, the Client will send Confirm message to the Server to verify the availability of the resources previously assigned by the Server. After receiving the message, the Server will respond with a Reply message, as shown below:

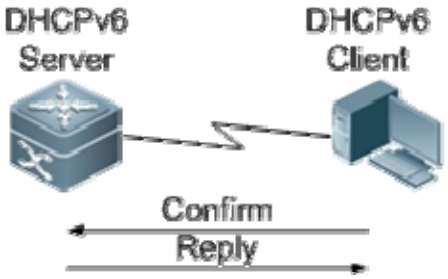


Fig 4. Server responding to the Confirm message

If the Client uses stateless address configuration but also acquires other parameters through DHCP, then the Client will send an Information-request message to the Sever, which will respond with a Reply message, as shown below:

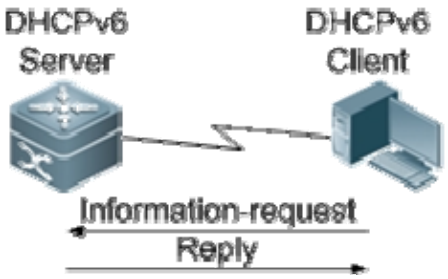


Fig 5. Server responding to the Information-request message

7.1.4 Protocol specification

DHCPv6 protocol specifications are detailed in RFC3315;

DHCPv6-PD protocol specifications are detailed in RFC3633;

7.2 Default configurations

The following table describes the default configurations of DHCPv6 Server.

Function	Default setting
DHCPv6 Server function	Disabled
DHCPv6 configuration information pool	Not configured

7.3 Configure DHCPv6 Server

7.3.1 Configure DHCPv6 Server

This task involves how to create and configure a DHCPv6 configuration information pool, and how to associate this pool with DHCPv6 Server on the interface. When this DHCPv6 Server is enabled, it will be able to assign addresses and other configuration information to clients. The configuration steps are shown below:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **ipv6 dhcp pool** *poolname*	Configure DHCPv6 configuration information pool and enter pool configuration mode.
DES-7200(config-dhcp)# **domain-name** *domain*	Configure a domain-name that can be assigned to DHCPv6 Client.

DES-7200(config-dhcp)# **dns-server** *ipv6-address*	Configure a DNS server for DHCPv6 Client.
DES-7200(config-dhcp)# **prefix-delegation** *ipv6-prefix/prefix-length client-DUID* [*lifetime*]	Configure an address prefix that can be assigned to a specific Client IA_PD.
DES-7200(config-dhcp)# **prefix-delegation pool** *poolname* [**lifetime** {*valid-lifetime* | *preferred-lifetime*}]	Configure a prefix pool for DHCPv6 Server, and address prefix can be assigned to clients from this prefix pool.
DES-7200(config-dhcp)# **iana-address prefix** *ipv6-prefix/prefix-length* [**lifetime** {*valid-lifetime* | *preferred-lifetime*}]	Configure an IA_NA address prefix for DHCPv6 Server, and IA_NA address can be assigned to clients within the scope of addresses designated by this prefix.
DES-7200(config-dhcp)# **exit**	Exit DHCPv6 pool configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter interface configuration mode.
DES-7200(config-if)# **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*]	Enable DHCPv6 Server on this interface.

Configuration example:

Configure a configuration information pool named pool1 and configure domain name, DNS Server, IA_NA, IA_PD and etc; then enable DHCPv6 Server on the interface of FastEthernet 0/1;

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# ipv6 dhcp pool pool1
DES-7200(config-dhcp)# domain-name example.com
DES-7200(config-dhcp)# dns-server 2008:1::1
DES-7200(config-dhcp)# prefix-delegation 2008:2::/64
0003000100d0f82233ac
DES-7200(config-dhcp)# prefix-delegation pool client-prefix-pool
lifetime 2000 1000
DES-7200(config-dhcp)# iana-address prefix 2008:50::/64
```

```
DES-7200(config-dhcp)# exit

DES-7200(config)# interface fastethernet 0/1

DES-7200(config-if)# ipv6 dhcp server pool1
```

7.3.2 Configure stateless DHCPv6 Server

Stateless DHCPv6 Server won't involve the configuration of prefix pool, because the Client has already obtained the address via RA. The Server will provide Client with configuration information other than the address. The configuration steps are shown below:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **ipv6 dhcp pool** *poolname*	Configure DHCPv6 configuration information pool and enter pool configuration mode.
DES-7200(config-dhcp)# **domain-name** *domain*	Configure a domain-name that can be assigned to DHCPv6 Client.
DES-7200(config-dhcp)# **dns-server** *ipv6-address*	Configure a DNS server for DHCPv6 Client.
DES-7200(config-dhcp)# **exit**	Exit DHCPv6 pool configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter interface configuration mode.
DES-7200(config-if)# **ipv6 dhcp server** *poolname* [**rapid-commit**] [**preference** *value*]	Enable DHCPv6 Server on this interface.
DES-7200(config-if)# **ipv6 nd other-config-flag**	Configure "other stateful configuration" flag bit in IPv6 RA.

Configuration example:

Configure a configuration information pool named pool1 and configure domain name, DNS Server and etc; then enable DHCPv6 Server on the interface of FastEthernet 0/1 and configure the flag bit in IPv6 RA.

```
DES-7200# configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
DES-7200(config)# ipv6 dhcp pool pool1

DES-7200(config-dhcp)# domain-name example.com

DES-7200(config-dhcp)# dns-server 2008:1::1

DES-7200(config-dhcp)# exit

DES-7200(config)# interface fastethernet 0/1

DES-7200(config-if)# ipv6 dhcp server pool1

DES-7200(config-if)# ipv6 nd other-config-flag
```

7.3.3 View DHCPv6 Server configurations

Use the following command to view DHCPv6 Server configurations and status information:

Command	Function
DES-7200# **show ipv6 dhcp**	Display the DUID information of the device.
DES-7200# **show ipv6 dhcp binding**	Display the address binding information of DHCPv6 server.
DES-7200# **show ipv6 dhcp interface**	Display DHCPv6 interface information.
DES-7200# **show ipv6 dhcp pool**	Display DHCPv6 pool information.

Example of viewing configurations:

```
DES-7200# show ipv6 dhcp

This device's DHCPv6 unique identifier(DUID): 00:03:00:01:00:d0:f8:22:33:b0


DES-7200# show ipv6 dhcp binding

           Client  DUID: 00:03:00:01:00:d0:f8:22:33:ac

             IAPD: iaid 0, T1 1800, T2 2880

               Prefix: 2001:20::/72

                      preferred lifetime 3600, valid lifetime 3600

                  expires at Jan 1 2008 2:23 (3600 seconds)
```

```
DES-7200# show ipv6 dhcp interface

            VLAN 1 is in server mode

              Server pool dhcp-pool

              Rapid-Commit: disable


DES-7200# show ipv6 dhcp pool

            DHCPv6 pool: dhcp-pool

              DNS server: 2011:1::1

              DNS server: 2011:1::2

              Domain name: example.com
```

7.4 Typical DHCPv6 Server configuration example

7.4.1 Networking requirements

Under the user environment, we usually need to deploy DHCPv6 Server at the core layer or convergence layer. The core-layer or convergence-layer device may also need to act as a DHCPv6 Server to assign and manage the IP addresses in the entire subnetwork.

7.4.2 Network topology

As shown below, we need to enable DHCPv6 Server function on the convergence-layer device in order to assign IPv6 address and other network configurations to PCs on the subnetwork. By configuring the range of available IA_NA addresses on the Server, the Server will be able to assign an available address to the PC from such range after receiving the solicit message from PC, which can return such address to the Server after use. Meanwhile, the Server can also provide such information as DNS Server address, domain name and etc.

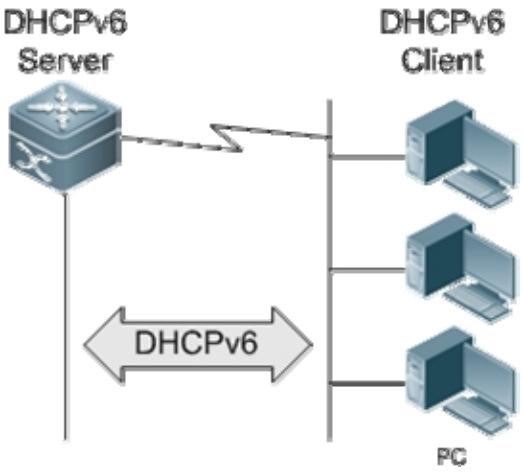


Fig 6. DHCPv6 Server network topology

7.4.3 Configuration tips

If the core device is used as DHCPv6 Server, the CPU and memory occupancy rate of such device may increase, and the pressure on Server will increase along with the rise in the number of clients. Therefore, DHCPv6 Server shall be a high-performance device and an independent device.

7.4.4 Configuration steps

1) Enable DHCPv6 Server function on the convergence-layer gateway device:

Configure a configuration information pool named pool1 and configure domain name, DNS Server, IA_NA and etc; then enable DHCPv6 Server on the interface of vlan 1.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# ipv6 dhcp pool pool1
DES-7200(config-dhcp)# domain-name example.com
DES-7200(config-dhcp)# dns-server 2008:1::1
DES-7200(config-dhcp)# iana-address prefix 2008:50::/64
DES-7200(config-dhcp)# exit
DES-7200(config)# interface vlan 1
DES-7200(config-if)# ipv6 dhcp server pool1
```

7.4.5 Verification

- Display DHCPv6 Server configuration of the gateway device:

```
DES-7200# show ipv6 dhcp interface

           VLAN 1 is in server mode

             Server pool pool1

             Rapid-Commit: disable


DES-7200# show ipv6 dhcp pool

           DHCPv6 pool: pool1

             DNS server: 2008:1::1

             Domain name: example.com
```

8 DHCPv6 Client Configuration

8.1 DHCPv6 Overview

Along with the development of IPv6 network, IPv6-based network is being applied more and more widely. As the framework proposed at the beginning of IPv6 design, the automatic configuration of network nodes has become a key feature of IPv6 network. In the new network framework, the concepts of stateless configuration and stateful configuration were brought forward. Through stateless auto-configuration, the new nodes in the network can complete all configurations via Route Advertisement; while in stateful auto-configuration, the network nodes need interact with relevant configuration server in the network in order to complete the configuration of network address and other parameters. As the only stateful configuration model developed at the present time, DHCPv6 is fully described in RFC3315.

Comparatively complete description on the application model of DHCPv6 has been given in RFC3315 (Dynamic Host Configuration Protocol for IPv6). Similar to the framework of sDHCPv4, the application model of DHCPv6 is composed of the DHCP server, DHCP clients and DHCP relay. The configuration parameters can be obtained through the interaction between DHCP clients and DHCP server, while the DHCP relay can link the DHCP clients with the DHCP server outside the local link. The message interaction and parameter maintenance basically follow the practices of DHCPv4, but DHCPv6 do give proper consideration to the message structure and process according to the new network.

In IPv6 network, the auto-configuration of network nodes can be divided into:

Stateless auto-configuration: Network nodes will acquire configuration parameters from route advertisement.

Stateful auto-configuration: Network nodes will acquire configuration parameters from the DHCPv6 server.

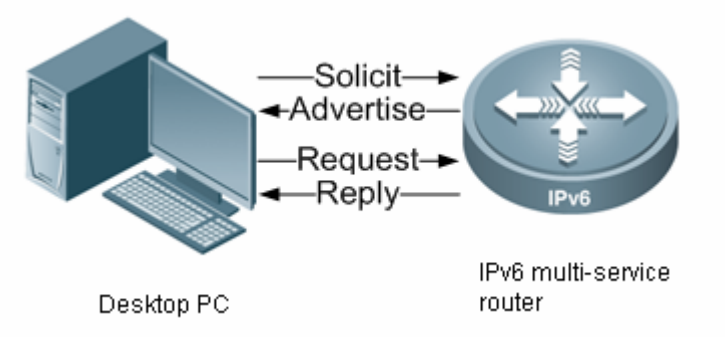


Fig 1 DHCPv6 stateful auto-configuration

As shown in the above figure, the new network node (host or interface) will send a multicast message (Solicit) to all the DHCPv6 servers and DHCPv6 relays in the local link (address: FF02::1:2; port: 547), and the DHCPv6 servers will send the unicast Advertise reply message after receiving such message. After selecting the DHCP server, the DHCP clients will send the Request message to solicit for configuration information, and the DHCP server will send Reply message after completing the allocation of parameters.

As mentioned above, such a 4-message interaction is very similar to the 4-message interaction in DHCPv4 (Discover - Offer - Request - Reply). Certainly, DHCPv6 has made further modifications and expansions.

- Multicast is used instead of broadcast because broadcast has been abolished in the IPv6 network.
- By utilizing the option of Rapid Commit, the 4-message interaction can be simplified into 2-message interaction (Solicit - Reply).
- New DHCP message structure, DHCPv6 has made huge modifications to the original DHCPv4 message, and has removed optional parameters in the header of DHCP message. Only few fields to be used in all interactions are preserved. Other optional fields are all encapsulated in the option field of the DHCP message. During the interaction with the DHCP server and the DHCP relay, the DHCP message sent by the DHCP client to the DHCP server will be wholly encapsulated in the DHCP relay message as an option.
- New address parameters. As mentioned above, in DHCPv6, the address field is deleted from the fixed header of the DHCP message, and the entire address parameters and relevant time parameters are encapsulated in an option called IA (Identity Association). Each DHCPv6 client is associated with one IA, and each IA can contain multiple addresses and relevant time information. The corresponding IA can be generated in accordance with the type of address, such as IA_NA (Identity association for non-temporary addresses) and IA_TA (Identity association for temporary addresses).
- New DHCP client/server identifier, namely DUID (DHCP Unique Identifier).

- Stateless DHCPv6 auto-configuration. During the auto-configuration of network nodes, the address configuration is independent from parameter configuration, and each corresponding configuration can be acquired via the DHCP protocol, which means network nodes can acquire other non-address parameters from the DHCPv6 server. Compared with the allocation method used in DHCPv4, this is a critical change. Relevant information is detailed in RFC3736.
- Prefix delegation. Apart from IPv6 address, network prefix can also be delegated via DHCPv6. This also accredits to the definition of IA in DHCPv6. A prefix can be delegated to the client in the form of address (or time parameter, etc) only by expanding the type of IA. Such a new type of IA is called IA_PD (Identity Association for Prefix Delegation), and it is detailed in RFC3633.

8.1.1 Introduction to the DHCPv6 Server

The DHCPv6 server realizes the allocation of IAPD and IANA. The allocation of IANA refers to the automatic allocation of IPv6 address to the DHCP client, which is similar to DHCPv4. The allocation of IAPD allows flexible site-level auto-configuration to control the address range of sites. Terminal devices (such as PC) can realize auto-configuration of address via stateless auto-configuration or stateful auto-configuration.

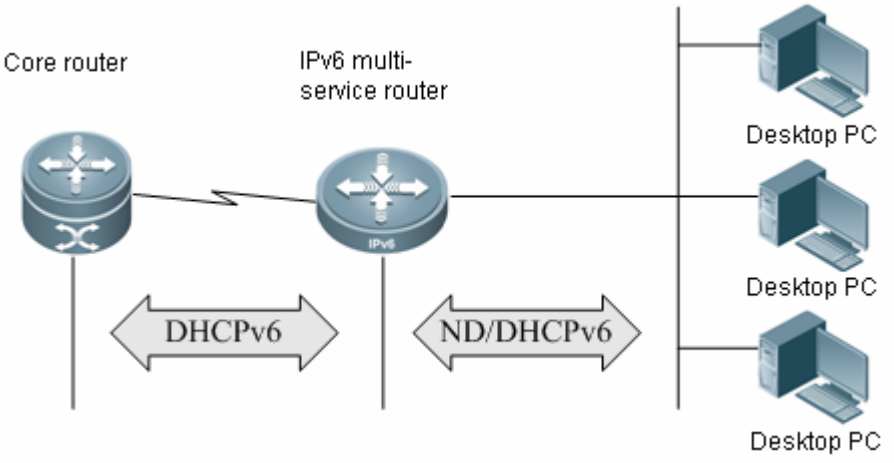


Fig 2 Prefix-based DHCPv6 application

The above figure illustrates the application of prefix-based DHCPv6 in IPv6 network.

- Core router runs prefix delegation (PD) based DHCPv6 server.
- IPv6 multi-service router runs the DHCPv6 client on the interface connecting to the core router, acquiring prefix space from the core router and storing it in the global prefix pool of IPv6.

- IPv6 multi-service router enables auto-configuration on the interface connecting to the desktop computer and runs interface-based router advertisement or address assignment (NA) based DHCPv6 server.
- The desktop computer completes address and parameter configuration via ND or address assignment (NA) based DHCPv6 client.

In the above model, DHCPv6 fulfils the following functions:

- The DHCP client (host, node) sends out prefix delegation (PD) based multicast solicit message within the link to look for DHCPv6 servers.
- The DHCP servers will send unicast advertisement message to the DHCP client after receiving such solicitation message.
- The DHCP client will select one server and send a multicast request message.
- The DHCP server will then send a unicast reply message to complete address assignment.

8.1.2 Introduction to the DHCPv6 Client

The DHCPv6 client can automatically acquire prefix space and other configuration parameters from the DHCPv6 server. After obtaining the prefix space, the DHCP client will store it in the global prefix space pool of IPv6, and then such prefix space can be assigned to other interfaces via prefix partition for prefix advertisement.

The DHCPv6 client gets relevant parameters based on interface, such as Domain Name Server, SNTP server. Relevant parameters configurations depend on the validity of interface.

8.1.3 Introduction to the DHCPv6 Relay

The DHCPv6 relay forwards DHCPv6 messages between the DHCPv6 server and the DHCP client. When the DHCP server and the DHCP client are not in the same physical network, the DHCP relay is responsible for forwarding the DHCP solicit and reply messages. The forwarding process is different from routing forwarding, which features transparent transmission. Generally, the router will not modify the contents of IP packets. Upon receiving the DHCP message, the DHCP relay will regenerate and forward another one.

The DHCP relay is just like a DHCP server for the DHCP clients and a DHCP client for the DHCP server.

8.2 DHCPv6 Configuration Task List

8.2.1 Configure the DHCPv6 Client

This task involves how to enable DHCPv6 client function and prefix solicitation on the interface.

To configure the DHCPv6 Client, run the following commands:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200 (config)# **interface** *type number*	Enter interface configuration mode.
DES-7200 (config-if)#**ipv6 dhcp client pd** *prefix-name* [*rapid-commit*]	Enable the DHCPv6 client and prefix solicitation on the interface.

For example:

```
DES-7200# configure terminal
DES-7200(config)# interface fastethernet 0/1
DES-7200(config-if)# ipv6 dhcp client pd pd_name
```

8.2.2 Restart the DHCPv6 Client on the Interface

To restart DHCPv6 Client on the interface, run the following commands:

Command	Function
DES-7200#**clear ipv6 dhcp client** *interface-type interface-number*	Restart the DHCPv6 client on this interface.

For example:

```
DES-7200# clear ipv6 dhcp client fastethernet 0/1
```

9 DHCPv6 Relay Agent Configuration

9.1 Understanding DHCPv6 Relay Agent

9.1.1 DHCPv6 Overview

With the IPv6 network development, IPv6 network is widely used gradually. One primary feature of the IPv6 network at the beginning of the IPv6 design is the autoconfiguration of the network node. The concepts of stateless autoconfiguration and stateful autoconfiguration are provided in the new network frame. For the stateless autoconfiguration, the newly-added network nodes complete all configurations through the Router Advertisement. While for the stateful autoconfiguration, the DHCPv6 server assigns the addresses and provides configuration parameters to the clients. For the detailed description about the DHCPv6, the only stateful autoconfiguration model at present, refer to the RFC3315. A typical exchange process between the DHCPv6 server and client is shown in the Figure-1:

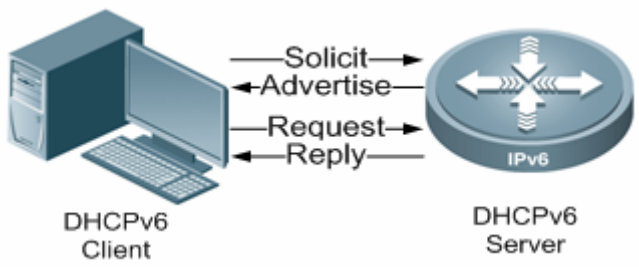


Figure-1 DHCPv6 Server-Client

1. The DHCPv6 Client sends the Solicit packet in the multicast form destined to the address FF02::1:2 and the UDP port 547 to the DHCPv6 Server and DHCPv6 Relay in the local link.
2. After the DHCPv6 Server receives the Solicit packet in the multicast form, it responses the Advertise packet in the unicast form.

3. After the DHCPv6 Client selects the DHCPv6 Server, the Client sends the Request packet in the multicast form destined to the address FF02::1:2 and the UDP port 547 within the local link.

4. After the DHCPv6 Server receives the Request packet, it sends the Reply packet in the unicast form. And it finishes the configuration process.

9.1.2 DHCPv6 Relay Agent Overview

In the section of *DHCPv6 Overview*, from the Figure-1, the DHCPv6 Client searches for the DHCPv6 Server through the reservation multicast address within the link range. To this end, the Client shall communicate with the Server. That is, the Client and the Server shall be configured in the same link, which brings about the management and upgrading inconvenience, economical waste(for example, configure one server in each sun-network), ect. DES-7200 product provides the DHCPv6 Relay Agent function to allow the clients to send the packets to the servers in the different links. The DHCPv6 Relay Agent can be generally configured in the clients' link and used to relay the exchange packets between the clients and the servers. For the clients, the DHCPv6 Relay Agent is transparent. Figure-2 shows the DHCPv6 Relay typical configuration topology.

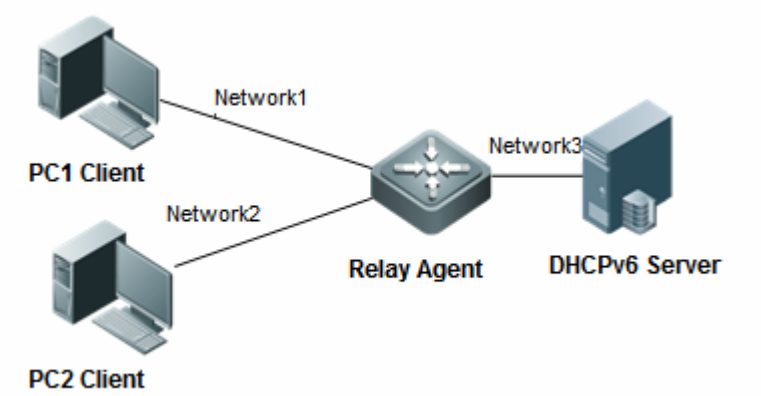


Figure-2 Typical Configuration Topology of DHCPv6 Relay

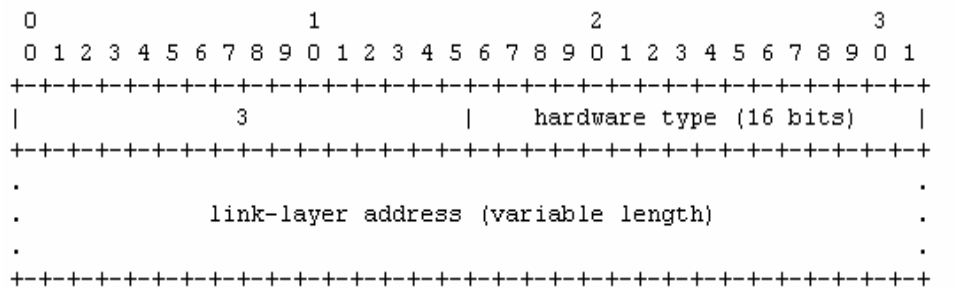
In the above configuration topology, both the PC1 and the PC2 in the Network1 and the Network2 can obtain the addresses allocated by the DHCPv6 Server in the Network3 through the Relay Agent.

9.1.3 Understanding DHCP Relay Agent

9.1.3.1 DUID

The RFC3315 defines the DUID(DHCP Unique Identifier) is the unique identifier to idetify the DHCPv6 device(including the Client, the Relay and the Server) in the network, used for the DHCPv6 device verification. DES-7200 product adopts the DUID-LL(DUID Based on Link-layer Address) specified in the RFC 3315 as the identification of the DHCPv6 device. The following explains the DUID-LL structure:

- DUID type: DUID-LL type value is 0x0003.
- Hardware type: the supported hardware type is Ethernet, 0x0001.
- Link layer address: the bridge MAC address for the device.



9.1.4 DHCPv6 Relay Agent Working Principle

The DHCPv6 Relay Agent encapsulates the DHCPv6 packets sent from the Client into the Relay-forward packets and then forwards those packets to the specified servers. Upon receiving the Relay-forward packets, the DHCPv6 server sends the Relay-reply packets. The DHCPv6 Relay Agent decapsulates the Relay-reply packets and forwards them to the Client.

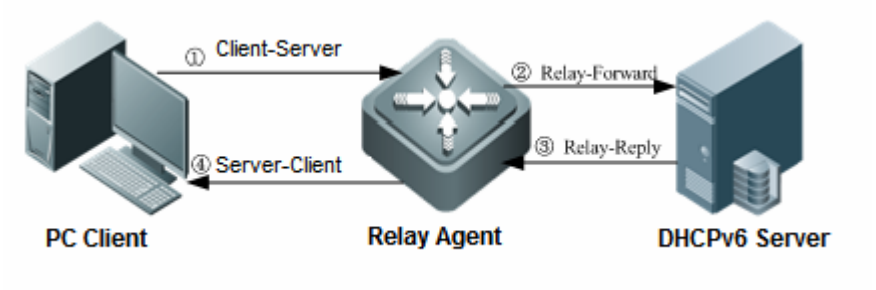


Figure-3 DHCPv6 Relay Working Process

The Figure-3 shows the detailed process that the DHCPv6 Client forwards the packet, obtains the IPv6 address and other configuration parameters through the DHCPv6 Relay Agent:

1. The DHCPv6 Client sends the DHCPv6 request packets to FF02::1:2, the multicast address for all DHCPv6 server and Relay Agent in the link;
2. After receiving the DHCPv6 request packets from the Client, the DHCPv6 Relay Agent encapsulates the packets in the Relay Message Option of the Relay-forward packet and sends the Relay-forward packet to the specified DHCPv6 server;
3. The DHCPv6 server resolutes the Client request from the Relay-forward packet, sets the IPv6 address and other parameters for the Client, encapsulates the reply packet into the Relay Message Option of the Relay-reply packet and sends the Relay-reply packet to the DHCPv6 Relay Agent;
4. The DHCPv6 Relay Agent resolutes the Relay-reply packet from the DHCPv6 Server and forwards them to the DHCPv6 Client;
5. The DHCPv6 Client configures the network according to the IPv6 address allocated by the DHCPv6 Server and other parameters;
6. The working process of the address lease/re-binding/release for the DHCPv6 Client and the refresh for the DHCPv6 Server is similar to the one of Relay Agent.

Note

According to the RFC3315, the address FF02::1:2 is the multicast address for all DHCPv6 Server and the Relay Agent in the link. That is to say, all DHCPv6 Server or Relay Agent in the link shall deal with the DHCPv6 request packets sent from that address.

9.1.5 Protocol and Standard

The related protocol and standard is:

RFC3315 Dynamic Host Configuration Protocol for IPv6 (DHCPv6)

9.2 Default Configuration

Function	Default value
DHCPv6 Relay Agent	Disabled

Function	Default value
DHCPv6 Relay Agen Server Address	Not specified.

9.3 Configuring DHCPv6 Relay Agent

By default, Relay Agent function is disabled. This section describes how to enable DHCPv6 Relay Agent function and configure the destination address for the specified interface.

- Configuring DHCPv6 Relay Agent Server Address
- Showing the configurations

9.3.1 Configuring the Destination Address for DHCP Relay Agent

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-type interface-name*	Enter the interface(layer-3) configuration mode.
DES-7200(config-if)# **ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*]	Specify the interface with the DHCPv6 Relay service enabled to forward the DHCPv6 packets received from the Client to the specified destination address.
DES-7200(config-if)# **end**	Exit from the interface configuration mode.

Use the **no ipv6 dhcp relay destination** *ipv6-address* [*interface-type interface-number*] command to delete the Relay Agent destination address.

For example:

The following example shows how to enable DHCPv6 Relay service on the interface VLAN 1:

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface vlan 1
```

```
DES-7200(config-if)#ipv6 dhcp relay destination 3001::2
DES-7200(config-if)#end
```

Caution

1. The IPv6 DHCP Relay Destination command can only be used on the layer-3 interface.
2. Up to 20 Relay Agent Destination addresses can be configured on one device.
3. If the Destination address is the multicast address, the interface name and number must be specified.

9.3.2 Showing the Destination Address for the DHCPv6 Relay Agent

Command	Function
DES-7200# **show ipv6 dhcp relay destination** { **all** | **interface** *interface-type interface-number* }	Show the IPv6 DHCP relay destination address list (for the specified interface).

The following shows the configuration:

```
DES-7200# show ipv6 dhcp relay destination all
Interface: Vlan1
Destination address(es)                    Output Interface
3001::2
FF02::1:2                                  Vlan2
```

9.4 Showing DHCPv6 Relay Agent Statistical Information

To make it convenient for the users to track the information of running the DHCPv6 Relay Agent function(for example, checking whether a large number of packet attack occurs or not), DES-7200 provides the function of showing DHCPv6 relay agent statistical information.

- Showing the statistical information
- Clearing the statistical information

9.4.1 Showing the statistical information

Command	Function
DES-7200# **show ipv6 dhcp relay statistics**	Show the related statistical information about the DHCPv6 Relay Agent packets.

The following example shows the DHCPv6 Relay Agent statistical information:

```
DES-7200# show ipv6 dhcp relay statistics
Packets dropped             :  2
   Error                   :  2
   Excess of rate limit     :  0
Packets received            :  28
   SOLICIT                 :  0
   REQUEST                 :  0
   CONFIRM                 :  0
   RENEW                   :  0
   REBIND                  :  0
   RELEASE                 :  0
   DECLINE                 :  0
   INFORMATION-REQUEST      :  14
   RELAY-FORWARD           :  0
   RELAY-REPLY             :  14
Packets sent                :  16
   ADVERTISE               :  0
   RECONFIGURE             :  0
   REPLY                   :  8
   RELAY-FORWARD           :  8
   RELAY-REPLY             :  0
```

9.4.2 Clearing the statistical information

Command	Function
DES-7200# **clear ipv6 dhcp relay statistics**	Clear the related statistical information about the DHCPv6 Relay Agent packets.

9.5 Typical Configuration Example of DHCPv6 Relay Agent

9.5.1 Network Requirements

Enable DHCPv6 Relay Agent on the Device1 and configure the destination address 3001::2;

Enable DHCPv6 Relay Agent on the Device2, configure the destination mulitcast address FF02::1:2 for all Server and Relay Agent, and specify the destination address for the outgoing L3 interface gi0/1.

9.5.2 Network Topology

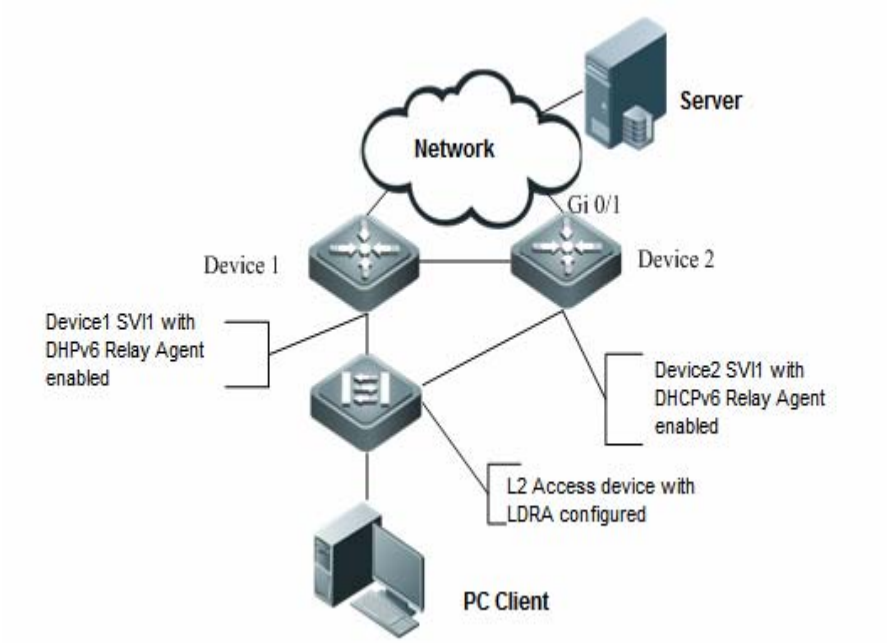


Figure-3 Network Topology for DHCPv6 Relay Agent

9.5.3 Configuration Tip

Enabling the DHCPv6 Relay Agent function for the PC gateway and configuring the destination address for the server or the next-hop Relay Agent device, preventing the Relay Agent from shouldering too much pressure by separately allocation.

9.5.4 Configuration Steps

1) Enable the DHCPv6 Relay Agent function on the Device1 and specify the destination address 3001::2:

```
DES-7200#config
Enter configuration commands, one per line.  End with CNTL/Z
DES-7200(config)#interface vlan 1
DES-7200(config-if)# ipv6 dhcp relay destination 3001::2
```

2) Enable the DHCPv6 Relay Agent function on the Device2 and specify the destination address FF02::1:2:

```
DES-7200#config
Enter configuration commands, one per line.  End with CNTL/Z
DES-7200(config)#interface vlan 1
DES-7200(config-if)#ipv6 dhcp relay destination FF02::1:2 interface gi
0/1
```

9.5.5 Showing Verification

1) Show the DHCPv6 Relay Agent configurations on the Device1:

```
DES-7200# show ipv6 dhcp relay destination all

Interface: Interface vlan 1
Server address(es)                        Output Interface
3001：：2
```

2) Show the DHCPv6 Relay Agent configurations on the Device2:

```
DES-7200# show ipv6 dhcp relay destination all

Interface: Interface vlan 1
Server address(es)                        Output Interface
FF02::1:2                                 gi0/1
```

10 DNS Configuration

10.1 DNS Overview

Each IP address may present a host name consisting of one or more strings separated by the decimal. Then, all you need to do is to remember the host name rather than IP address. This is the function of the DNS protocol.

There are two methods to map from the host name to the IP address: 1) Static Mapping: A device maintains its host name to IP address mapping table and uses it only by itself. 2) Dynamic Mapping: The host name to IP address mapping table is maintained on the DNS server. In order for a device to communicate with others by its host name, it needs to search its corresponding IP address on the DNS server.

The domain name resolution (or host name resolution) is the process that the device obtains IP address which corresponds to the host name by the host name. The DES-7200 switches support the host name resolution locally or by the DNS. During the resolution of domain name, you can firstly adopt the static method. If it fails, use the dynamic method instead. Some frequently used domain names can be put into the resolution list of static domain names. In this way, the efficiency of domain name resolution can be increased considerably.

10.2 Configuring Domain Name Resolution

10.2.1 Default DNS Configuration

The default configurations of DNS are as follows:

Attribute	Default value
Enable/disable the DNS resolution service	Enable
IP address of DNS server	None
Status Host List	None

Attribute	Default value
Maximum number of DNS servers	6

10.2.2 Enabling DNS Resolution Service

This section describes how to enable the DNS resolution service.

Command	Function
DES-7200(config)# **ip domain-lookup**	Enable DNS.

The command **no ip domain-lookup** is used to disable DNS.

```
DES-7200(config)# ip domain-lookup
```

10.2.3 Configuring the DNS Server

This section describes how to configure the DNS server. The dynamic domain name resolution can be carried out only when the DNS Server is configured.

The **no ip name-server** [*ip-address*] command can be used to remove the DNS server. Where, the **ip-address** parameter indicates the specified DNS server to be removed. If this parameter is omitted, all the DNS servers will be removed.

Command	Function
DES-7200(config)# **ip name-server** *ip-address*	Add the IP address of the DNS Server. The switch will add a DNS Server when this command is executed every time. If the domain name can't be obtained from the first DNS Server, the switch will send the DNS request to the subsequent several servers until the correct response is received. The system can support six DNS servers at most.

10.2.4 Configuring the Host Name to IP/IPv6 Address Mapping Statically

This section describes how to configure the host name to IP/IPv6 address mapping. The switch maintains a host name to IP/IPv6 address corresponding table, which is also referred to as the host name to IP/IPv6 address mapping

table. You can obtain the mapping table in two ways: manual configuration and dynamic learning.

Command	Function
DES-7200(config)# **ip host** *host-name ip-address*	Configure the host name to IP address mapping manually.
DES-7200(config)# **ipv6 host** *host-name ip-address*	Configure the host name to IPv6 address mapping manually.

This command with the parameter **no** can be used to remove the mapping between the host name and IP/IPv6 address.

10.2.5 Clearing the Dynamic Buffer Table of Host Names

This section describes how to clear the dynamic buffer table of host names. If the command **clear host** or **clear host** * is entered, the dynamic buffer table will be cleared. Otherwise, only the entries of specified domain names will be cleared.

Command	Function
DES-7200# **clear host** [*word*]	Clear the dynamic buffer table of host names. The host names configured statically will not be removed.

10.2.6 Showing Domain Name Resolution Information

This section describes how to display the DNS configuration.

Command	Function
DES-7200# **show hosts**	Show the DNS configuration.

```
DES-7200# show hosts
DNS name server   :
192.168.5.134   static
    host              type       address
www.163.com           static     192.168.5.243
www.DES-7200.com        dynamic    192.168.5.123
```

10.3 Typical DNS Configuration Examples

10.3.1 Example of Static DNS Configuration

10.3.1.1 Topological Diagram

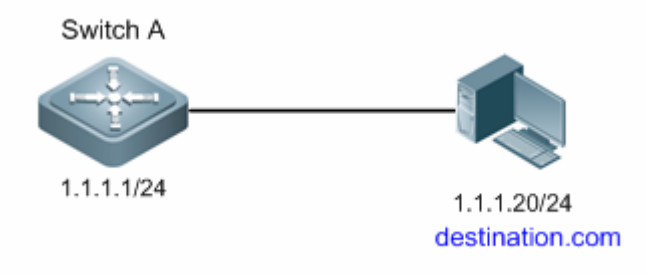


Figure1 Network topology for static DNS configuration

10.3.1.2 Application Requirements

Since Switch A will frequently access the host of destination.com, we can use static DNS to access the host of IP 1.1.1.20 through the domain name of destination.com, so as to enhance the efficiency of domain resolution.

10.3.1.3 Configuration Tips

1. Make sure the route between device and host is reachable.
2. The mapping between host name and IP address is correct.

10.3.1.4 Configuration Steps

Manually configure the mapping between host name and IP address. In this example, configure the host name to "destination.com" and the corresponding IP address to 1.1.1.20.

```
SwitchA(config)#ip host destination.com 1.1.1.20
```

10.3.1.5 Verifications

Step 1: View DNS information. Key point: the mapping between host and IP address shall be correct.

```
SwitchA#show host
Name servers are:
Host            type    Address                  TTL(sec)
```

```
destination.com    static  1.1.1.20                ---
```

Step 2: Execute "ping destination.com" command to verify the result.

```
SwitchA#ping destination.com
Translating "destination.com"...[OK]
Sending 5, 100-byte ICMP Echoes to 1.1.1.20, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

From the above information, we can learn that Switch A has successfully accessed the host with IP address being 1.1.1.20 through the host name of destination.com by means of static DNS.

10.3.2 Example of Dynamic DNS Configuration

10.3.2.1 Topological Diagram

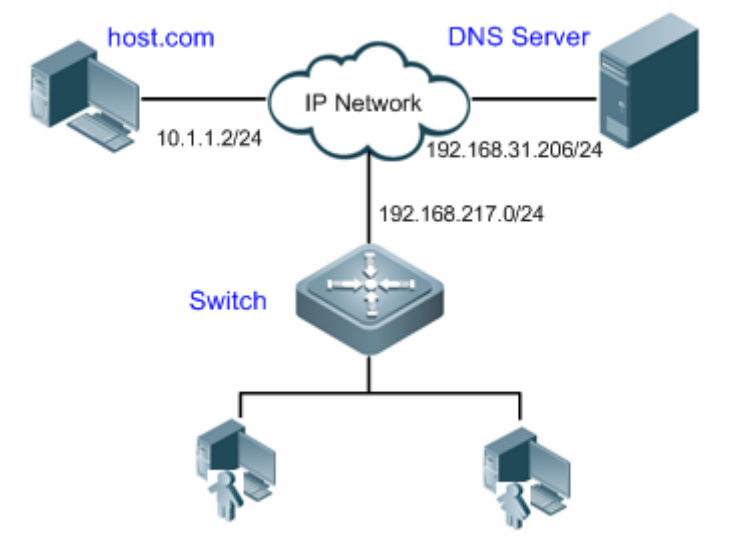


Figure2 Network topology for dynamic DNS configuration

10.3.2.2 Application Requirements

1. The IP address of DNS server is 192.168.31.206/24.
2. The switch is the DNS client and can access the host of 10.1.1.2 through the host name of host.com by means of dynamic DNS.

10.3.2.3 Configuration Tips

1. The route between DNS client, DNS server and access PC shall be reachable.
2. DNS shall be enabled. The DNS feature is enabled by default.
3. The IP address of DNS server has been correctly configured.

10.3.2.4 Configuration Steps

Step 1: Configure DNS server

Different DNS servers need to be configured differently. Please configure DNS server according to the actual conditions.

Configure the mapping between host and IP address on DNS server. In this example, configure host name as "host.com" and IP address as 10.1.1.2/24.

Step 2: Configure DNS client

The route between DNS client, DNS server and access PC shall be reachable. The interface IP configurations are shown in the topological diagram.

! DNS shall be enabled. The DNS feature is enabled by default.

```
DES-7200(config)#ip domain-lookup
```

! Configure the IP address of DNS server as 192.168.31.206

```
DES-7200(config)#ip name-server 192.168.31.206
```

10.3.2.5 Verifications

Step 1: Execute "ping host.com" command to verify the result.

```
DES-7200#ping host.com

Translating " host.com "...[OK]
Sending 5, 100-byte ICMP Echoes to 10.1.1.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

From the above information, we can learn that the client device can ping the host, and the corresponding destination IP is 10.1.1.2. Through dynamic DNS, the host with IP address being 10.1.1.2 can be accessed through the host name of host.com.

Step 2: View DNS information. Key point: the host name and IP address.

```
DES-7200#show host
```

```
Name servers are:
192.168.31.206 static

Host                type      Address          TTL(sec)
host.com            dynamic   10.1.1.2          3503
```

From the above information, we can learn that the mapping between host name and host IP is correct.

11 FTP Server Configuration

11.1 Overview

You can set a device as the FTP server. Then you can connect to the FTP server through a FTP client and upload or download documents through the FTP protocol.

FTP server enables you to get documents from devices like Syslog file. You can also copy documents to the file system of devices directly.

11.1.1 FTP Commands Supported

Upon receiving a FTP connection request, the FTP server requires the FTP client offer login user name and password for authentication.

The FTP client can run commands only when it passes authentication. Not all FTP client commands are supported at present. The following table shows the FTP client commands supported:

ascii	delete	mdelete	mput	quit	send
bin	dir	mdir	nlist	recv	size
bye	disconnection	mget	open	rename	system
cd	get	mkdir	passive	rhelp	type
cdup	image	mls	put	rmdir	user
close	ls	modtime	pwd	rstatus	

For the method to use above mentioned FTP client commands, refer to FTP client software document. In addition, many FTP client tools, for instance, CuteFTP and FlashFXP have graphic operation interface. Users no longer need to use FTP commands.

11.2 Configure the FTP Server

11.2.1 Enable or Disable the FTP Server

By default, the FTP Server is disabled. To enable the FTP server, run the **ftp-server enable** command in the global configuration mode. It should be noted that the FTP client cannot access the FTP server before you configure the top directory, login user name and password of the FTP server. So it is recommended to refer to the later sections to configure the top directory, login user name and password before enabling the FTP Server for the first time.

To disable the FTP server, run the **no ftp-server enable** command in the global configuration mode.

Command	Function
DES-7200(config)# **ftp-server enable**	Enable the FTP Server.
DES-7200(config)# **no ftp-server enable**	Disable the FTP Server.

Caution

In real network, only one client is allowed to access the FTP server at a time.

11.2.2 Configure the Top Directory

The function limits the range that the FTP client can access. (For the details on how to view and manage the directories on the device, refer to *File System Configuration Guide*.) For instance, you can set the top directory to the "/syslog" directory. After logging in the FTP Server, the FTP client can access only the files and folders under the "/syslog" directory.

To configure the top directory, run the **ftp-server topdir** command in the global configuration mode. The **no** form of this command removes the top directory configuration and prohibits the FTP client to access any files on the FTP server.

Command	Function

DES-7200(config)# **ftp-server topdir** *directory*	Configures the top directory of the FTP Server.
DES-7200(config)# **no ftp-server topdir**	Removes the top directory configuration and prohibits the FTP client to access any files on the FTP server.

Assume that log files are stored under the "/syslog" directory. To download log files from a device through the FTP client on the management PC while prohibiting the FTP client from accessing the files other than the "/syslog" directory, configure the top directory as below:

```
DES-7200(config)# ftp-server topdir /syslog
```

After configuration, the FTP client can only access the files and sub directories under the "/syslog" directory. Given the limit of the top directory, the FTP client cannot back to the parent directory of the "/syslog" directory.

11.2.3 Configure Session Idle Time Out

The FTP Server does not support parallel connections. When a user logs in to the FTP Server, the FTP Server may maintain this connection in case of abnormal abortion. Consequently, the FTP Server occupies this connection for a long period of time and cannot respond the login requests of other users.

Session idle timeout can be used to solve this problem. When the FTP Server does not interact with one user within a specific period of time, the FTP Server considers that the connection is not available and automatically disconnects the connection. The session idle timeout is 30 minutes by default.

To configure session idle timeout, run the **ftp-server timeout** command in the global configuration mode.

Command	Function
DES-7200(config)# **ftp-server timeout** *time*	Sets the session idle timeout. time: idle timeout in the range of 1-3600 minutes
DES-7200(config)# **no ftp-server timeout**	Restores the idle timeout to the default value (30 minutes)

The following example sets the session idle timeout to 5 minutes:

```
DES-7200(config)# ftp-server timeout 5
```

If the FTP client has not executed any operation within five minutes, the FTP Server automatically disconnects the connection and then begins to respond other connection requests.

Caution

The session idle timeout refers to the time period between two operations in a FTP session. The FTP Server starts to calculate the session idle time from 0 after completing a command (for instance, transferring a file) and stops calculation before executing a new command. Consequently, this configuration will not influence some time-consuming file transmission.

11.2.4 Configure Login User Name and Password

The FTP Server uses login user name and password to authentication clients. By default, the login user name and password are null.

Anonymous user and null password are not supported on the FTP Server. To configure valid login user name and password in the global configuration mode, run the **ftp-server username** and **ftp-server password** commands in the global configuration mode. Only one user name and password can be configured on the FTP Server.

Command	Function
DES-7200(config)# **ftp-server username** *username*	Sets user name.
DES-7200(config)# **no ftp-server username**	Removes the user name configuration.
DES-7200(config)# **ftp-server password** [*type*] *password*	Sets a password.
DES-7200(config)# **no ftp-server password**	Removes the password configuration.

A user name consists of up to 64 characters, including English letter, half-width numeral and half-width symbol, not blank space.

A password consists of letters or numerals. Blank space is allowed behind and in front of the password, but it will be ignored. The length of a password in plain text mode ranges from 1 to 25 characters and a password in cipher text mode ranges from 4 to 52 characters.

The following example sets the user name to “admin” and password to ”letmein”.

```
DES-7200(config)# ftp-server username admin
DES-7200(config)# ftp-server password letmein
```

11.2.5 View Status and Debugging Information

To view status and debugging information, run the **show ftp-server** and **debug ftpserver** command in the privileged EXEC configuration mode.

Command	Function
DES-7200# **show ftp-server**	Shows the status of the FTP Server.
DES-7200# **debug ftpserver**	Turns on the debugging of the FTP Server.
DES-7200# **no debug ftpserver**	Turns off the debugging of the FTP Server.

The following example shows the status information of the FTP Server:

```
DES-7200# show ftp-server
ftp-server information
=====================================
enable : Y
topdir : /
timeout: 20min
username config : Y
password config : Y
type: BINARY
control connect : Y
ftp-server: ip=192.167.201.245  port=21
ftp-client: ip=192.167.201.82  port=4978
port data connect : Y
ftp-server: ip=192.167.201.245  port=22
ftp-client: ip=192.167.201.82  port=4982
passive data connect : N
```

The following example turns on the debugging of the FTP Server:

```
DES-7200# debug ftpserver
FTPSRV_DEBUG:(RECV)  SYST
FTPSRV_DEBUG:(REPLY)  215 DNOS Type: L8
FTPSRV_DEBUG:(RECV)  PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY)  200 PORT Command okay.
```

The following example turns off the debugging of the FTP Server:

```
DES-7200# no debug ftpserver
```

11.3 Typical FTP Server configuration Example

11.3.1 Networking Requirements

The logs of a device (Switch A in the following figure) are stored in the directory of "/syslog". By configuring the FTP Server, the following requirements must be met:

- The client can login FTP server with username of "admin" and password of "DES-7200".
- After successful login, the FTP client on the management PC can directly download logs from the device, but the FTP client is not allowed to access files in directories other than "/syslog".
- If the current client carries out no operation within 5 minutes, the FTP server will be disconnected automatically. After disconnection, the FTP server can respond to the new access requests.

11.3.2 Network Topology

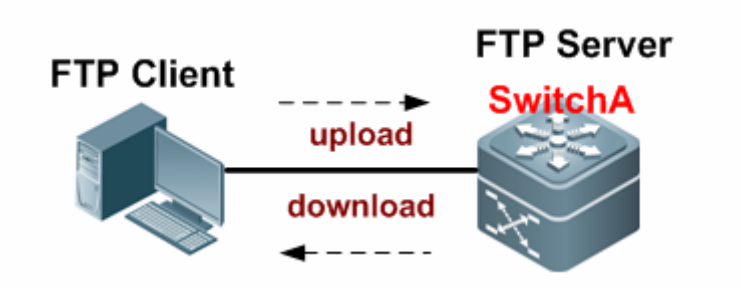


Diagram for typical AAA application

11.3.3 Configuration Tips

To meet the above requirements, execute the following steps:

1. Configure the username and password for server login as "admin" and "DES-7200" respectively;
2. Configure session timeout timer as 5 minutes;
3. Configure the top directory of server as "/syslog";
4. Enable FTP server;

11.3.4 Configuration Steps

Configure SwitchA as the FTP Server

Step 1: Configure the username and password for server login as "admin" and "DES-7200" respectively

```
DES-7200#configure

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)#ftp-server username admin

DES-7200(config)#ftp-server password DES-7200
```

Step 2: Configure session timeout timer as 5 minutes

```
DES-7200(config)#ftp-server timeout 5
```

Step 3: Configure the top directory of server as "/syslog";

```
DES-7200(config)#ftp-server topdir /syslog
```

Step 4: Enable FTP server

```
DES-7200(config)#ftp-server enable
```

11.3.5 Verification

Step 1: Display the relevant state of FTP server:

```
DES-7200(config)#show ftp-server

   ftp-server information

==================================

enable : Y

topdir : /syslog

timeout: 5min

username config : Y

password config : Y

transfer type: ASCII

control connection : N

port data connection : N

passive data connection : N
```

Step 2: Debug the FTP server

```
DES-7200# debug ftpserver
FTPSRV_DEBUG:(RECV)   SYST
FTPSRV_DEBUG:(REPLY)  215 DNOS Type: L8
FTPSRV_DEBUG:(RECV)   PORT 192,167,201,82,7,120
FTPSRV_DEBUG:(REPLY)  200 PORT Command okay.
```

DES-7200

Network Management Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 SNMP Configuration

1.1 SNMP Overview

1.1.1 Introduction

As the abbreviation of Simple Network Management Protocol, SNMP has been a network management standard (RFC1157) since the August, 1988. So far, the SNMP becomes the actual network management standard for the support from many manufacturers. It is applicable to the situation of interconnecting multiple systems from different manufacturers. Administrators can use the SNMP protocol to query information, configure network, locate failure and plan capacity for the nodes on the network. Network supervision and administration are the basic function of the SNMP protocol.

As a protocol in the application layer, the SNMP protocol works in the client/server mode, including three parts as follows:

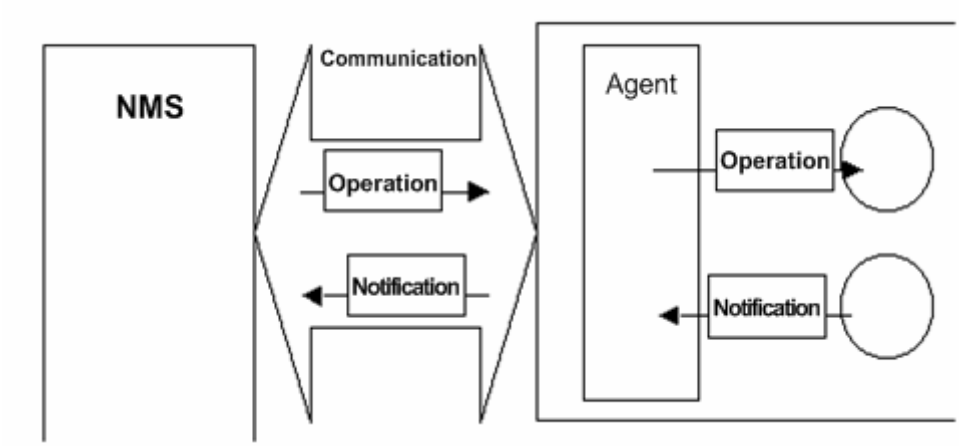
- SNMP network manager
- SNMP agent
- MIB (management information base)

The SNMP network manager, also referred to as NMS (Network Management System), is a system to control and monitor the network using the SNMP protocol. HP OpenView, CiscoView and CiscoWorks 2000 are the typical network management platforms running on the NMS. DES-7200 has developed a suit of software (Star View) for network management against its own network devices. These typical network management software are convenient to monitor and manage network devices.

The SNMP Agent is the software running on the managed devices. It receives, processes and responds the monitoring and controlling messages from the NMS, and also sends some messages to the NMS.

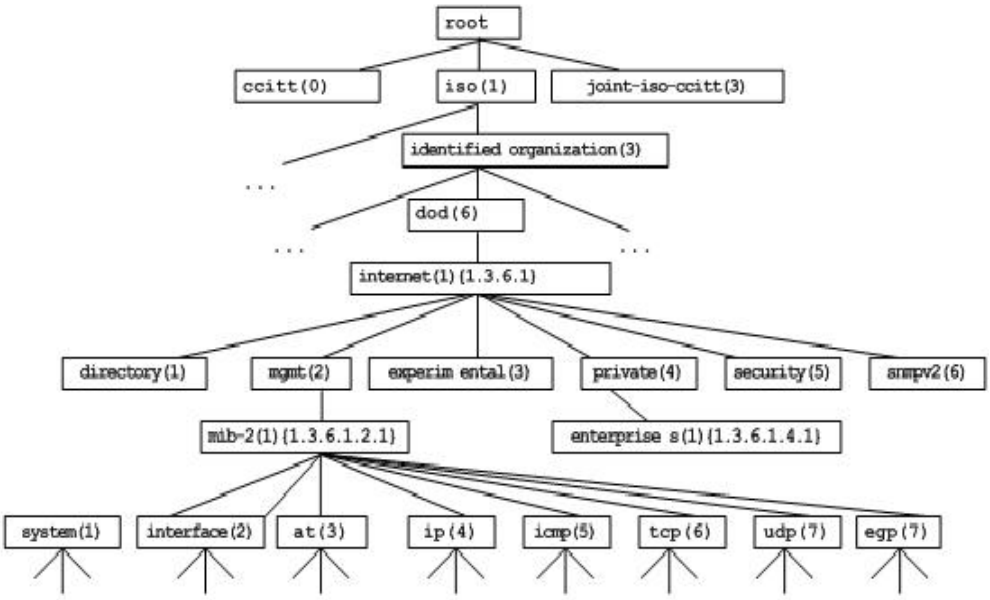
The relationship between the NMS and the SNMP Agent can be indicated as follows:

Relationship between the NMS and the SNMP Agent



The MIB (Management Information Base) is a virtual information base for network management. There are large volumes of information for the managed network equipment. In order to uniquely identify a specific management unit in the SNMP message, the tree-type hierarchy is used to by the MIB to describe the management units in the network management equipment. The node in the tree indicates a specific management unit. Take the following figure of MIB as an example to name the objectives in the tree. To identify a specific management unit system in the network equipment uniquely, a series of numbers can be used. For instance, the number string {1.3.6.1.2.1.1} is the object identifier of management unit, so the MIB is the set of object identifiers in the network equipment.

Tree-type MIB hierarchy



1.1.2 SNMP Versions

This software supports these SNMP versions:

- SNMPv1: The first formal version of the Simple Network Management Protocol, which is defined in RFC1157.
- SNMPv2C: Community-based Administrative Framework for SNMPv2, an experimental Internet protocol defined in RFC1901.
- SNMPv3: Offers the following security features by authenticating and encrypting packets:
  1. Ensure that the data are not tampered during transmission.
  2. Ensure that the data come from a valid data source.
  3. Encrypt packets to ensure the data confidentiality.

Both the SNMPv1 and SNMPv2C use a community-based security framework. They restrict administrator's operations on the MIB by defining the host IP addresses and community string.

With the GetBulk retrieval mechanism, SNMPv2C sends more detailed error information type to the management station. GetBulk allows you to obtain all the information or a great volume of data from the table at a time, and thus reducing the times of request and response. Moverover, SNMPv2C improves the capability of handing errors, including expanding error codes to distinguish different kinds of errors, which are represented by one error code in SNMPv1. Now, error types can be distinguished by error codes. Since there may be the management workstations supporting SNMPv1 and SNMPv2C in a network, the SNMP agent must be able to recognize both SNMPv1 and SNMPv2C messages, and return the corresponding version of messages.

1.1.3 SNMP Management Operations

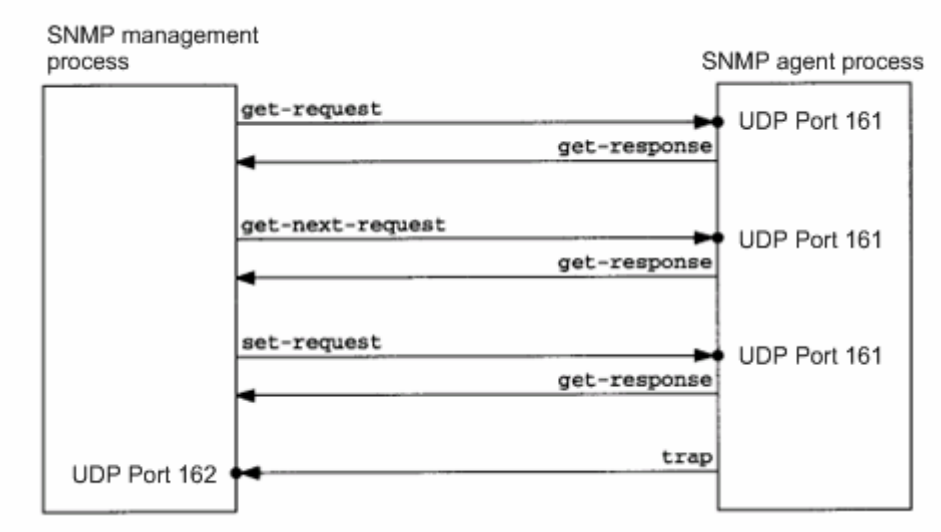
For the information exchange between the NMS and the SNMP Agent, six types of operations are defined:

1. Get-request: The NMS gets one or more parameter values from the SNMP Agent.
2. Get-next-request: The NMS gets the next parameter value of one or more parameters from the SNMP Agent.
3. Get-bulk: The NMS gets a bulk of parameter values from the SNMP Agent.
4. Set-request: The NMS sets one or more parameter values for the SNMP Agent.
5. Get-response: The SNMP Agent returns one or more parameter values, the response of the SNMP Agent to any of the above 3 operations of the NMS.

6. Trap: The SNMP Agent proactively sends messages to notify the NMS that some event will occur.

The first four messages are sent from the NMS to the SNMP Agent, and the last two messages are sent from the SNMP Agent to the NMS (Note: SNMPv1 does not support the Get-bulk operation). These operations are described in the following figure:

Message types in SNMP



NMS sends messages to the SNMP Agent in the first three operations and the SNMP Agent responds a message through the UDP port 161. However, the SNMP Agent sends a message in the Trap operation through the UDP port 162.

1.1.4 SNMP Security

Both SNMPv1 and SNMPv2 use the community string to check whether the management workstation is entitled to use MIB objects. In order to manage devices, the community string of NMS must be identical to a community string defined in the devices.

A community string Features:

- Read-only: Authorized management workstations are entitled to read all the variables in the MIB.
- Read-write: Authorized management workstations are entitled to read and write all the variables in the MIB.

Based on SNMPv2, SNMPv3 can determine a security mechanism for processing data by security model and security level. There are three types of security models: SNMPv1, SNMPv2C and SNMPv3.

The table below describes the supported security models and security levels.

Model	Level	Authentication	Encryption	Description

Model	Level	Authentication	Encryption	Description
SNMPv1	noAuthNoPriv	Community string	None	Ensures the data validity through community string.
SNMPv2c	noAuthNoPriv	Community string	None	Ensures the data validity through community string.
SNMPv3	noAuthNoPriv	User name	None	Ensures the data validity through user name.
SNMPv3	authNoPriv	MD5 or SHA	None	Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism.
SNMPv3	authPriv	MD5 or SHA	DES	Provides HMAC-MD5 or HMAC-SHA-based authentication mechanism and CBC-DES-based encryption mechanism.

1.1.5 SNMP Engine ID

The engine ID is designed to identify a SNMP engine uniquely. Every SNMP entity contains a SNMP engine, a SNMP engine ID identifies a SNMP entity in a management domain. So every SNMPV3 entity has a unique identifier named SNMP Engine ID.

The SNMP Engine ID is an octet string of 5 to 32 bytes, which is defined in RFC3411:

- The first four bytes indicate the private enterprise number of an enterprise (assigned by IANA) in hex system.
- The fifth byte indicates how to identify the rest bytes.

0: Reserved

1: The following 4 bytes indicate an IPv4 address.

2: The following 16 bytes indicate an IPv6 address.

3: The following 6 bytes indicate an MAC address

4: Texts of up to 27 bytes defined by manufacturers

5: A hexadecimal value of up to 27 bytes defined by manufacturers

6-127: Reserved

128-255: In the format specified by manufacturers.

1.2 SNMP Configuration

To configure SNMP, enter the global configuration mode.

1.2.1 Setting the Community String and Access Authority

SNMPv1 and SNMPv2C adopt community string-based security scheme. The SNMP Agent supports only the management operations from the management workstations of the same community string. The SNMP messages without matching the community string will be discarded. The community string serves as the password between the NMS and the SNMP Agent.

- Configure an ACL rule to allow the NMS of the specified IP address to manage devices.
- Set the community's operation right: ReadOnly or ReadWrite.
- Specify a view for view-based management. By default, no view is configured. That is, the management workstation is allowed to access to all MIB objects
- Indicate the IP address of the NMS who can use this community string. If it is not indicated, any NMS can use this community string. By default, any NMS can use this community string.

To configure the SNMP community string, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**host** *host-ip*] [**ipv6** *ipv6-aclname*][*aclnum* | *aclname*]	Set the community string and its right.

One or more coummnity strings can be specified for the NMS of different rights. To remove the community name and its right, run the **no snmp-server community** command in the global configuration mode.

1.2.2 Configuring MIB Views and Groups

With view-based access control model, you can determine whether the object of a management operation is in a view or not. For access control, generally some users are associated with a group and then the group is associated with a view. The users in a group have the same access right.

- Set an inclusion view and an exclusion view.
- Set a Read-only view and a Read-write view for a group.
- Set security levels, whether to authenticate, and whether to encrypt for SNMPv3 users.

To configure the MIB views and groups, run the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **snmp-server view** *view-name oid-tree* {**include | exclude**}	Create a MIB view to include or exclude associated MIB objects.
DES-7200(config)# **snmp-server group** *groupname* {**v1** | **v2c** |**v3** {**auth** | **noauth** | **priv**}} [**read** *readview*] [**write** *writeview*] [**access** {[**ipv6** *ipv6_aclname*] [*aclnum* | *aclname*] }]	Create a group and associate it with the view.

You can delete a view by using the **no snmp-server view** *view-name* command, or delete a tree from the view by using the **no snmp-server view** *view-name oid-tree* command. You can also delete a group by using the **no snmp-server group** *groupname* command.

1.2.3 Configuring SNMP Users

User-based security model can be used for security management. In this mode, you should configure user information first. The NMS can communicate with the SMP Agent by using a valid user account.

For SNMPv3 users, you can specify security level, authentication algorithm (MD5 or SHA), authentication password, encryption algorithm (only DES now) and encryption password.

To configure a SNMP user, run the following commands in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **snmp-server user** *username roupname* {**v1** | **v2** | **v3** [**encrypted**] [**auth** { **md5**|**sha** } *auth-password*] [**priv des56** *priv-password*] } [**access** {[**ipv6** *ipv6_aclname*] [*aclnum* | *aclname*] }]	Configure the user information.

To remove the specified user, execute the **no snmp-server user** *username groupname* command in the global configuration mode.

1.2.4 Configuring Host Address

In special cases, the SNMP Agent may also proactively send messages to the NMS.

To configure the NMS host address that the SNMP Agent proactively sends messages to, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **snmp-server host** {*host-addr* | **ipv6** *ipv6-addr* } [**vrf** *vrfname*] [**traps**] [**version** {**1|2c |3 [auth | noauth | priv**]}] *community-string* [udp-port *port-num*] [***type***]	Set the SNMP host address, vtf, community string, message type (or security level in SNMPv3).

1.2.5 Configuring SNMP Agent Parameters

You can configure the basic parameters of the SNMP Agent, including contact, device location and sequence number. With these parameters, the NMS knows the contact, location and other information of the device.

To configure the SNMP agent parameters, run the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **snmp-server contact** *text*	Configure the contact.
DES-7200(config)# **snmp-server location** *text*	Configure the location.
DES-7200(config)# **snmp-server chassis-id** *number*	Configure the sequence number.

1.2.6 Defining the Maximum Message Size of the SNMP Agent

In order to enhance network performance, you can configure the maximum packet size of the SNMP Agent. To configure the maximum packet size of the SNMP Agent, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **snmp-server packetsize** *byte-count*	Set the maximum packet size of the SNMP Agent.

1.2.7 Shielding the SNMP Agent

The SNMP Agent service is a service provided by DES-7200product and enabled by default. When you do not need it, you can shield the SNMP agent service and related configuration by executing the following command in the global configuration mode:

Command	Function
DES-7200(config)# **no snmp-server**	Shield the SNMP agent service.

1.2.8 Disabling the SNMP Agent

DES-7200 products provide a different command from the shield command to disable the SNMP Agent. This command will act on all of the SNMP services instead of shielding the configuration information of the SNMP Agent. To disable the SNMP agent service, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **no enable service snmp-agent**	Disable the SNMP agent service.

1.2.9 Configuring the SNMP Agent to Send the Trap Message to the NMS Initiatively

The TRAP message is a message automatically sent by the SNMP Agent to the NMS unsolicitedly, and is used to report some critical and important events. By default the SNMP Agent is not allowed to send the TRAP message. To enable it, run the following command in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **snmp-server enable traps** [*type*] [*option*]	Allow the SNMP Agent to send the TRAP message proactively.
DES-7200(config)# **no snmp-server enable traps** [*type*] [*option*]	Forbid the SNMP Agent to send the TRAP message proactively.

1.2.10 Configuring LinkTrap Policy

You can configure whether to send the LinkTrap message of an interface. When this function is enabled and the link status of the interface changes, the SNMP will send the LinkTrap message. Otherwise, it will not. By default, this function is enabled.

Command	Function
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# [**no] snmp trap** link-status	Enable or disable sending the LinkTrap message of the interface.

The following configures not to send LinkTrap message on the intereface:

```
DES-7200(config)# interface gigabitEthernet 1/1
DES-7200(config-if)#no snmp trap link-status
```

1.2.11 Configuring the Parameters for Sending the Trap Message

To set the parameters for the SNMP Agent to send the Trap message, execute the following commands:

Command	Function
DES-7200(config)# **snmp-server trap-source** *interface*	Specify the source port sending the Trap message.
DES-7200(config)# **snmp-server queue-length** *length*	Specify the queue length of each Trap message.
DES-7200(config)# **snmp-server trap-timeout** *seconds*	Specify the interval of sending Trap message.

1.3 SNMP Monitoring and Maintenance

1.3.1 Checking the Current SNMP Status

To monitor the SNMP status and troubleshoot SNMP configurations, DES-7200 product provides monitoring commands for SNMP, with which it is possible to easily check the SNMP status of the current network device. In the privileged mode, execute **show snmp** to check the current SNMP status.

```
DES-7200# show snmp
Chassis: 1234567890 0987654321
Contact: wugb@i-net.com.cn
Location: fuzhou
2381 SNMP packets input
   5 Bad SNMP version errors
   6 Unknown community name
   0 Illegal operation for community name supplied
   0 Encoding errors
   9325 Number of requested variables
   0 Number of altered variables
   31 Get-request PDUs
   2339 Get-next PDUs
   0 Set-request PDUs
2406 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   4 No such name errors
   0 Bad values errors
   0 General errors
   2370 Get-response PDUs
   36 SNMP trap PDUs
SNMP global trap: disabled
SNMP logging: enabled
SNMP agent: enabled
```

The above statistics is explained as follows:

Showing Information	Description
Bad SNMP version errors	SNMP version is incorrect.
Unknown community name	The community name is not known.
Illegal operation for community name supplied	Illegal operation
Encoding errors	Code error
Get-request PDUs	Get-request message
Get-next PDUs	Get-next message
Set-request PDUs	Set-request message

Showing Information	Description
Too big errors (Maximum packet size 1500)	Too large response message
No such name errors	Not in the specified management unit
Bad values errors	Specified value type error
General errors	General error
Get-response PDUs	Get-response message
SNMP trap PDUs	SNMP trap message

1.3.2 Checking the MIB Objects Supported by the Current SNMP Agent

To check the MIB objects supported by the current SNMP Agent, run the **show snmp mib** command in the privileged mode:

```
DES-7200# show snmp mib
sysDescr
sysObjectID
sysUpTime
sysContact
sysName
sysLocation
sysServices
sysORLastChange
snmpInPkts
snmpOutPkts
snmpInBadVersions
snmpInBadCommunityNames
snmpInBadCommunityUses
snmpInASNParseErrs
snmpInTooBigs
snmpInNoSuchNames
snmpInBadValues
snmpInReadOnlys
snmpInGenErrs
snmpInTotalReqVars
snmpInTotalSetVars
snmpInGetRequests
snmpInGetNexts
snmpInSetRequests
snmpInGetResponses
snmpInTraps
snmpOutTooBigs
snmpOutNoSuchNames
snmpOutBadValues
snmpOutGenErrs
```

```
snmpOutGetRequests
snmpOutGetNexts
snmpOutSetRequests
snmpOutGetResponses
snmpOutTraps
snmpEnableAuthenTraps
snmpSilentDrops
snmpProxyDrops
entPhysicalEntry
entPhysicalEntry.entPhysicalIndex
entPhysicalEntry.entPhysicalDescr
entPhysicalEntry.entPhysicalVendorType
entPhysicalEntry.entPhysicalContainedIn
entPhysicalEntry.entPhysicalClass
entPhysicalEntry.entPhysicalParentRelPos
entPhysicalEntry.entPhysicalName
entPhysicalEntry.entPhysicalHardwareRev
entPhysicalEntry.entPhysicalFirmwareRev
entPhysicalEntry.entPhysicalSoftwareRev
entPhysicalEntry.entPhysicalSerialNum
entPhysicalEntry.entPhysicalMfgName
entPhysicalEntry.entPhysicalModelName
entPhysicalEntry.entPhysicalAlias
entPhysicalEntry.entPhysicalAssetID
entPhysicalEntry.entPhysicalIsFRU
entPhysicalContainsEntry
entPhysicalContainsEntry.entPhysicalChildIndex
entLastChangeTime
```

1.3.3 Viewing SNMP Users

To view the SNMP users configured on the current SNMP agent, run the **show snmp user** command in the privileged mode:

```
DES-7200# show snmp user
User name: test
Engine ID: 8000131103000000000000
storage-type: permanent    active
Security level: auth priv
Auth protocol: SHA
Priv protocol: DES
Group-name: g1
```

1.3.4 Viewing SNMP Views and Groups

To view the group configured on the current SNMP agent, run the **show snmp group** command in the privileged mode:

```
DES-7200# show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
```

```
readview: default
writeview: default
notifyview:

groupname: public
securityModel: v1
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:

groupname: public
securityModel: v2c
securityLevel:noAuthNoPriv
readview: default
writeview: default
notifyview:
```

To view the view configured on the current SNMP agent, run the **show snmp view** command in the privileged mode:

```
DES-7200# show snmp view
default(include) 1.3.6.1
test-view(include) 1.3.6.1.2.1
```

1.3.5 Viewing Host Information

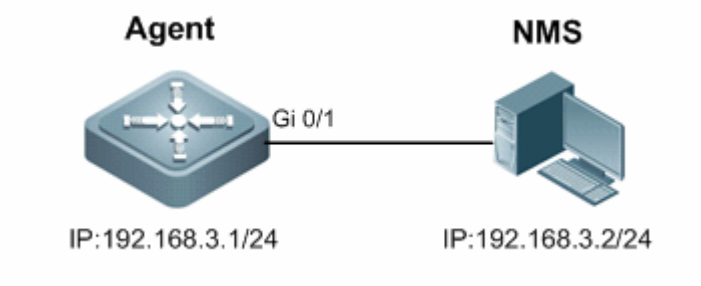
To view the host information configured on the SNMP agent, run the **show snmp host** command in the privileged mode:

```
DES-7200# show snmp host
Notification host: 192.168.64.221
udp-port: 162   type: trap
user: public    security model: v1
Notification host: 2000:1234::64
udp-port: 162   type: trap
user: public    security model: v1
```

1.4 Typical SNMP Configuration Example

1.4.1 SNMP v1/v2 Configuration Example

1.4.1.1 Topological Diagram



Topology for SNMP v1/2 application

1.4.1.2 Application Requirements

The Network Management Station (NMS) manages the network device (Agent) by applying the community-based authentication model, and the network device can control the operation permission (read or write) of the community to access the specified MIB objects. For example, community "user1" can only read and write objects under System (1.3.6.1.2.1.1) node.

The network device can only be managed by NMS with a specific IP (i.e., 192.168.3.2/24).

The network device can actively send messages to NMS.

The NMS can acquire the basic system information of the device, such as contact, location, ID and etc.

1.4.1.3 Configuration Tips

By creating MIB view and associating authentication name (Community) and access permission (Read or Write), the first application need can be met.

While configuring the authentication name and access permission, associate ACL or specify the IP of administrator using this authentication name to meet the second application need (this example associates the ACL).

Configure the address of SNMP host and enable the Agent to actively send Traps.

Configure the parameters of SNMP proxy.

1.4.1.4 Configuration Steps

Step 1: Configure MIB view and ACL.

! Create a MID view named "v1", which contains the associated MIB object (1.3.6.1.2.1.1).

```
DES-7200(config)#snmp-server view v1 1.3.6.1.2.1.1 include
```

! Create an ACL named "a1" to permit the IP address of 192.168.3.2/24.

```
DES-7200(config)#ip access-list standard a1
DES-7200(config-std-nacl)#permit host 192.168.3.2
DES-7200(config-std-nacl)#exit
```

Step 2: Configure authentication name and access permission.

! Configure Community of "user1", associate read and write permission for MIB view of "v1", and associate the ACL of "a1".

```
DES-7200(config)#snmp-server community user1 view v1 rw a1
```

Step 3: Configure the Agent to actively send messages to NMS.

! Configure the address of SNMP host to 192.168.3.2, message format to Version 2c and authentication name to "user1".

```
DES-7200(config)#snmp-server host 192.168.3.2 traps version 2c user1
```

! Enable the Agent to actively send traps.

```
DES-7200(config)#snmp-server enable traps
```

Step 4: Configure parameters of SNMP proxy.

! Configure system location.

```
DES-7200(config)#snmp-server location fuzhou
```

! Configure system contact.

```
DES-7200(config)#snmp-server contact DES-7200.com.cn
```

! Configure system ID.

```
DES-7200(config)#snmp-server chassis-id 1234567890
```

Step 5: Configure the IP address of Agent.

! Configure the IP address of interface VLAN 1 as 192.168.3.1/24.

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.3.1 255.255.255.0
DES-7200(config-if-VLAN 1)#exit
```

1.4.1.5 Verification

Step 1: Display configurations of the device.

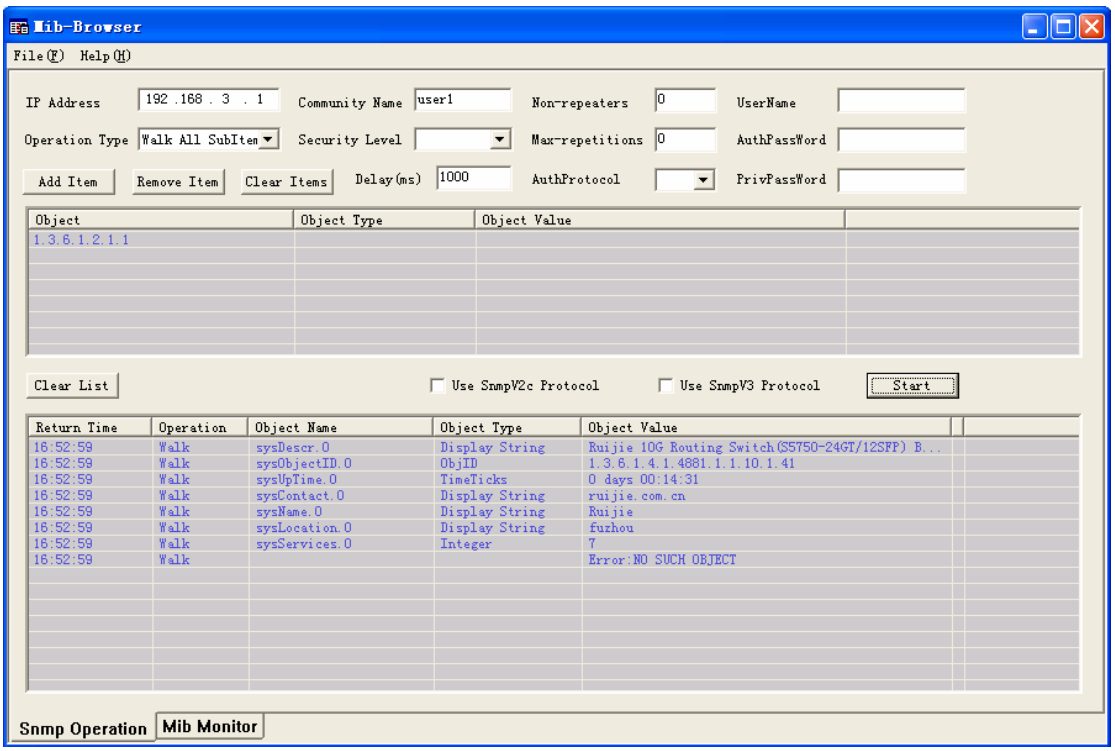
```
DES-7200#show running-config
!
ip access-list standard a1
 10 permit host 192.168.3.2
!
interface VLAN 1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
```

```
!
snmp-server view v1 1.3.6.1.2.1.1 include
snmp-server location fuzhou
snmp-server host 192.168.3.2 traps version 2c user1
snmp-server enable traps
snmp-server contact DES-7200.com.cn
snmp-server community user1 view v1 rw a1
snmp-server chassis-id 1234567890
```

Step 2: Display information about SNMP view and group.

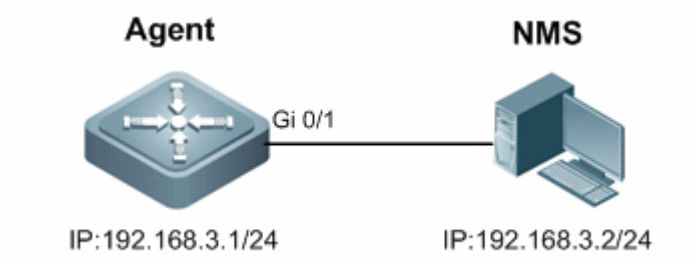
```
DES-7200#show snmp view
v1(include) 1.3.6.1.2.1.1                //define MIB object of “v1”
default(include) 1.3.6.1                 //default MIB object
DES-7200#show snmp group
groupname: user1                   //Configure Community as SNMP group
securityModel: v1
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
groupname: user1
securityModel: v2c
securityLevel:noAuthNoPriv
readview: v1
writeview: v1
notifyview:
```

Step 3: Install MIB-Browser. Type in device IP of "192.168.3.1" in the field of IP Address; type in "user1" in the field of Community Name; click "Add Item" button and select the specific management unit for querying MIB, such as the System shown below. Click Start button to implement MIB query of network device. The query result is shown in the bottommost box:



1.4.2 SNMP v3 Configuration Example

1.4.2.1 Topological Diagram



SNMPv3 application topology

1.4.2.2 Application Requirements

Network Management Station manages the network device (Agent) by applying user-based security model. For example: the user name is "user1", authentication mode is MD5, authentication key is "123", encryption algorithm is DES56, and the encryption key is "321".

The network device can control user's permission to access MIB objects. For example: "User1" can read the MIB objects under System (1.3.6.1.2.1.1) node, and can only write MIB objects under SysContact (1.3.6.1.2.1.1.4.0) node.

The network device can actively send authentication and encryption messages to the network management station.

1.4.2.3 Configuration Tips

Create MIB view and specify the included or excluded MIB objects.

Create SNMP group and configure the version to "v3"; specify the security level of this group, and configure the read-write permission of the view corresponding to this group.

Create user name and associate the corresponding SNMP group name in order to further configure the user's permission to access MIB objects; meanwhile, configure the version number to "v3" and the corresponding authentication mode, authentication key, encryption algorithm and encryption key.

Configure the address of SNMP host, configure the version number to "3" and configure the security level to be adopted.

1.4.2.4 Configuration Steps

Step 1: Configure MIB view and group.

! Create a MIB view of "view1" and include the MIB object of 1.3.6.1.2.1.1; further create a MIB view of "view2" and include the MIB object of 1.3.6.1.2.1.1.4.0.

```
DES-7200(config)#snmp-server view view1 1.3.6.1.2.1.1 include
DES-7200(config)#snmp-server view view2 1.3.6.1.2.1.1.4.0 include
```

! Create a group named "g1" and select the version number of "v3"; configure security level to "priv" to read "view1" and write "view2".

```
DES-7200(config)#snmp-server group g1 v3 priv read view1 write view2
```

Step 2: Configure SNMP user.

! Create a user named "user1", which belongs to group "g1"; select version number of "v3" and configure authentication mode to "md5", authentication key to "123", encryption mode to "DES56" and encryption key to "321".

```
DES-7200(config)#snmp-server user user1 g1 v3 auth md5 123 priv des56 321
```

Step 3: Configure the address of SNMP host.

! Configure the host address as 192.168.3.2 and select version number of "3"; configure security level to "priv" and associate the corresponding user name of "user1".

```
DES-7200(config)#snmp-server host 192.168.3.2 traps version 3 priv user1
```

! Enable the Agent to actively send traps to NMS.

```
DES-7200(config)#snmp-server enable traps
```

Step 4: Configure the IP address of Agent.

! Configure the IP address of interface VLAN 1 as 192.168.3.1/24.

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.3.1 255.255.255.0
DES-7200(config-if-VLAN 1)#exit
```

1.4.2.5 Verification

Step 1: Display configurations of device.

```
DES-7200#show running-config
!
interface VLAN 1
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
!
snmp-server view view1 1.3.6.1.2.1.1 include
snmp-server view view2 1.3.6.1.2.1.1.4.0 include
snmp-server user user1 g1 v3 encrypted auth md5
7EBD6A1287D3548E4E52CF8349CBC93D priv des56
D5CEC4884360373ABBF30AB170E42D03
snmp-server group g1 v3 priv read view1 write view2
snmp-server host 192.168.3.2 traps version 3 priv user1
snmp-server enable traps
```

Step 2: Display SNMP user.

```
DES-7200#show snmp user
User name: user1
Engine ID: 800013110300d0f8221120
storage-type: permanent    active
Security level: auth priv
Auth protocol: MD5
Priv protocol: DES
Group-name: g1
```

Step 3: Display SNMP view.

```
DES-7200#show snmp view
view1(include) 1.3.6.1.2.1.1
view2(include) 1.3.6.1.2.1.1.4.0
default(include) 1.3.6.1
```

Step 4: Display SNMP group.

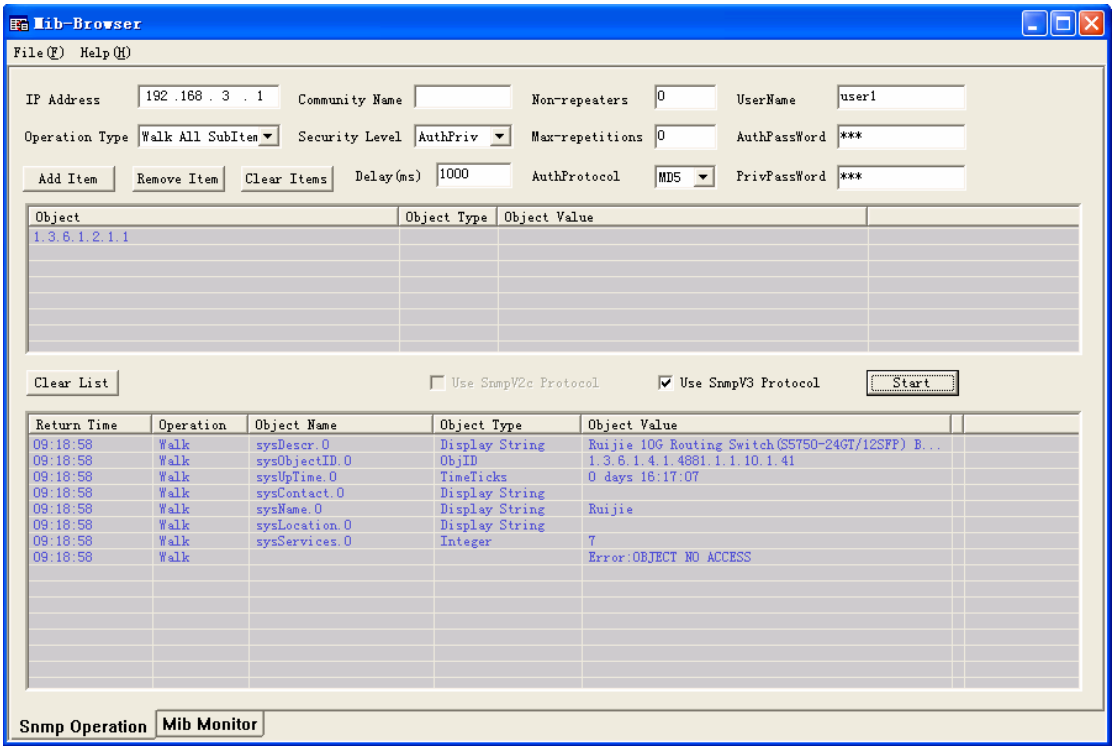
```
DES-7200#show snmp group
groupname: g1
securityModel: v3
securityLevel:authPriv
```

```
readview: view1
writeview: view2
notifyview:
```

Step 5: Display host information configured by the user.

```
DES-7200#show snmp host
Notification host: 192.168.3.2
udp-port: 162
type: trap
user: user1
security model: v3 authPriv
```

Step 6: Install MIB-Browser. Type in device IP of "192.168.3.1" in the field of IP Address; type in "user1" in the field of UserName; select "AuthPriv" from Security Level; type in "123" in the field of AuthPassWord; select "MD5" from AuthProtocol; type in "321" in the field of PrivPassWord. Click "Add Item" button and select the specific management unit for querying MIB, such as the System shown below. Click Start button to implement MIB query of network device. The query result is shown in the bottommost box:



2 RMON Configuration

2.1 Overview

RMON (Remote Monitoring) is a standard monitoring specification of IETF (Internet Engineering Task Force). It can be used to exchange the network monitoring data among various network monitors and console systems. In the RMON, detectors can be placed on the network nodes, and the NMS determines which information is reported by these detectors, for example, the monitored statistics and the time buckets for collecting history. The network device such as the switch or router acts as a node on the network. The information of current node can be monitored by means of the RMON.

There are three stages in the development of RMON. The first stage is the remote monitoring of Ethernet. The second stage introduces the token ring which is referred to as the token ring remote monitoring module. The third stage is known as RMON2, which develops the RMON to a high level of protocol monitor.

The first stage of RMON (known as RMON1) contains nine groups. All of them are optional (not mandatory), but some groups should be supported by the other groups.

The switch implements the contents of Group 1, 2 , 3 and 9: the statistics, history, alarm and event.

2.1.1 Statistics

Statistics is the first group in RMON. It measures the basic statistics information of each monitored subnet. At present, only the Ethernet interfaces of network devices can be monitored and measured. This group contains a statistics of Ethernet, including the discarded packets, broadcast packets, CRC errors, size block, conflicts and etc.

2.1.2 History

History is the second group in RMON. It collects the network statistics information regularly and keeps them for processing later. This group contains two subgroups:

The subgroup History Control is used to set such control information as sampling interval and sampling data source.

The subgroup Ethernet History provides history data about the network section traffic, error messages, broadcast packets, utilization, number of collision and other statistics for the administrator.

2.1.3 Alarm

Alarm is the third group in RMON. It monitors a specific management information base (MIB) object at the specified interval. When the value of this MIB object is higher than the predefined upper limit or lower than the predefined lower limit, an alarm will be triggered. The alarm is handled as an event by means of recording the log or sending the SNMP Trap message.

2.1.4 Event

Event is the ninth group in RMON. It determines to generate a log entry or a SNMP Trap message when an event is generated due to alarms.

2.2 RMON Configuration Task List

2.2.1 Configuring Statistics

One of these commands can be used to add a statistic entry.

Command	Function
DES-7200(config-if)# **rmon collection stats** *index* [**owner** *ownername*]	Add a statistic entry.
DES-7200(config-if)# **no rmon collection stats** *index*	Remove a statistic entry.

Caution The current version of DES-7200 product supports only the statistics of Ethernet interface. The index value should be an integer between 1 to 65535. At present, at most 100 statistic entries can be configured at the same time.

2.2.2 Configuring History

One of these commands can be used to add a history entry.

Command	Function
DES-7200(config-if)# **rmon collection history** *index* [**owner** *ownername*] [**buckets** *bucket-number*] [**interval** *seconds*]	Add a history entry.
DES-7200(config-if)# **no rmon collection history** ***i****ndex*	Remove a history entry.

Caution The current version of DES-7200 product supports only the records of Ethernet. The index value should be within 1 to 65535. At most 10 history entries can be configured.

Bucket-number: Specifies the used data source and time interval. Each sampling interval should be sampled once. The sampling results are saved. The Bucket-number specifies the maximum number of sampling. When the maximum is reached for the sampling records, the new one will overwrite the earliest one. The value range of Bucket-number is 1 to 65535. Its default value is 10.

Interval: Sampling interva in the range of 1 to 3600 seconds, 1800 seconds by default.

2.2.3 Configuring Alarm and Event

One of these command can be used to configure the alarm:

Command	Function
DES-7200(config)# **rmon alarm** *number variable interval* {**absolute	delta**} **rising-threshold** *value* [*event-number*] **falling-threshold** *value* [*event-number*] [**owner** *ownername*]	Add an alarm entry.
DES-7200(config)# **rmon event** *number* **[log] [trap** *community*] [**description** description-string]	Add an event entry.
DES-7200(config)# **no rmon alarm** *number*	Remove an alarm.
DES-7200(config)# **no rmon event** *number*	Remove an event.

number: Alarm index in the range of 1 to 65535.

variable: Variable to be monitored by the alarm(in integer).

interval: Sampling interval in the range of 1 to 4294967295.

Absolute: each sampling value compared with the upper and lower limits.

Delta: the difference with previous sampling value compared with the upper and lower limits.

value: Upper and lower limits.

Event-number: when the value exceeds the upper or lower limit, the event with the index of Event-number will be triggered.

Log: Record the event.

Trap: Send the Trap message to the NMS when the event is triggered.

Community: Community string used for sending the SNMP Trap message.

Description-string: Description of the event.

2.2.4 Showing RMON status

Command	Function
DES-7200(config)# **show rmon alarms**	Show alarms.
DES-7200(config)# **show rmon events**	Show events.
DES-7200(config)# **show rmon history**	Show history.
DES-7200(config)# **show rmon statistics**	Show statistics.

2.3 RMON Configuration Examples

2.3.1 Example of Configuring Statistics

If you want to get the statistics of Ethernet Port 3 , use the following commands:

```
DES-7200(config)# interface gigabitEthernet 0/3
DES-7200(config-if)# rmon collection stats 1 owner aaa1
```

2.3.2 Example of Configuring History

Use the following commands if you want to get the statistics of Ethernet Port 3 every 10 minutes:

```
DES-7200(config)# interface gigabitEthernet 0/3
DES-7200(config-if)# rmon collection history 1 owner aaa1 interval 600
```

2.3.3 Example of Configuring Alarm and Event

If you want to configure the alarm function for a statistical MIB variable, the following example shows you how to set the alarm function to the instance ifInNUcastPkts.6 (number of non-unicast frames received on port 6; the ID of the instance is 1.3.6.1.2.1.2.2.1.12.6) in ***IfEntry*** table of MIB-II. The specific function is as follows: the switch checks the changes to the number of non-unicast frames received on port 6 every 30 seconds. If 20 or more than 20 non-unicast frames are added after last check (30 seconds earlier), or only 10 or less than 10 are added, the alarm will be triggered, and event 1 is triggered to do corresponding operations (record it into the log and send the Trap with "community" name as "rmon"). The "description" of the event is "ifInNUcastPkts is too much"). The "owner" of the alarm and the event entry is "aaa1".

```
DES-7200(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.12.6 30 delta
rising-threshold 20 1 falling-threshold 10 1 owner aaa1
DES-7200(config)#rmon event 1 log trap rmon description "ifInNUcastPkts is
too much " owner aaa1
```

2.3.4 Example of Showing RMON Status

2.3.4.1 show rmon alarm

```
DES-7200# show rmon alarms
Alarm : 1
Interval : 1
Variable : 1.3.6.1.2.1.4.2.0
Sample type : absolute
Last value : 64
Startup alarm : 3
Rising threshold : 10
Falling threshold : 22
Rising event : 0
Falling event : 0
Owner : aaa1
```

2.3.4.2 show rmon event

```
DES-7200# show rmon events
Event : 1
Description : firstevent
```

```
Event type : log-and-trap
Community : public
Last time sent : 0d:0h:0m:0s
Owner : aaa1
Log : 1
Log time : 0d:0h:37m:47s
Log description : ipttl
Log : 2
Log time : 0d:0h:38m:56s
Log description : ipttl
```

2.3.4.3 show rmon history

```
DES-7200# show rmon history
Entry : 1
Data source : Gi1/1
Buckets requested : 65535
Buckets granted : 10
Interval : 1
Owner : aaa1
Sample : 198
Interval start : 0d:0h:15m:0s
DropEvents : 0
Octets : 67988
Pkts : 726
BroadcastPkts : 502
MulticastPkts : 189
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 0
Fragments : 0
Jabbers : 0
Collisions : 0
Utilization : 0
```

2.3.4.4 show rmon statistics

```
DES-7200#  show rmon statistics
Statistics : 1
Data source : Gi1/1
DropEvents : 0
Octets : 1884085
Pkts : 3096
BroadcastPkts : 161
MulticastPkts : 97
CRCAlignErrors : 0
UndersizePkts : 0
OversizePkts : 1200
Fragments : 0
Jabbers : 0
Collisions : 0
Pkts64Octets : 128
Pkts65to127Octets : 336
```

```
Pkts128to255Octets : 229
Pkts256to511Octets : 3
Pkts512to1023Octets : 0
Pkts1024to1518Octets : 1200
Owner : Zhangsan
```

3 NTP Configuration

3.1 Understanding NTP

Network Time Protocol (NTP) is designed for time synchronization on network devices. A device can synchronize its clock source and the server. Moreover, the NTP protocol can provide precise time correction (less than one millisecond on the LAN and dozens of milliseconds on the WAN, compared with the standard time) and prevent from attacks by means of encryption and confirmation.

To provide precise time, NTP needs precise time source, the Coordinated Universal Time (UTC). The NTP may obtain UTC from the atom clock, observatory, satellite or Internet. Thus, accurate and reliable time source is available.

To prevent the time server from malicious destroying, an authentication mechanism is used by the NTP to check whether the request of time correction really comes from the declared server, and check the path of returning data. This mechanism provides protection of anti-interference.

DES-7200 switches support the NTP client and server. That is, the switch can not only synchronize the time of server, but also be the time server to synchronize the time of other switches. But when the switch works as the time server, it only support the unicast server mode.

3.2 Configuring NTP

This chapter describes how to configure the NTP client and server.

- Configuring the global NTP authentication mechanism.
- Configuring the global NTP authentication key.
- Configuring the global NTP trusted key ID.
- Configuring the NTP server.
- Disabling the interface to receive the NTP message.
- Enabling or disabling NTP.
- Configuring the NTP real-time synchronization
- Configuring the NTP update-calendar
- Configuring the NTP master

- Configuring the access control privilege of the NTP service

3.2.1 Configuring the Global NTP Authentication Mechanism

The NTP client of DES-7200 supports encrypted communication with the NTP server by means of key encryption.

There are two steps to configure the NTP client to communicate with the NTP server by means of encryption:

Step 1, Authenticate the NTP client and configure the key globally;

Step 2, Configure the trusted key for the NTP server.

To initiate the encrypted communication with the NTP server, you need to set authentication key for the NTP server in addition to perfomring Step 1.

By default, the NTP client does not use the global security authentication mechanism. Without this mechanism, the communication will not be encrypted. However, enabling the global security authentication does not mean that the encryption is used to implement the communication between the NTP server and the NTP client. You need to configure other keys globally and an encryption key for the NTP server.

To configure the global security authentication mechanism, run the following commands in the global configuration mode:

Command	Function
ntp authenticate	Configure the global NTP security authentication mechanism.
no ntp authenticate	Disable the global NTP security authentication mechanism.

The message is verified by the trusted key specified by the **ntp authentication-key** or **ntp trusted-key** command.

3.2.2 Configuring the Global NTP Authentication Key

The next step to configure the global security authentication for the NTP is to set the global authentication key.

Each key is identified by a unique key-id globally. The customer can use the command **ntp trusted-key** to set the key corresponding to the key-id as a global trusted key.

To specify a global authentication key, run the following commands in the global configuration mode:

Command	Function
ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Specify a global authentication key. *key-id*: in the range of 1 to 4294967295 *key-string*: Any *enc-type*: Two types: 0 and 7
no ntp authentication-key *key-id* **md5** *key-string* [*enc-type*]	Remove a global authentication key.

The configuration of global authentication key does not mean the key is effective; therefore, the key must be configured as a global trusted key before using it.

Caution The current NTP version can support up to 1024 authentication keys and only one key can be set for each server for secure communication.

3.2.3 Configure the Global NTP Trusted key ID

The last step is to set a global authentication key as a global trusted key. Only by this trusted key the user can send encrypted data and check the validity of the message.

To specify a global trusted key, run the following commands in the global configuration mode:

Command	Function
ntp trusted-key *key-id*	Specify a global trusted key ID.
no ntp trusted-key *key-id*	Remove a global trusted key ID.

The above-mentioned three steps of settings are the first procedure to implement security authentication mechanism. To initiate real encrypted communication between the NTP client and the NTP server, a trusted key must be set for the corresponding server.

Caution When a global authentication key is removed, its all trusted information are removed.

3.2.4 Configuring the NTP Server

No NTP server is configured by default. DES-7200's client system supports simultaneous interaction with up to 20 NTP servers, and one authentication key can be set for each server to initiate encrypted communication with the NTP server after relevant settings of global authentication and key are completed.

NTP version 3 is the default version of communication with the NTP server. Meanwhile, the source interface can be configured to send the NTP message, and the NTP message from the relevant server can only be received on the sending interface.

To configure the NTP server, run the following commands in the global configuration mode:

Command	Function
ntp server *ip-addr* [**version** *version*][**source** *if-name number*][***key*** *keyid*][**prefer**]	Configure the NTP server. *version* (NTP version number): 1 to 3 *if-name* (interface type): Aggregateport, Dialer GigabitEthernet, Loopback, Multilink, Null, Tunnel, Virtual-ppp, Virtual-template and VLAN *keyid*: 1 to 4294967295
no ntp server *ip-addr*	Remove the NTP server.

Only when the global security authentication and key setting mechanisms are completed, and the trusted key for communicating with server is set, can the NTP client initiate the encrypted communication with the NTP server. To this end, the NTP server should have the same trusted key configured.

3.2.5 Disabling the Interface to Receiving the NTP Message

The function of this command is to disable the interface to receive the NTP message.

By default, the NTP messages received on any interface are available to the NTP client for clock synchronization. This function can shield the NTP messages received on the relevant interface.

Caution

This command takes effect only for the interface whose IP address can be configured to receive and send packets.

To disable the interface to receive the NTP message, run the following commands in the interface configuration model:

Command	Function
interface *interface-type number*	Enter the interface configuration mode.
ntp disable	Disable the function of receiving NTP messages on the interface.

To enable the function of receiving NTP messages on the interface, use the command **no ntp disable** in the interface configuration mode.

3.2.6 Enabling or Disabling NTP

The **no ntp** command is to disable the NTP synchronization service, stop the time synchronization, and clear relevant information of NTP configuration.

The NTP function is disabled by default, but may be enabled as long as the NTP server is configured.

To disable the NTP, run the following commands in the global configuration mode:

Command	Function
no ntp	Disable the NTP function.
ntp authenticate or **ntp server** *ip-addr* [**version** *version*][**source** *if-name number*][***key*** *keyid*][***prefer***]	Enable the NTP function.

3.2.7 Configuring the NTP Real-time Synchronization

To configure the NTP real-time synchronization, run the following commands in the global configuration mode:

Command	Function
ntp synchronization	Enable the NTP real-time synchronization.
no ntp synchronization	Disable the NTP real-time synchronization.

During the synchronization, the **no ntp** command and the **no ntp synchronization** command both can stop or disable the time synchronization.

The difference of those two commands is that the **no ntp** command not only disables the NTP function, but also clears the related NTP settings.

3.2.8 Configuring the NTP Update-Calendar

The function of this command is to disable the interface to receive the NTP message.

To configure the NTP update-calendar, run the following commands in the global configuration model:

Command	Function
ntp update-calendar	Configure the update calendar.
no ntp update-calendar	Disable the function of NTP update calendar.

By default, the NTP update-calendar is not configured. After configuration, the NTP client updates the calendar at the same time when the time synchronization of external time source is successful. It is recommended to enable this function for keeping the accurate calendar.

3.2.9 Configuring the NTP Master

The function of this command is to set the local time as the NTP master(the reference source of the local time is reliable), providing the synchronized time for other devices.

In general, the local system synchronizes the time from the external time source directly or indirectly. However, if the time synchronization of local system fails for the network connection trouble, ect, use the command to set the reliable reference source of the local time, providing the synchronized time for other devices.

Once set, the system time can not be synchronized to the time source with higher starum.

Note

The starum indicates the level of current clock, reference indicates the address of the server used for synchronization, freq indicates the clock frequency of current system, precision indicates the precision of current system clock, reference time indicates the UTC time of reference clock on the synchronization server, clock offset indicates the offset of current clock, root delay indicates the delay of current clock, root dispersion indicates the precision of top server, peer dispersion indicates the precision of synchronization server.

To configure the NTP master, run the following commands in the global configuration mode:

Command	Function
ntp master	Set the local time as the NTP master and specify the corresponding starum. The time starum ranges from 1-15, 8 by default.
no ntp master	Cancel the NTP master settings.

The following example shows how to set the reliable reference source of the local time and set the time starum as 12:

```
DES-7200(config)# ntp master 12
```

Caution

Using this command to set the local time as the master (in particular, specify a lower starum value), is likely to be covered by the effective clock source. If multiple devices in the same network use this command, the time synchronization instability may occur due to the time difference between the devices.

In addition, before using this command, if the system has never been synchronized with an external clock source, it is necessary to manually calibrate the system clock to prevent too much bias. (For how to how to manually calibrate the system clock, please refer to the section of system time configuration of "Basic switch management Configuration Guide")

This command is not restricted by ntp access control (even if the NTP access control function has corresponding matching limit, this command is still in force).

3.2.10 Configuring the Access Control Privilege of NTP Service

NTP services access control function provides a minimal security measures (more secure way is to use the NTP authentication mechanism). By default, no NTP access control rules are configured in the system.

To set the NTP services access control privilege, run the following command in the global configuration mode.

Command	Function
ntp access-group { peer | serve | serve-only | query-only } *access-list-number|access-list-name*	Set the access control privilege of the local service.
no ntp access-group { peer | serve | serve-only | query-only } *access-list-number|access-list-name*	Cancel the settings of access control privilege of the local service.

peer: not only allow the time requests and control queries for the local NTP service, but also allow the time synchronization between the local device and the remote system (full access privilege).

serve: only allow the time requests and control queries for the local NTP service, not allow the time synchronization between the local device and the remote system.

serve-only: only allow the time requests for the local NTP service.

query-only: only allow the control queries for the local NTP service.

access-list-number: IP access control list label; the range of 1 ~ 99 and 1300 ~ 1999. On how to create IP access control list, refer to the relevant description in "Access Control List Configuration Guide".

access-list-name: IP access control list name. On how to create IP access control list , refer to the the relevant description in "Access Control List Configuration Guide" .

When an access request arrives, NTP service matches the rules in accordance with the sequence from the smallest to the largest to access restriction, and the first matched rule shall prevail. The matching order is peer, serve, serve-only, query-only.

Caution

Control query function (the network management device controls the NTP server, such as setting the leap second mark or monitor the working state,ect) is not supported in the current system. Although it matches with the order in accordance with the above rules, the related requests about the control and query are not supported.

If you do not configure any access control rules, then all accesses are allowed. However, once the access control rules are configured, only the rule that allows access can be carried out.

The following example shows how to allow the peer device in acl1 to control the query, request for and synchronize the time with the local device; and limit the peer device in acl2 to request the time for the local device:

```
DES-7200(config)# ntp access-group peer 1

DES-7200(config)# ntp access-group serve-only 2
```

3.3 Showing NTP Information

3.3.1 NTP Debugging

If you want to debug the NTP function, this command may be used to output necessary debugging information for troubleshooting.

To debug the NTP function, run the following commands in the privilege mode:

Command	Function
debug ntp	Enable the debugging function.
no debug ntp	Disable the debugging function.

3.3.2 Showing NTP Information

Execute the **show ntp status** command in the privileged mode to show the current NTP information.

To display the NTP function, run the following command in the privileged mode:

Command	Function
show ntp status	Show the current NTP information.

Only when the relevant communication server is configured can this command be used to print the display information.

```
DES-7200# show ntp status
Clock is synchronized, stratum 9, reference is 192.168.217.100
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**18
reference time is AF3CF6AE.3BF8CB56 (20:55:10.000 UTC Mon Mar 1 1993)
clock offset is 32.97540 sec, root delay is 0.00000 sec
root dispersion is 0.00003 msec, peer dispersion is 0.00003 msec
```

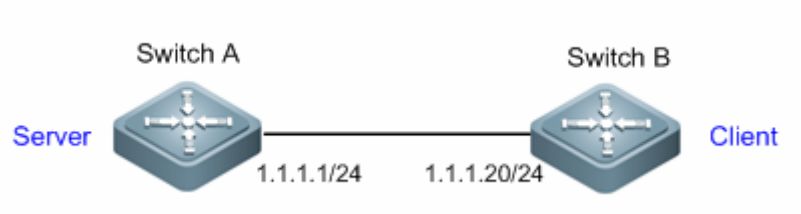
Note

The starum indicates the level of current clock, reference indicates the address of the server used for synchronization, freq indicates the clock frequency of current system, precision indicates the precision of current system clock, reference time indicates the UTC time of reference clock on the synchronization server, clock offset indicates the offset of current clock, root delay indicates the delay of current clock, root dispersion indicates the precision of top server, peer dispersion indicates the precision of synchronization server.

3.4 Typical NTP Configuration Examples

3.4.1 Configuring NTP client/server Mode

3.4.1.1 Topological Diagram



NTP client/server model

3.4.1.2 Application Requirements

1) On Switch A, configure local clock as the NTP master clock, with clock stratum being 12;

2) Configure Switch B as the NTP client and specify Switch A as the NTP server;

3) The hardware clock of Switch B shall be synchronized as well.

3.4.1.3 Configuration Tips

NTP server

Generally, the local system will directly or indirectly synchronize with the external clock sources. However, the local system may not be able to synchronize with the external clock sources due to the failure of network connections. In such a case, you can execute "ntp master" command to configure the local clock as NPT master clock to synchronize time to other devices.

NTP client

Configure the NTP server

By configuring NTP hardware clock update, NTP client can use the clock value synchronized from external clock sources to update its hardware clock, so that the hardware clock can also maintain precise.

3.4.1.4 Configuration Steps

Configuration of NTP server

! Configure NTP master clock. Configure local clock as the trusted reference clock source, with clock stratum being 12;

```
SwitchA(config)#ntp master 12
```

Configuration of NTP client

! Configure Switch A as the NTP server

```
SwitchB(config)#ntp server 1.1.1.1
```

! Configure NTP hardware clock update

```
SwitchB(config)# ntp update-calendar
```

3.4.1.5 Verify Configurations

Check the time before configuring NTP synchronization

! Check the time of reference clock source

```
SwitchA#show clock

17:12:48 UTC Tue, Sep 8, 2009
```

! Check the time of client before synchronization

```
SwitchB#show clock

12:01:10 UTC Sat, Jan 1, 2000
```

! Check the NTP status of client before synchronization

```
SwitchB(config)#show ntp status

Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**0

reference time is 0.0 (00:00:00.000 UTC Thu, Jan 1, 1970)
clock offset is 0.00000 sec, root delay is 0.00000 sec

root dispersion is 0.00000 msec, peer dispersion is 0.00000 msec
```

The above information shows that the time hasn't been synchronized yet;

After configuring NTP synchronization, display NTP configurations. Key points: NTP server address and stratum.

The following log will be printed on CLI interface:

```
*Sep  8 18:10:37: %SYS-6-CLOCKUPDATE: System clock has been updated to
18:10:37 UTC Tue Sep  8 2009.

SwitchB#show ntp status

Clock is synchronized, stratum 13, reference is 1.1.1.1
nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24

reference time is CE511CC9.37EB5B2D (18:11:21.000 UTC Tue, Sep 8, 2009)
clock offset is -0.00107 sec, root delay is 0.00000 sec

root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

The above information shows that the NTP client has connected to the server and the time of Switch B has been synchronized with the time of Switch A, with stratum level being higher than that of Switch A by 1 level (i.e., 13).

3.4.2 Configure NTP client/server Mode with authentication

3.4.2.1 Topological Diagram

NTP client/server model

3.4.2.2 Application Requirements

On Switch A, configure local clock as the NTP master clock, with clock stratum being 12;

Configure Switch B as the NTP client and specify Switch A as the NTP server;

Enable the authentication mechanism to prevent illegal users from maliciously attacking the clock server.

3.4.2.3 Configuration Tips

Configuring NTP server/client authentication will involve the following steps:

1) Enable NTP global authentication
2) Configure the key for NTP global authentication and the corresponding key ID
3) Specify NTP global trusted key ID
4) The authentication key used by NTP client to communicate with NTP server shall be identical with the corresponding Key ID.

3.4.2.4 Configuration Steps

Configuration of NTP server

Step 1: Configure NTP master clock. Configure local clock as the trusted reference clock source, with clock stratum being 12;

```
SwitchA(config)#ntp master 12
```

Step 2: Configure NTP authentication;

! Enable NTP global authentication

```
SwitchA(config)# ntp authenticate
```

! Configure NTP global authentication key as "helloworld" and the corresponding key ID as "6"

```
SwitchA(config)# ntp authentication-key 6 md5 helloworld
```

! Specify "6" as the NTP global trusted key ID

```
SwitchA(config)# ntp trusted-key 6
```

Configuration of NTP client

Step 1: Configure NTP authentication;

! Enable NTP global authentication

```
SwitchB(config)# ntp authenticate
```

! Configure NTP global authentication key as "helloworld" and the corresponding key ID as "6"

```
SwitchB(config)# ntp authentication-key 6 md5 helloworld
```

! Specify "6" as the NTP global trusted key ID

```
SwitchB(config)# ntp trusted-key 6
```

! Configure Switch A as the NTP server and set the key ID for communicating with this server as "6"

```
SwitchB(config)# ntp server 1.1.1.1 key 6
```

3.4.2.5 Verify Configurations

Display the configurations of NTP server. Key points: NTP master clock configuration, NTP server's IP address, and authentication related configurations.

```
SwitchA#show run

!

interface VLAN 1

 no ip proxy-arp

 ip address 1.1.1.1 255.255.255.0

!

ntp authentication-key 6 md5 07360623191d300a004609 7

ntp authenticate

ntp trusted-key 6

ntp master 12
```

!

Display the configurations of NTP client. Key points: IP address and key ID of NTP server, and authentication related configurations.

```
SwitchB #show run

!

interface VLAN 1

 no ip proxy-arp

 ip address 1.1.1.20 255.255.255.0
```

```
!

ntp authentication-key 6 md5 141a4f012d1d3c23174905 7

ntp authenticate

ntp trusted-key 6

ntp server 1.1.1.1 key 6

!
```

After proper configuration, the following log will be printed on the CLI interface:

```
*Sep  9 11:31:29: %SYS-6-CLOCKUPDATE: System clock has been updated to
11:31:29 UTC Wed Sep  9 2009.
```

The above log indicates that the clock of SwitchB (NTP client) has been updated.

Display NTP status of NTP server

```
SwitchA #show ntp status

Clock is synchronized, stratum 12, reference is 127.127.1.1

nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24

reference time is CE521261.E52DECA2 (11:39:13.000 UTC Wed, Sep 9, 2009)

clock offset is 0.00000 sec, root delay is 0.00000 sec

root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

Display NTP status of NTP client. Key points: NTP server address and stratum.

```
SwitchB#show ntp status

Clock is synchronized, stratum 13, reference is 1.1.1.1

nominal freq is 250.0000 Hz, actual freq is 250.0000 Hz, precision is 2**24

reference time is CE5212A1.E5D712A0 (11:40:17.000 UTC Wed, Sep 9, 2009)

clock offset is -0.00005 sec, root delay is 0.00000 sec

root dispersion is 0.00002 msec, peer dispersion is 0.00002 msec
```

The above information shows that the NTP client has successfully connected to the server and the time of Switch B has been synchronized with the time of Switch A, with stratum level being higher than that of Switch A by 1 level (i.e., 13).

4 SNTP Configuration

4.1 Overview

Network Time Protocol (NTP) is designed for time synchronization on network devices. Another protocol, Simple Network Time Protocol(SNMP) can be used to synchronize the network time, too.

NTP protocol can be used across various platforms and operating systems, and provide precise time calculation (1-50ms precision) and prevent from latency and jitter in the network. NTP also provides the authentication mechanism with high security level. However, NTP algorithm is complicated and demands better system.

As a simplified version of NTP, SNTP simplifies the algorithm of time calculation but also has great performance, with precision of about 1s.

SNTP Client is totally compatible with the NTP Server due to the consistency of the SNTP and NTP messages.

4.1.1 Understanding SNTP

SNTP works in the way of Client/Server. The standard Server system time is set by receiving the GPS signal or the atomic clock. The Client obtains its accurate time from the service time accessing the server regularly, and adjusts its system clock to synchronize the time.

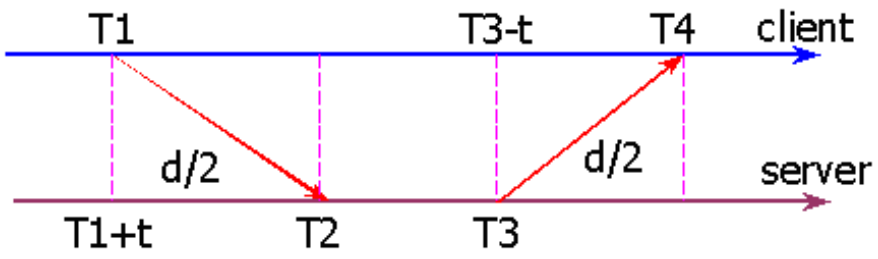


Figure-1

Originate Timestamp	T1	time request sent by client

Receive Timestamp	T2	time request received at server
Transmit Timestamp	T3	time reply sent by server
Destination Timestamp	T4	time reply received at client

T1: time request sent by client(refer to the client time) with the mark “Originate Timestamp”;

T2: time request received at server(refer to the server time) with the mark “Receive Timestamp”;

T3: time reply by server(refer to the server time) with the mark “Transmit Timestamp ”;

T4: time reply received at client(refer to the client time) with the mark “Destination Timestamp”.

T: time deviation between the Server and the Client

d: time between the Server and the Client

The following formula calculates the time:

∵ T2 = T1 + t + d / 2;

∴ T2 - T1 = t + d / 2;

∵ T4 = T3 – t + d / 2;

∴ T3 - T4 = t – d / 2;

∴ d = (T4 - T1) - (T3 - T2);

t = ((T2 - T1) + (T3 - T4)) / 2;

Then, according to the value of t and d, SNTP Client gets the current time: T4+t.

4.2 Configuring SNTP

This chapter describes how to configure the SNTP.

- Default configuration.
- Enabling SNTP.
- Configuring the IP address for the NTP server.
- Configuring the SNTP sync interval.
- Configuring the local time-zone.

4.2.1 Default Configuration

By default, the SNTP configurations are as follows:

Function	Default
SNTP state	Disabled.
IP address for the NTP server	0.
SNTP Sync Interval	1800s
Local Time-zone	GMT+8

4.2.2 Enabling SNTP

To enable the SNTP, run the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **sntp enable**	Enable the SNTP and synchronize the time once immediately. (in order to prevent frequent time synchronization, the sync-interval must not be less than 5s.)

To disable the SNTP, use the **no sntp enable** command.

4.2.3 Configuring the IP address for the NTP server

The SNTP Client is totally compatible with the NTP Server due to the inconsistency of SNTP and NTP messages. There are many NTP servers in the network, you can choose one switch with less latency as the NTP server.

For the detailed NTP server ip addresses, please logon to *http://www.time.edu.cn/* or *http://www.ntp.org/.* For example, 192.43.244.18(time.nist.gov).

To set the IP address for the SNTP server, run the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **sntp server** *ip-address*	Specify the IP address for the SNTP server.

4.2.4 Configuring the SNTP Sync Interval

To adjust the time regularly, you need to set the sync interval for SNTP Client to access the NTP server SNTP Client regularly.

To configure the SNTP sync interval, run the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **sntp interval** *seconds*	Configure the SNTP sync interval, in second. Interval range: 60-65535s; Default value: 1800s.

Caution

The sync interval configuration can not take effect immediately. You shall execute the **sntp enable** command immediately after configuring the SNTP sync interval.

4.2.5 Configuring the Local Time-zone

The time obtained through the SNTP communication is Greenwich Mean Time(GMT). In order to obtain the exact local time, you need to set the local time to adjust the mean time.

To configure the local time-zone, run the following commands in the interface configuration model:

Command	Function
DES-7200(config)#**clock time-zone** *time-zone*	Configure the time-zone, ranging from GMT-23 to GMT+23, wherein "-" indicates western area, "+" indicates eastern area and "0" indicates Greenwich mean time. The default time-zone is GMT+8, Beijing time.

To restore the local time-zone to the default, use the command **no clock time-zone**.

4.3 Showing SNTP Information

Execute the **show sntp** command in the privileged mode to show the current SNTP information.

```
DES-7200# show sntp

SNTP state              : ENABLE          //to view whether SNTP is enabled
  or not

SNTP server             : 192.168.4.12   //NTP Server

SNTP sync interval      : 60            //SNTP sync interval

Time zone             : +8              //Local Time-zone
```

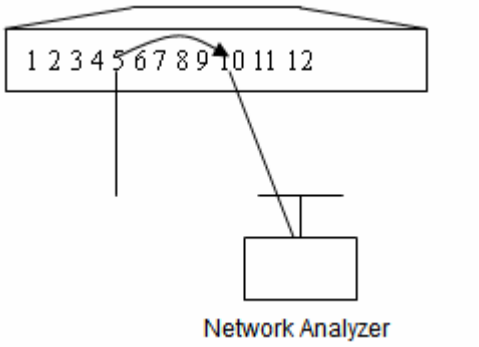
5 SPAN Configuration

5.1 Overview

With SPAN, you can analyze the communications between ports by copying a frame from one port to another port connected with a network analysis device or RMON analyzer. The SPAN mirrors all the packets sent/received at a port to a physical port for analysis.

For example, all the frames on the GigabitEhternet port 5 are mirrored to the GigabitEhternet port 10, as shown in Figure 18-1. Although the network analyzer connected to port 10 is not directly connected to port 5, it can receive all the frames from port 5.

Figure 1-1 SPAN Configuration Example



The SPAN allows you to monitor all the frames incoming/outgoing the source port, including the route input frames.

The SPAN does not affect the normal packet switching of the switch. Instead, it copies the frames incoming/outgoing the source port to the destination port. However, the frames may be discarded on an overflowed destination port, for example, when an 100Mbps port monitors an 1000Mbps port.

5.2 SPAN Concepts and Terms

This section describes the concepts and terms related to SPAN configuration.

5.2.1 SPAN Session

One SPAN session is the combination of one destination port and source port. You can monitor the received, transmitted, and bi-directional frames of one or multiple interfaces.

You can set up one or multiple SPAN sessions. Switched port and routed port can be configured with only one SPAN session. However, switched port, routed port, and AP can be configured as source port and destination port. The SPAN session does not affect the normal operation of the switch.

You can configure the SPAN session on one disabled port, but the SPAN does not take effect until you enable the destination and source ports. The **show monitor session** *session number* command allows you to show the operation status of the SPAN session. One SPAN session does not take effect immediately after the swtich is powered on until the destination port is active.

5.2.2 Frame Type

5.2.2.1 Frame Direction

The SPAN session includes the following frame types:

Received frames

Received frames include all known unicast frames and routing frames, and each received frame is copied to the destination port. In one SPAN session, you can monitor the the frames inputted from one or multiple source ports. Although a frame inputted from the source port is dropped due to some reasons, for example, port security, it is still sent to the destination port. This does not affect the function of the SPAN.

Transmitted frames

All the frames sent from the source port are copied to the destination port. In one SPAN session, you can monitor the frames input from one or multiple source ports. If a frame from a port to the source port is dropped due to some reasons, the frame will not be sent to the destination port as well. Moreover, the format of the frames destined to the source port may change, for example, routed frames, source MAC address, destination MAC address, VLAN ID and TTL. Similarly, the format of the frames copied to the destination port will change.

Bi-directional frames

Bi-directional frames include the above mentioned two frames. In one SPAN session, you can monitor the frames received and transmitted from/to one or multiple source ports.

5.2.2.2 SPAN Traffic

You can use the SPAN to monitor all network communications, including multicast frames and BPDU frames.

5.2.3 Source Port

A source port (also known as monitored interface) is a switched port or routed port monitored for network analysis. In one SPAN session, you can monitor received, transmitted and bi-directional frames. There is no limit on the maximum number of the source ports.

A source port has the following features:

It can be a switched port, routed port or AP.

It cannot be a destination port at the same time.

It can specify the inbounding or outbounding direction of the monitored frames.

The source port and the destination port can reside in the same VLAN or different VLANs.

5.2.4 Destination Port

The SPAN session has a destination port (also known as the monitoring port) used to receive the frames copied from the source port.

The destination port has the following features:

It can be a Switched Port , Routed Port or AP.

The destination port can not be the source port at the same time.

5.2.5 Interaction between the SPAN and Other Functions

The SPAN interacts with the following functions.

- Spanning Tree Protocol (STP) — the destination port of SPAN participates in the STP.

5.3 Configuring SPAN

This section describes how to configure the SPAN on your switch.

5.3.1 Default SPAN Configuration

Function	Default Configuration
SPAN status	Disabled

5.3.2 Creating a SPAN Session and Specifying the Monitoring Port and Monitored Port

To set up a SPAN session and sepcify the destination port and the source port, execute the following commands.

Command	Function
DES-7200(config)# **monitor session** *session_number* **source interface** *interface-id* [,| -] {**both**	**rx**	**tx**}	Specify the source port. *interface-id*: Specify corresponding interface id.
DES-7200(config)# **monitor session** *session_number* **destination interface** *interface-id* [**switch**]	Specify the destination port. *interface-id*: Specify corresponding interface id. The **switch** parameter supports exchange on the mirrored destination port.

To delete a SPAN session, use the **no monitor session** *session_number* command in the global configuration mode. To delete all the SPAN sessions, use the **no monitor session all** command in the global configuration mode. You can use the **no monitor session** *session_number* **source interface** *interface-id* command or the **no monitor session** *session_number* **destination interface** *interface-id* command to delete the source port or destination port in the global configuration mode.

The following example shows how to create session 1. First, clear the configuration of session 1, and then mirror the frames from port 1 to port 8. The **Show monitor session** command allows you to verify your configuration.

```
DES-7200(config)# no monitor session 1
DES-7200(config)# monitor session 1 source interface gigabitEthernet 3/1 both
DES-7200(config)# monitor session 1 destination interface gigabitEthernet 3/8
DES-7200(config)# end
DES-7200# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

Caution

Session 1 is used to support ther global cross-linecard port mirror.

5.3.3 Deleting a Port from the SPAN Session

To delete a port from a SPAN session, execute the following commands:

Command	Function
DES-7200(config)# **no monitor session** *session_number* **source interface** *interface-id* [,| -] [**both**	**rx**	**tx**]	Specify the source port to delete. *interface-id*: Specify corresponding interface id.

You can use the **no monitor session** *session_number* **source interface** *interface-id* command to delete the source port from a SPAN session in the global configuration mode. The following example shows how to delete port 1 from session 1 and verify your configuration.

```
DES-7200(config)# no monitor session 1 source interface gigabitethernet 1/1
both
DES-7200(config)# end
DES-7200# show monitor session 1
sess-num: 1
dest-intf:
GigabitEthernet 3/8
```

5.3.4 Configuring the Flow-based Mirror

To configure the flow-based mirror, execute the following commands:

Command	Function
DES-7200(config)# [**no**] **monitor session** *session_number* **source interface** *interface-id* **rx acl** *name*	Specify the matched acl name for the mirrored flow and the mirrored source and destination ports.

Caution

Only the incoming port mirror is supported.

For the ACL configuration commands, see the related configuration guide.

5.3.5 Configuring one-to –many Mirror

The one-to-many mirror is the mirror with one mirrored source port and multiple mirrored destination ports. An one-to-many mirror includes three types of ports: the source port, the forwarding port and the destination port. To mirror the same source port to multiple destination ports, you can follow the steps below to:

- Set a RSPAN session(see the RSPAN configuration guide) with the one-to-many mirrored source port and mirrored forwarding port configured.
- Set the MAC loopback of the RSPAN forwarding port in the interface configuration mode.
- Add the forwarding port and the one-to-many mirrored destination port to the RSPAN VLAN in the Aceess mode.

Command	Function
DES-7200(config-if)# **mac-loopback**	Set the MAC loopback in the interface configuration mode.

- For the RSPAN forwarding port, no other settings are configured or no network cable is connected.
- You may not configure the switching on the RSPAN forwarding port.
- The following are the warnings for the MAC loopback configuration:

Caution

For the port with MAC loopback configured, if other protocols are enabled on this port, it is possible that the loopback packets lead to the running error of other protocols. For example, when enabling the Spanning Tree Protocol on the port with MAC loopback configured, and enabling the Loop Guard function(See STP configuration guide) at the same time, the BPDU messages from the STP will be sent back to the STP. To this end, for the STP, the loop occurs in the current network. To prevent the loops, you can set the port role as Backup Port and the port state as Block by the STP algorithm. However, it results in the abnormal forwarding of the data packets on this port. It is necessary to disable the MAC loopback function and the Loop Guard function to restore the port forwarding.

5.3.6 Other Precautions

- Connect the network analyzer to the monitoring port.
- When the SPAN is enabled, the configuration change has the following result.

1) If you change the VLAN configuration of the source port, the configuration takes effect immediately.

2) If you change the VLAN configuration of the destination port, the configuration takes effect immediately.

3) If you have disabled the source port or destination port, the SPAN does not take effect.

4) If you add the source or destination port to an AP, this will remove the source port or destination port from the SPAN.

5.3.7 Product Support

For DES-7200 series, if the vid for the tagged packet is inconsistent with the one for the VLAN to which the switch interface(take the interface A for example) belongs and the packets are sent to the interface A, the packets will not be forwarded or mirrored to the destination port.

For DES-7200 series, if IGMP Snooping function is enabled, the IGMP protocol messages cannot be mirrored to the designated port and the unknown multicast packets can not be mirrored neither.

For DES-7200 series, if the mirrored destination port is congested(for example, a 100Mbps destination port monitors a 1000Mbps source port), the Pause frames are sent from the source port.

For DES-7200 series, if the STP has not been enabled, the BPDU packets sent from the CPU can not be mirrored to the destination port.

By default, other ports on the DES-7200 series can not send the packets to the mirrored destination port. The mirrored destination port can not learn the address but it sends the packets to other ports. To allow the other ports to send the packets to the mirrored destination port and make the mirrored destination port to learn the address, you can configure the mirrored destination port switching.

For DES-7200 series, if the mirrored source port is the route port, the packets on the mirrored destination port are tag packets.

For DES-7200 series, with the multicast routing packets mirrored, the output packets on the mirrored destination port are the multicast packets before being routed.

For DES-7200 series, the functions of mirror and IPFIX sampling cannot be configured at the same direction on the same port simultaneously, but can be configured at different directions on the same port simultaneously. For example, the input mirror and input sampling or the output mirror and output sampling

cannot be co-configured; but the input mirror and output sampling or the output mirror and input sampling can be co-configured.

5.4 Showing the SPAN Status

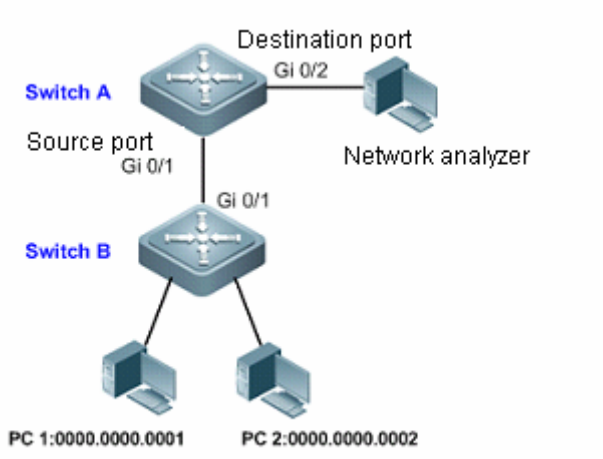
The **show monitor** command shows the current SPAN status. The following example illustrates how to show the current status of SPAN session 1.

```
DES-7200# show monitor session 1
sess-num: 1
src-intf:
GigabitEthernet 3/1 frame-type Both
dest-intf:
GigabitEthernet 3/8
```

5.5 Typical SPAN Configuration Examples

5.5.1 Example of Flow-based Mirror Configuration

5.5.1.1 Topology Diagram



Topology for simple SPAN application

5.5.1.2 Application Requirements

The network analyzer shall be able to monitor all dataflow forwarded by Switch A to Switch B and monitor specific dataflow from Switch B (such as the traffic from PC1 and PC2).

5.5.1.3 Configuration tips

1. Configure SPAN on the device (Switch A) connecting with network analyzer; configure the port (Gi 0/1) connected with Switch B as SPAN source port, and configure the port (Gi 0/2) connected with network analyzer as SPAN destination port.

2. Configure flow-based mirror (traffic from PC1 and PC2) on SPAN source port (Gi 0/1).

5.5.1.4 Configuration Steps

Step 1: Configure interconnection ports.

! Configure port Gi 0/1 of Switch A as Trunk Port.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

Step 2: Configure ACL.

! Create MAC extended ACL of "DES-7200" on Switch A to permit source MACs of 0000.0000.0001 and 0000.0000.0002.

```
SwitchA(config)#mac access-list extended DES-7200
SwitchA(config-mac-nacl)#permit host 0000.0000.0001 any
SwitchA(config-mac-nacl)#permit host 0000.0000.0002 any
SwitchA(config-mac-nacl)#exit
```

Step 3: Create SPAN session and specify the source port and destination port.

! On Switch A, create Session 1 and configure Gi 0/1 as the source port for mirroring bidirectional dataflow, and configure flow-based ingress mirror.

```
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 tx
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 rx acl
DES-7200
```

! On Switch A, configure Gi 0/2 as the destination port of Session 1

```
SwitchA(config)#monitor session 1 destination interface gigabitEthernet 0/2
```

5.5.1.5 Verification

Step 1: Display configurations of respective devices.

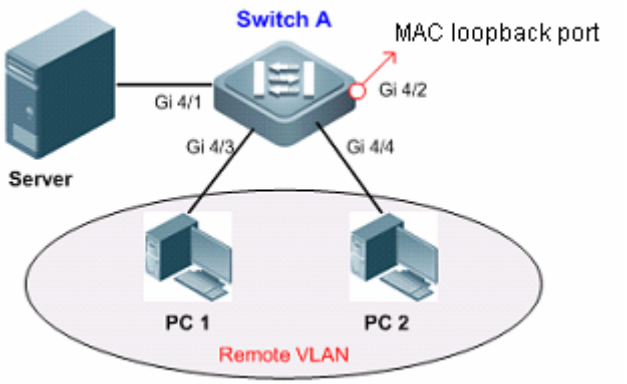
```
SwitchA#show running-config
!
mac access-list extended DES-7200
 10 permit host 0000.0000.0001 any etype-any
 20 permit host 0000.0000.0002 any etype-any
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
monitor session 1 destination interface GigabitEthernet 0/2
monitor session 1 source interface GigabitEthernet 0/1 tx
monitor session 1 source interface GigabitEthernet 0/1 rx acl DES-7200
!
```

Step 2: Display SPAN state of the device.

```
SwitchA#show monitor session 1
sess-num: 1                          //SPAN Session
span-type: LOCAL_SPAN                 //Local SPAN
src-intf:                             //information about SPAN source port
GigabitEthernet 0/1        frame-type Both
rx acl id 2900                        //Traffic-based SPAN
acl name DES-7200
dest-intf:                            //Information about SPAN destination port
GigabitEthernet 0/2
```

5.6 Example of One-to-Many Mirror Configuration

5.6.1.1 Topology Diagram



Topology for one-to-many SPAN application

5.6.1.2 Application requirement

Achieve one-to-many mirror on a single device, namely both PC 1 and PC 2 can monitor the flow sent and received on the server port.

5.6.1.3 Configuration tips

1. Create Remote VLAN on the device (Switch A)

2. Configure the device (Switch A) as the source device of RSPAN and configure the server-connecting port (Gi 4/1) as the source port; select one port (Gi 4/2) in Down state as the egress port, add this port to Remote VLAN and configure MAC loopback.

3. Join the ports directly connected with PC1 and PC2 into Remote VLAN.

Caution

1. This example only applies to DES-7200 series.

2. Configuring MAC loopback on the egress port will allow the broadcasting of mirror dataflow in Remote VLAN, so that any port joining Remote VLAN can monitor the source port, allowing one-to-many mirroring. If the source device is connected with multiple devices, we can configure Remote VLAN on the interconnected devices to realize remote SPAN.

5.6.1.4 Configuration Steps

Step 1: Configure Remote VLAN on the associated devices.

! Create Remote VLAN 100 on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 100
SwitchA(config-vlan)#remote-span
SwitchA(config-vlan)#exit
```

Step 2: Configure RSPAN source device.

! On Switch A, create RSPAN Session 1; configure this device as the source device and configure Gi 4/1 as the source port for mirroring bidirectional dataflow.

```
SwitchA(config)#monitor session 1 remote-source
SwitchA(config)#monitor session 1 source interface gigabitEthernet 4/1 both
```

! On Switch A, configure Gi 4/2 as the egress port and join the port into Remote VLAN 100; configure MAC loopback. We can find out that the port state changes from Down to Up.

```
SwitchA(config)#monitor session 1 destination remote vlan 100 interface
gigabitEthernet 4/2 switch
SwitchA(config)#interface gigabitEthernet 4/2
SwitchA(config-if-GigabitEthernet 4/2)#switchport access vlan 100
SwitchA(config-if-GigabitEthernet 4/2)#mac-loopback
```

Step 3: Join the ports directly connected with PC1 and PC2 into Remote VLAN.

! Join ports Gi 4/3 and Gi 4/4 of Switch A into Remote VLAN 100.

```
SwitchA(config)#interface range gigabitEthernet 4/3-4
SwitchA(config-if-range)#switchport access vlan 100
```

5.6.1.5 Verification

Step 1: Display configurations of the device.

```
SwitchA#show running-config
!
vlan 100
 remote-span
interface GigabitEthernet 4/2
 switchport access vlan 100
 mac-loopback
!
interface GigabitEthernet 4/3
 switchport access vlan 100
!
interface GigabitEthernet 4/4
 switchport access vlan 100
!
monitor session 1 remote-source
monitor session 1 destination remote vlan 100 interface GigabitEthernet 4/2
switch
monitor session 1 source interface GigabitEthernet 4/1 both
```

Step 2: Display RSPAN state

```
SwitchA#show monitor
sess-num: 1
span-type: SOURCE_SPAN                    //source device
src-intf:
GigabitEthernet 4/1       frame-type Both
dest-intf:
GigabitEthernet 4/2
remote vlan 100                           //belonging to Remote VLAN
mtp_switch on                             //Allow the destination port to
exchange normal traffic
```

6 RSPAN Configuration

6.1 Overview

RSPAN is the expansion of SPAN. Remote mirroring breaks the restriction that mirrored port and mirroring port must be on the same device. Multiple network devices are deployed between them and administrators can observe the data packets on the remotely mirroring port by analyzer in the central machine room.

All the mirrored packets are transmitted to the remote mirroring port via a special RSPAN Vlan (also known as Remote VLAN). Typical application topology is shown as below.

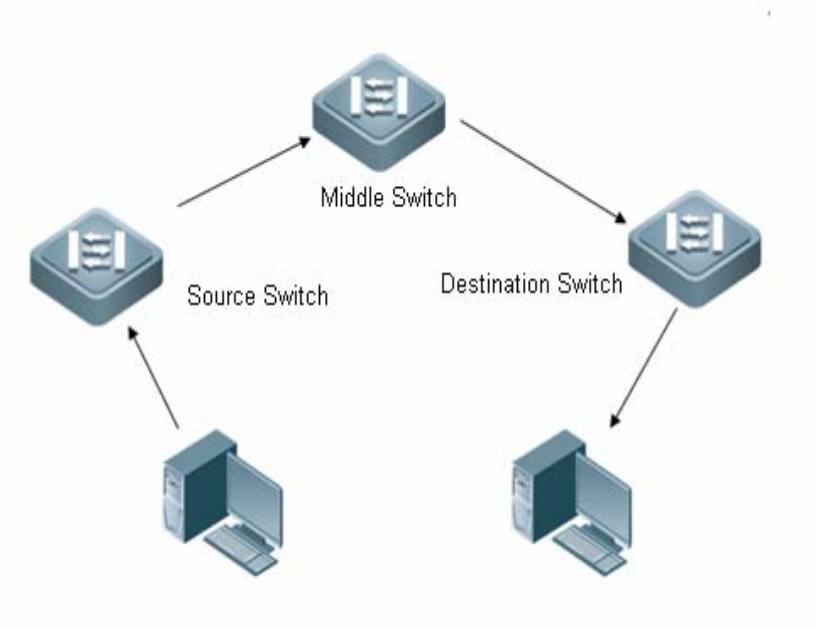


Figure 1 Typical RSPAN application topology

Figure 1 illustrates three roles:

- Source switch: Where the mirrored port is. The source switch copies the packets of source port and forwards them through the Remote VLAN to the middle swithc or the destination swithc.
- Middle switch: The one between the source switch and the destination switch. It transmmits the mirrored pakcets to the next middle switch or the destination switch via Remote VLAN. If the source switch is directly connected with the destination switch, then there is no middle swith.

- Destination switch: Where the mirroring destination port is. It forwards the mirrored packets received from Remote VLAN to the monitoring device via the mirroring destination port.

The table below presents ports that participate mirroring on the switch:

Switch	Mirrored Port	Function
Source switch	Source Port	Monitored user port that copies UDP to the designated output port or the reflector port via local port mirroring. There are many source ports.
	Reflector port	Used for one-to-many mirroring. The packets from the mirrored source port are reflected through the reflector port and then outputted through the output port. The reflector port cannot forward traffic. It is recommended to set the port in down state to be reflector port and disable any configuration on it.
	Output port	Send mirrored packets to the middle switch or the destination switch.
Middle switch	Common port	Send mirrored packets to the destination switch. It is recommended to configure two Trunk ports on the middle switch to connect the devices on both sides.
Destination switch	Source port	Receive remote mirrored packets.
	Destination port	Monitoring port of remote mirrored packets.

A special VLAN, Remote VLAN is defined for remote port mirroring. The Remote VLAN transmits only mirrored packet rather than bearing normal services. All mirrored packets are transmitted from the source swithc through the Remote VLAN to the designated port of the destination switch. Hence, you can monitor the packets of the source switch on the destination switch.

 **Note**	RSPAN and local SPAN can be enabled simultaneously on the source switch, the middle switch and the destination switch. The packets of Remote VLAN bring no influence on the CPU utilization. You can enable or disable communications on the mirroring destination port. Communications is disabled by default. It is recommended to set the mirrored source port and reflector port in different VLANs. AP can not be set as the Reflector Port. Remote VLAN can neither be VLAN 1 nor Private VLAN. Remote VLAN does not join GVRP.

6.2 Configuring RSPAN

- Configurtion preparation
- Configure the source switch
- Configure the middle swtich
- Configure the destination switch
- Configure flow-based RSPAN

6.2.1 Configuration Preparation

- Determine the source switch, the middle switch and the destination switch.
- Determine the mirrored source port, the reflector port, the mirrored destination port and Remote VLAN.
- Guarentee L2 interoperability between the source switch and the destination switch in Remote VLAN.
- Determine the direction of monitored packets.
- Enable Remote VLAN

6.2.2 Configuring the Source Switch

- RSPAN session
- Source port

- Output port
- Remote VLAN
- VSPAN
- One-to-many mirroring
- Configuration steps

6.2.2.1 Configuring RSPAN Session

RSPAN session has the same features as local SPAN session. For details, refer to SPAN Configuration Guide.

Product support	DES-7200 series supports 128 RSPAN sessions.

6.2.2.2 Configuring Source Port

Source port is also known as monitored port. In a RSPAN session, data streams of source port are monitored for analysis or troubleshooting. Users can monitor incoming, outgoing or both data streams. The number of source ports is also not limitted.

The source port comes with the following features:

- Source port can be switched port, routed port or AP.
- Multiple source ports on the source switch can be mirrored to the designated output port.
- Source port and output port cannot be set to the same one.
- When the mirrored source port is a Layer 3 port, Layer 2 and Layer 3 packets can be monitored.
- In case of bidirectional monitoring of multiple ports, you only need to monitor one flow direction of packets.
- You can monitor the incoming and outgoing packets on the STP-enabled port in block state.
- The source port and the destination port can belong to the same VLAN or different VLANs.

6.2.2.3 Configuring Output Port

The RSPAN mirroed streams are broadcasted from the output port of the source switch to the middle switch. The output port features:

- The output port can be switched port, routed port or AP.

- The output port belongs to only one RSPAN session.

Product support	DES-7200 series support one output port per RSPAN session.

6.2.2.4 Configuring Remote VLAN

RSPAN mirrored streams are broadcasted via the Remote VLAN. The Remote VLAN transmits only mirrored packets rather than bearing normal services. All mirrored packets are transmitted from the source swithc through the Remote VLAN to the designated port of the destination switch. Hence, you can monitor the packets of the source switch on the destination switch.

Remote VLAN features:

- Remote VLAN can neither be VLAN 1 nor private VLAN.
- One Remote VLAN corresponds to one RSPAN session.

Product support	For DES-7200 series, the source switch supports up to 128 Remote VLANs and the middle switch and the destination switch support up to 1791 Remote VLANs.

 **Note**	The reflector port needs to join the Remote VLAN. The reflector port cannot forward traffic as normal port. It is recommended to set the port in down state as reflector port and disable other configurations on it.

6.2.2.5 Configure VSPAN

VSPAN, the abbreviation of VLAN SPAN, refers to mirroring the data streams of some VLANs as source to the destination port of the destinatio device.

VSPAN features:

- A VLAN other than Remote VLAN can be set as the source of mirrored packets by the monitor session session-num source vlan vlan-id [rx | tx | both] command.
- Some VLANs other than Remote VLAN can be set as the source of mirrored packets by the monitor session session-num filter vlan vlan-id-list command.

6.2.2.6 Configuring One-to-many Mirroring

RSPAN session supports more than one destination device, each device supports one destination port. To enable one-to-many mirroring, run the following command to configure the reflector port on the source switch:

Command	Function
DES-7200(config)# **monitor session** *session_num* **destination remote vlan** *remote_vlan-id* [*reflector-port*] **interface** *interface-name* [**switch**]	Configure Remote VLAN and reflector port. The reflector port should join the Remote VLAN. The Switch keywork indicates the destination port joins switching.

Product support	For DES-7200 series, each session supports one reflector port.

Note	The reflector port needs to join the Remote VLAN. The reflector port cannot forward traffic as normal port. It is recommended to set the port in down state as reflector port and disable other configurations on it.

6.2.2.7 Configuration Steps

Configure the source switch by the following steps:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode.
DES-7200(config-Vlan)# **remote-span**	Set the VLAN as the remote SPAN VLAN.
DES-7200(config-Vlan)# **exit**	Return to the global configuration mode.
DES-7200(config)# **monitor session** *session_num* **remote-source**	Configure the remote mirroring source.
DES-7200(config)# **monitor session** *session-num* **source interface** *interface-name* [**rx** | **tx** | **both**]	Configure the remote mirrored source port (rx and tx of the source port can be set to the same or different destination port; but each of them can be configured with one destination port only.)

DES-7200(config)#**monitor session** *session_num* **destination remote vlan** *remote_vlan-id [reflector-port]* **interface** *interface-name* **[switch]**	Configure Remote VLAN and reflector port. The reflector port should join the remote VLAN. It is unnecessary to configure the Reflector port for DES-7200 series. The output destination portis mandatory. **switch** indicates the destination port joins switching.
DES-7200(config)# **monitor session** *session_number* **source interface** *interface-id rx* **acl** *name*	Set theACL for the streams to be mirrored.

Caution

- It is not recommended to add common ports to Remote VLAN.
- Do not set the port that is connected to the middle switch or the destination switch to be the mirrored source port, or otherwise it will may cause flow confusion in the network.
- In a RSPAN session, if the middle switch uses the port of non-E series line cards as forwarding port, only RX or TX mirroring can be configured on the source switch. And if alternative configuration of TX mirroring and RX mirroring is executed on the source switch, you should clear the MAC address of Remote VLAN on the middle switch.

6.2.3 Configuring the Middle Switch

In a RSPAN session, the middle switch ensures transparnet transmission of mirrored packets in a VLAN.

Command	Function
DES-7200# configure terminal	Enter the global configuration mode.
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode.

DES-7200(config-Vlan)# **remote-span**	Set the VLAN as the remote-span VLAN.
DES-7200(config-Vlan)# **exit**	Return to the global configuration mode.

6.2.4 Configuring the Destination Switch

6.2.4.1 Destination Port

The remote RSPAN device forwards the mirrored packets received from the Remote VLAN to the monitoring device through the destination port.

Destination port features:

- The destination port can be switched port, routed port or AP.
- The destination port can be set to enable or disable communications. Communicatios is disabled by default. Under default configuration, neither the packets from other ports nor the packets from CPU are forwarded.

Product support	◆ For DES-7200 series, there is no limit on the number of RSPAN destination switches supported in case of one-to-many mirroring. ◆ For DES-7200 series, each RSPAN destination switch supports one destination port. ◆ For DES-7200 series, the destination port of the RSPAN destination switch cannot be protected port.

6.2.4.2 Configuration Steps

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **vlan** *vlan-id*	Enter the VLAN configuration mode.
DES-7200(config-Vlan)# **remote-span**	Set the VLAN as remote-span Vlan.
DES-7200(config-Vlan)# **exit**	Return to the global configuration mode.
DES-7200(config)# **monitor session** *session_num* **remote-destination**	Configure the remote mirroring destination.

DES-7200(config)# **monitor session** *session-num* **destination remote vlan** *vlan-id* **interface** *interface-name* **[switch]**	Configure Remote VLAN and the remote mirroring destination port. **switch** indicates the destination port joins switching.
DES-7200(config)# **interface** *interface-name*	Enter the remote mirrorring destination port.
DES-7200(config-if)# { **switchport access vlan** *vid* | **switchport trunk native vlan** *vid* }	*Vid:* VID for remote-span vlan. If the destination port is acess port, join the destination port to remote-span vlan; If the destination port is trunk port, join the destination port to remote-span vlan and set the remote-span vlan as the native vlan for the destination port.

6.2.5 Configuring Flow-baed RSPAN

As the expansion of local SPAN, RSPAN supports flow-based mirroring as well. For details, refer to *Mirroring Configuration Guide*.

Note	Flow-based RSPAN brings no influence on communications. Users can set ACL at the inbounding direction of the source port of the source RSPAN switch. Standard ACL, extended ACL, MAC ACL and user-defined ACL are supported. Users can set port ACL at the inbounding direction of the source port of the source RSPAN switch, and set port ACL at the outbounding direction of the destination port of the destination RSPAN switch. Users can apply ACL at the outbounding direction of Remote VLAN on the soruce RSPAN switch, and apply ACL at the inboudning direction of Remote VLAN on the destination RSPAN switch.

6.3 Showing RSPAN Session

Command	Function
DES-7200# **show monitor**	Show the mirroring configuation.

For example:

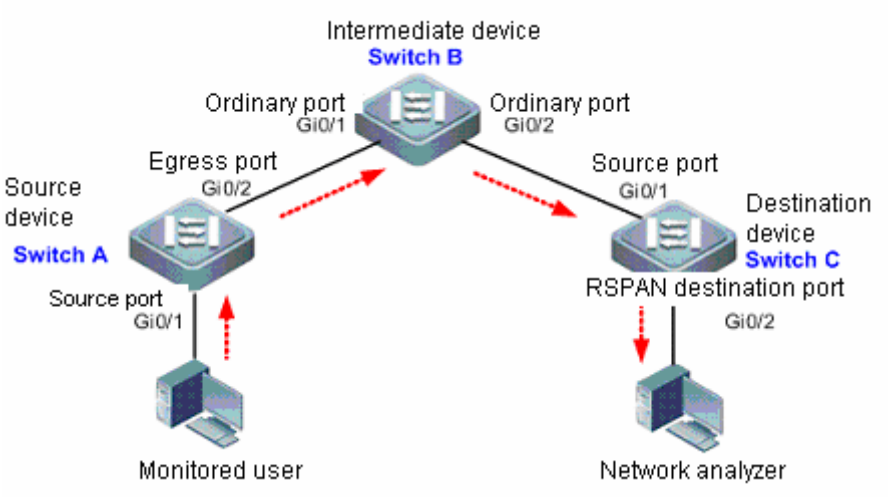
```
DES-7200# show monitor
sess-num: 1
src-intf:
```

```
GigabitEthernet 0/4 frame-type Both
dest-intf:
GigabitEthernet 0/6
remote vlan 3
```

6.4 Typical RSPAN Configuration Examples

6.4.1 Example of configuring RSPAN without supporting reflector port

6.4.1.1 Topological Diagram



Application topology for RSPAN without supporting reflector port

6.4.1.2 Application Requirements

- The network analyzer can monitor the user through remote span.
- Data can be exchanged normally between devices.

6.4.1.3 Configuration Tips

1. Configure Remote VLAN on the source device (Switch A), intermediate device (Switch B) and destination device (Switch C).

2. On the source device, configure the port (Gi 0/1) directly connected with user as the source port, and configure the port (Gi 0/2) connected with intermediate device as the egress port; enable traffic exchange on the egress port.

3. On the intermediate device, ports (Gi 0/1 and Gi 0/2) connected with source device and destination device are configured to ordinary ports.

4. On the destination device, the port (Gi 0/1) connected with the intermediate device acts as the source port (configured to ordinary port), and the port (Gi 0/2) connected with network analyzer shall be configured to RSPAN destination port, on which traffic exchange shall be enabled.

Caution

1. This example applies to devices which doesn't support the reflector port.

2. The RSPAN traffic forwarded through the egress port of source device can be broadcasted in Remote VLAN, so that any port other than the source device can monitor the source port after joining Remote VLAN, allowing one-to-many remote mirroring. If a RSPAN destination port is specified on the destination device, then the RSPAN traffic will only be forwarded to this destination port.

6.4.1.4 Configuration Steps

Step 1: Configure the Remote VLAN.

! Create VLAN 7 on Switch A and set it as Remote VLAN.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 7
SwitchA(config-vlan)#remote-span
SwitchA(config-vlan)#exit
```

! Configurations of Switch B and Switch C are the same as above.

Step 2: Configure the RSPAN source device.

! On Switch A, configure port Gi 0/2 as the Trunk Port for connecting Switch B.

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

! On Switch A, create RSPAN Session 1; configure this device as the source device and configure Gi 0/1 as the source port and Gi 0/2 as the egress port.

```
SwitchA(config)#monitor session 1 remote-source
SwitchA(config)#monitor session 1 source interface gigabitEthernet 0/1 both
```

```
SwitchA(config)#monitor session 1 destination remote vlan 7 interface
gigabitEthernet 0/2 switch
```

Step 3: Configure RSPAN intermediate device

! On Switch B, configure ports Gi 0/1 and Gi 0/2 as the Trunk Port.

```
SwitchB(config)#interface range gigabitEthernet 0/1-2
SwitchB(config-if-range)#switchport mode trunk
```

Step 4: Configure RSPAN destination device

! On Switch C, configure port Gi 0/1 as the Trunk Port, which is used as the source port to connect Switch B

```
SwitchC(config)#interface gigabitEthernet 0/1
SwitchC(config-if-GigabitEthernet 0/1)#switchport mode trunk
```

! On Switch C, create RSPAN Session; configure this device as the destination device and configure Gi 0/2 as RSPAN destination port.

```
SwitchC(config)#monitor session 1 remote-destination
SwitchC(config)#monitor session 1 destination remote vlan 7 interface
gigabitEthernet 0/2 switch
```

6.4.1.5 Verification

Step 1: Display configurations of the device.

! Configurations of Switch A

```
SwitchA#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2
switch
monitor session 1 source interface GigabitEthernet 0/1 both
!
```

! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
```

```
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport mode trunk
```

! Configurations of Switch C

```
SwitchC#show running-config
!
vlan 7
 remote-span
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface GigabitEthernet 0/2
switch
```

Step 2: Display RSPAN information of the device

! Switch A

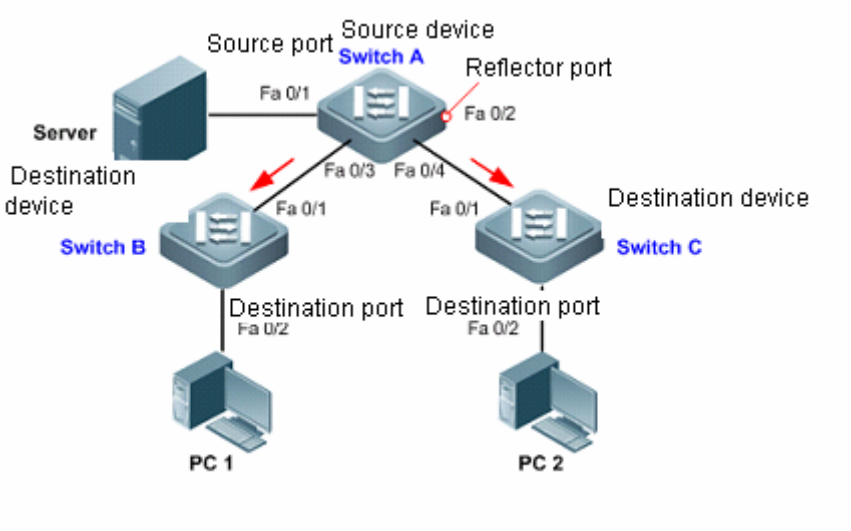
```
SwitchA#show monitor
sess-num: 1                                    //RSPAN Session
span-type: SOURCE_SPAN                         //RSPAN source device
src-intf:                                      //information about RSPAN source port
GigabitEthernet 0/1       frame-type Both
dest-intf:                                     //information about RPSAN egress port
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                          //Allow the egress port to exchange
normal traffic
```

! Switch C

```
SwitchC#show monitor
sess-num: 1                                    //RSPAN Session
span-type: DEST_SPAN                           //RSPAN destination device
dest-intf:                                     //information about RSPAN destination port
GigabitEthernet 0/2
remote vlan 7
mtp_switch on                         //Allow the destination port to
exchange data
```

6.4.2 Example of configuring RSPAN supporting reflector port

6.4.2.1 Topological Diagram



Application topology for RSPAN supporting reflector port

6.4.2.2 Application Requirements

Achieve one-to-many remote SPAN, namely both PC1 and PC2 can monitor the traffic sent and received on the service through remote SPAN.

6.4.2.3 Configuration Tips

1. Create Remote VLAN on all associated devices (Switch A, B and C).

2. Configure the server-connecting device (Switch A) as RSPAN source device and configure the server-connecting port (Fa 0/1) as RSPAN source port; configure one port (Fa 0/2) in Down state as the reflector port.

3. Configure the PC-connecting devices (Switch B and Switch C) as RSPAN destination device and configure the PC-connecting ports (Fa 0/2) as RSPAN destination port.

4. The ports interconnecting devices are only needed to be configured as Trunk port, which by default can forward the RSPAN traffic in Remote VLAN.

Caution

1. This example applies to devices which support the reflector port.

2. The RSPAN traffic forwarded through the reflector port can be broadcasted in Remote VLAN, so that any port joining the Remote VLAN can monitor the source port, allowing one-to-many mirroring. If a RSPAN destination port is specified on the destination device, then the RSPAN traffic will only be forwarded to this destination port.

3. If multiple intermediate devices exist between source device and destination device, we only need to configure Remote VLAN on the intermediate devices and configure interconnecting ports as Trunk Port to realize cross-device remote SPAN.

6.4.2.4 Configuration Steps

Step 1: Create Remote VLAN on the device.

! Create Remote VLAN 7 on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#vlan 7
SwitchA(config-vlan)#remote-span
SwitchA(config-vlan)#exit
```

! Configurations of Switch B and Switch C are the same as above.

Step 2: Configure RSPAN source device.

! On Switch A, create RSPAN Session 1; configure this device as the source device and configure Fa 0/1 as RSPAN source port and Fa 0/2 as the reflector port. We can find out that the port state changes from Down to Up.

```
SwitchA(config)#monitor session 1 remote-source
SwitchA(config)#monitor session 1 source interface fastEthernet 0/1 both
SwitchA(config)#monitor session 1 destination remote vlan 7 reflector-port
interface fastEthernet 0/2 switch
```

Step 3: Configure RSPAN destination device.

! On Switch B, create RSPAN Session 1; configure this device as the destination device and configure Fa 0/2 as RSPAN destination port.

```
SwitchB(config)#monitor session 1 remote-destination
SwitchB(config)#monitor session 1 destination remote vlan 7 interface
fastEthernet 0/2  switch
```

! Configurations of Switch C are the same as above.

Step 4: Configure ports interconnecting devices as Trunk port.

! Configure ports Fa 0/3 and Fa 0/4 of Switch A as Trunk Port.

```
SwitchA(config)#interface range fastEthernet 0/3-4
SwitchA(config-if-range)#switchport mode trunk
```

! Configure port Gi 0/1 of Switch B as Trunk Port.

```
SwitchB(config)#interface fastEthernet 0/1
SwitchB(config-if-FastEthernet 0/1)#switchport mode trunk
```

! Configurations of Switch C are the same as those of Switch B.

6.4.2.5 Verification

Step 1: Display configurations of respective devices.

! Configurations of Switch A

```
SwitchA#show running-config
!
vlan 7
 remote-span
!
interface FastEthernet 0/3
 switchport mode trunk
!
interface FastEthernet 0/4
 switchport mode trunk
!
monitor session 1 remote-source
monitor session 1 destination remote vlan 7 reflector-port interface
FastEthernet 0/2 switch
monitor session 1 source interface FastEthernet 0/1 both
```

! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 7
 remote-span
!
interface FastEthernet 0/1
 switchport mode trunk
!
monitor session 1 remote-destination
monitor session 1 destination remote vlan 7 interface FastEthernet 0/2 switch
```

! Configurations of Switch C won't be introduced herein.

Step 2: Display RSPAN status

! Configurations of Switch A

```
SwitchA#show monitor
sess-num: 1                                    //RSPAN Session
span-type: SOURCE_SPAN                         //RSPAN source device
src-intf:                                      //information about RSPAN source
port
FastEthernet 0/1          frame-type Both
dest-intf:                                     //information about RSPAN
destination port
FastEthernet 0/2
remote vlan 7
mtp_switch on                              //Allow the destination port to
exchange traffic
```

! Configurations of Switch B

```
SwitchB#show monitor
sess-num: 1
span-type: DEST_SPAN
dest-intf:
FastEthernet 0/2
remote vlan 7
mtp_switch on
```

! Configurations of Switch C won't be introduced herein.

DES-7200
IP Routing Configuration Guide
Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

Note

The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products.

The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 Protocol-Independent Configuration

1.1 IP Routing

1.1.1 Configuring Static Routes

Static routes are manually configured so that the packets can be sent to the specified destination network go through the specified route. When it fails to learn the routes of some destination networks, it becomes critical to configure static routes. It is a common practice to configure a default route for the packets that do not have a definite route.

To configure static routes, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)**# ip route** [**vrf** *vrf_name*] *network mask* {*ip-address* | *interface-type interface-number* [*ip-address*]} [*distance*] [**tag** *tag*] [**permanent**] [**weight** *weight*] [**track** *object-number*]	Configure static routes.
DES-7200(config)**# no ip route** *network mask*	Delete Static Route
DES-7200(config)**# ip static route-limit** *number*	Specify the maximum number of static routes.
DES-7200(config)**# no ip static route-limit**	Restore the default maximum number of static routes.

For the example of configuring static routes, see “Example of Dynamic Routes Overriding Static Routes” in this chapter.

If they are not deleted, DES-7200 product will always retain the static routes. However, you can replace the static routes with the better routes learned by the dynamic routing protocols. Better routes mean that they have smaller distances. All routes including the static ones carry the parameters of the management distance. The following table shows the management distances of various sources of DES-7200 product:

Route source	Default management distance

Route source	Default management distance
Directly connected networks	0
Static route	1
OSPF route	110
ISIS route	115
RIP route	120
Unreachable route	255

Note

The static route redistribution shall be configured if the static routes are advertised by the dynamic routing protocols such as RIP and OSPF.

When a port is “down”, all routes to that port will disappear from the routing table. In addition, when DES-7200 product fails to find the forwarding route to the next-hop address, the static route will also disappear from the routing table.

When the specified VRF static routes are added to the corresponding VRF, if the egress is specified at the same time, but the VRF of the egress does not match the specified VRF, the addition will fail. If no VRF is specified, it is added to the global routing table by default.

By default, the weight of static route is 1. To view the static routes of non-default weight, execute the **show ip route weight** command. When there are load balanced routes to an IP address, the switch will assign traffic by their weights. The higher the weight of a route is, the more the route forwards. Router WCMP limit is 32, while the switch WCMP limit is related to product model because the weights supported by various chips are different. For the detailed information about the route weight value of specific model, please refer to the product specification paper.

When the sum of load-balancing route weights exceeds WCMP limit, the exceeded routes will not take effect. For example, if the WCMP limit on a device is 8, only one static route configuration is effective:

```
DES-7200(config)#ip route 10.0.0.0 255.0.0.0 172.0.1.2 weight 6
DES-7200(config)#ip route 10.0.0.0 255.0.0.0 172.0.1.4 weight 6
DES-7200(config)#show ip route 10.0.0.0
Routing entry for 10.0.0.0/8
  Distance 1, metric 0
  Routing Descriptor Blocks:
  *172.0.1.2, generated by "static"
DES-7200(config)#show ip route weight
------------[distance/metric/weight]-----------
```

```
S    10.0.0.0/8 [1/0/6] via 172.0.1.2
```

The maximum number of static routes is 1024 by default. If the number of static routes configured exceeds the specified upper limit, they will not be automatically deleted, but the addition will fail.

To view the configuration of IP route, execute the **show ip route** command to view the IP routing table. For details, refer to *Protocol-independent Command Configuration.*

1.1.2 Configuring Default Route

Not all devices have a complete network-wide routing table. To allow every device to route all packets, it is a common practice that the powerful core network is provided with a complete routing table, while the other devices have a default route set to this core router. Default routes can be transmitted by the dynamic routing protocols, and can also be manually configured on every router.

Default routes can be generated in two ways: 1) manual configuration. For details, see *Configuring Static Routes* in the last section; 2) manually configuring the default network.

Most internal gateway routing protocols have a mechanism that transmits the default route to the entire routing domain. The device that needs to transmit the default route must have a default route. The transmission of the default route in this section applies only to the RIP routing protocol. The RIP always notifies the “0.0.0.0” network as the default route to the routing domain. For more information on how OSPF generates and transmits the default routes, see *OSPF Routing Protocol Configuration Guide*.

To general static routes, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip default-network** network	Configure the default network.
DES-7200(config)# **no ip default-network** network	Delete the default network.

Note

To generate the default routes by using the **default-network** command, the following condition must be met: The default network is not a directly-connected port network, but is reachable in the routing table.

Under the same condition, the RIP can also transmit the default route. Alternatively, there is another way to do so, that is, by configuring the default static route or learning the 0.0.0.0/0 router via other routing protocols.

If the router has a default route, whether learned by the dynamic routing protocol or manually configured, when you use the **show ip route** command, the "gateway of last resort" in the routing table will show the information of the last gateway. A routing table may have multiple routes as alterative default routes, but only the best default route becomes the "gateway of last resort".

1.1.3 Configuring the Number of Equivalent Routes

If the load balancing function is needed, you can set the number of equivalent routes for control. An equivalent route is an alternative path to the same destination address. When there is only one equivalent route, one destination address can be configured with only one route, and the load balancing function is cancelled.

To configure the number of equivalent routes, execute the following commands in the global configuration mode. The **no** form of this command restores the default number of equivalent routes.

This command is valid for both ipv4 and ipv6. That is to say, after configuring this command, the maximum numbers of the equivalent route path to IPv4 and IPv6 destination are the same value configured.

Command	Function
maximum-paths [*number*]	Configure the number of equivalent routes (in the range 1 to 32).

1.2 Route-Map

Route-map is a collection of filter policy for the routing protocol and policy route, independent from the detailed routing protocol. Route-map is used to filter and modify the routing information for the routing protocol, and control the packet forwarding for the policy route.

To define the route map, use the following command in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define the route map. *Sequence*: 0-65535
DES-7200(config)# **no route-map** *route-map-name* {[**permit** | **deny**] *sequence*}	Remove the route map.

When you configure the rules for a route map, you can execute one or multiple **match** or **set** commands. If there is no match command, all will be matched. If there is no set command, not any action will be taken.

To define the matching conditions for the rules, execute the following commands in the route map configuration mode:

Command	Function
DES-7200(config-route-map)# **match community** {*standard-list-number* | *expanded-list-number* | *community-list-name*}	Match the community attribute of BGP route.
DES-7200(config-route-map)# **match interface** *interface-type interface-number*	Match the next-hop interface for the route.
DES-7200(config-route-map)# **match ip address** *access-list-number* [*…access-list-number*]	Match the ACL IP address.
DES-7200(config-route-map)# **match ip next-hop** *access-list-number* [*…access-list-number*]	Match the next-hop IP address in the ACL.
DES-7200(config-route-map)# **match ip route-source** *access-list-number* [*…access-list-number*]	Match the route source IP address in the ACL.
DES-7200(config-route-map)# **match ipv6 address** { *access-list-name* | **prefix-list** *prefix-list-name* }	Match the IPv6 ACL or prefix list.

Command	Function
DES-7200(config-route-map)# **match ipv6 next-hop** { *access-list-name* | **prefix-list** *prefix-list-name* }	Match the next-hop IP address in the ACL or the prefix list.
DES-7200(config-route-map)# **match ipv6 route-source** { *access-list-name* | **prefix-list** *prefix-list-name* }	Match the route source IP addres in the ACL or the prefix list.
DES-7200(config-route-map)# **match metric** *metric*	Match the route metric value. *metric* ：0-4294967295
DES-7200(config-route-map)# **match origin** {**egp** | **igp** | **incomplete**}	Match the route origin type.
DES-7200(config-route-map)# **match route-type** {**local** | **internal** | **external** [**level-1** | **level-2**]}	Match the route type.
DES-7200(config-route-map)# **match tag** *tag*	Match the route tag value. *tag* ：0-4294967295

To define the oeration after matching, use the following command in the route map configuration mode:

Command	Function
DES-7200(config-route-map)# **set aggregator as** *as-num ip_addr*	Set the AS attribute value for the route aggregator.
DES-7200(config-route-map)# **set as-path prepend** *as-number*	Set the AS_PATH attribute value.
DES-7200(config-route-map)# **set comm-list** *community-list-number* | *community-list-name* **delete**	Cancel all community attribute value in the COMMUNITY_LIST.
DES-7200(config-route-map)# **set community** {*community-number*[*community-numbe…*] **additive** | **none**}	Set the COMMUNITY attribute value.

Command	Function
DES-7200(config-route-map)# **set dampening** *half-life reuse suppress max-suppress-time*	Set the route dampening parameter.
DES-7200(config-route-map)#**set extcommunity** {**rt** *extend-community-value* | **soo** *extend-community-value*}	Set the extended community attribute value.
DES-7200(config-route-map)# **set ip default next-hop** *ip-address*	Set the default next-hop IP address.
DES-7200(config-route-map)# **set ip next-hop** *ip-address*	Set the next-hop IP address.
DES-7200(config-route-map)# **set ip next-hop verify-availability** *ip-address* **track** *track-object-num*	Set the reachability of the next-hop IP address.
DES-7200(config-route-map)# **set level** {**stub-area** | **backbone** | **level-1** | **level-1-2** | **level-2**}	Set the route area.
DES-7200(config-route-map)# **set local-preference** *number*	Set the LOCAL_PREFERENCE value.
DES-7200(config-route-map)# **set metric** *metric*	Set the metric value of the route redistribution.
DES-7200(config-route-map)# **set metric** [+ *metric-value* |- *metric-value* | *metric-value*]	Set the metric type of route redistribution.
DES-7200(config-route-map)# **set metric-type** {**type-1** | **type-2 | external** | **internal**}	Set the metric type of route redistribution.
DES-7200(config-route-map)# **set next-hop** *next-hop*	Set the next-hop IP address for the route redistribution. *next-hop*： next-hop IP address.

Command	Function
DES-7200(config-route-map)# **set origin** {**egp** | **igp** | **incomplete**}	Set the route origin attribute.
DES-7200(config-route-map)**#set originator-id** *ip-addr*	Set the route originator id.
DES-7200(config-route-map)**# set tag** *tag*	Set the tag value for the route redistribution.

For different route-map applications, the results of the **match** and **set** command are different. To make the user know whether the **match** and **set** command is appropriate for the current application or not, DES-7200 provides the user the message in the following circumstances:

When associating the **route-map** command, check the appropriateness of the **match** and **set** command configuration in the **route-map** and the current associated application. If it is not appropriate, the message prompts.

When configuring the **route-map**, **match** or **set** command, check the appropriateness of all applications associated with the **route-map** and the **match** and **set** command configuration in the **route-map.** If it is not appropriate, the message prompts.

1.3 Route Redistribution

1.3.1 Configuring Route Redistribution

To support the routers to run multiple routing protocol processes, DES-7200 product provides the function for redistributing the route information from one routing process to another routing process. For example, you can redistribute the routes in the OSPF routing area to the RIP routing area , or those in the RIP routing area to the OSPF routing area. Routes can be redistributed among all the IP routing protocols.

In route redistribution, the route maps are often used to enforce conditional control over the mutual route redistribution between two routers.

To redistribute routes from one routing area to another and control route redistribution, execute the following commands in the routing process configuration mode:

Command	Function

Command	Function
DES-7200(config-router)# **redistribute** *protocol* [*process-id*] [**metric** *metric*] [**metric-type** *metric-type*] [**match internal** | **external** *type*| **nssa-external** *type*] [[**tag** *tag*] [**route-map** *route-map-name*] [**subnets**]	Set route redistribution. *Protocol* (protocol type): bgp, connected, isis, rip, static
DES-7200(config-router)# **default-metric** *metric*	Set the default metric for all redistributed routes.

Route redistribution may easily cause loops, so you must be very careful in using them.

Note

When the route redistribution is configured in the OSPF routing process, the metric of 20 is allocated to the redistributed routes with the type of Type-2 by default. This type belongs to the least credible route of the OSPF.

1.3.2 Configuring Default Route Distribution

To advertise the default route, it is necessary for routing protocol to introduce the default route to the process, or enforce generating a default route.

To distribute the default route, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]	Introduce the default route to the routing protocol process and advertise the route default. **always(optional):** a default route is always introduced to the process no matter whether the default route exists in the local routing table or not. **metric(optional):** set the metric value for the introduced default route. **metric-type(optional):** set the default route type. **route-map(optional):** filter and set the default route.
DES-7200(config-router)# **no default-information originate** [**always**] [**metric** *metric*] [**metric-type** *type*] [**route-map** *map-name*]	Cancel the introduction of the default route to the routing protocol process and the route default advertisement.

1.3.3 Route Filtering

Route filtering is the process to control the incoming/outgoing routes so that the router only learns the necessary and predictable routes, and only advertise the necessary and predictable routes to external trusted devices. The divulgence and chaos of the routes may affect the running of the network. Particularly for telecom operators and financial service networks, it is essential to configure route filtering.

1.3.3.1 Controlling Route Updating Advertising

To prevent other routers or routing protocols from dynamically learning one or more route message, you can configure the control over route updating advertising to prevent the specified route update.

To prevent route updating advertising, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* **out** [*interface-type interface-number*]	According to ACL rules, permit or deny some routes. **Prefix:** This keyword specifies the prefix list for filtering routes. The prefix list should be separately configured by using the **ip prefix-list** command.
DES-7200(config-router)# **no distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name}* **out** [*interface-type interface-number* | *protocol*]	Remove the configuration.

Note

When you configure the OSPF, you cannot specify the interface and the features are only applicable to the external routes of the OSPF routing area.

1.3.3.2 Controlling Route Updating processing

To avoid processing some specified routes of the incoming route update packets, you can configure this feature. This feature does not apply to the OSPF routing protocol.

To control route updating processing, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **distribute-list** {[*access-list-number* | *access-list-name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name*} **in** [*interface-type interface-number*]	According to ACL rules, permit or deny receiving distributed routes. **Prefix:** This keyword specifies the prefix list for filtering routes. The prefix list should be separately configured by using the ip prefix-list command. **Gateway:** Use the prefix list to filter the routes distributed according to the source of the routes.
DES-7200(config-router)# **no distribute-list** {[*access-list-number* | *name*] | **prefix** *prefix-list-name* [**gateway** *prefix-list-name*] | **gateway** *prefix-list-name* } **in** [*interface-type interface-number*]	Remove the configuration.

1.4 IP Event Dampening Configuration

1.4.1 Overview

For a layer-3 switch, when a layer-3 network interface changes state frequently (UP/DOWN), it will cause repeated flapping of routing table on the device. If routing protocols have been configured, the routing protocols may also spread such flap throughout the network, making their neighbors to update and recalculate routes repeatedly. It will not only waste network bandwidth, but also result in the instability of entire network. From the perspective of the device, repeated route update and calculation will consume substantial CPU resources and compromise the normal operation of client's network.

The IP Event Dampening feature introduces a mechanism to suppress interface flapping and avoid bandwidth wasting and network instability. By configuring suppression feature on the layer-3 interface, the interface can automatically identify and suppress abnormal UP/DOWN flapping of the interface. From the perspective of routing protocols, since such abnormal interface is placed in DOWN state, a single-node link failure will not be spread by the routing protocols. When the interface stops flapping and stabilizes, the interface will be unsuppressed. IP Event Dampening well reduces network convergence times and system CPU consumption and improves the stability of entire network.

1.4.2 Interface State Change Events

The feature of IP Event Dampening perceives and controls interface behavior by adopting a mechanism of calculating the penalty upon any change in interface state. Each up-down flapping of interface will lead to the accumulation of penalties. When the interface stabilizes, the penalties will decrease exponentially. Through such penalty calculation, the interface can intelligently perceive its own state and take corresponding measures. Figure 1 is a chart that displays interface state events as they are perceived by upper layer routing protocols. This suppression algorithm is actually the application of route flap suppression algorithm (RFC2439) on network interface state.

1.4.2.1 Suppress Threshold

This value is the threshold configured for the accumulated penalty in order to identify interface flapping. When the value of accumulated penalty exceeds this threshold, the interface is considered flapping and will be dampened.

1.4.2.2 Half-Life Period

The half-life period refers to the time required for the penalty to decay to the half value when the interface is stable. It determines how fast the accumulated penalty can decay exponentially. The shorter the half-life period is, the faster the decaying and stable interface detection will be, but the sensitivity to flap detection will become lower. The default half-life period timer is 5 seconds.

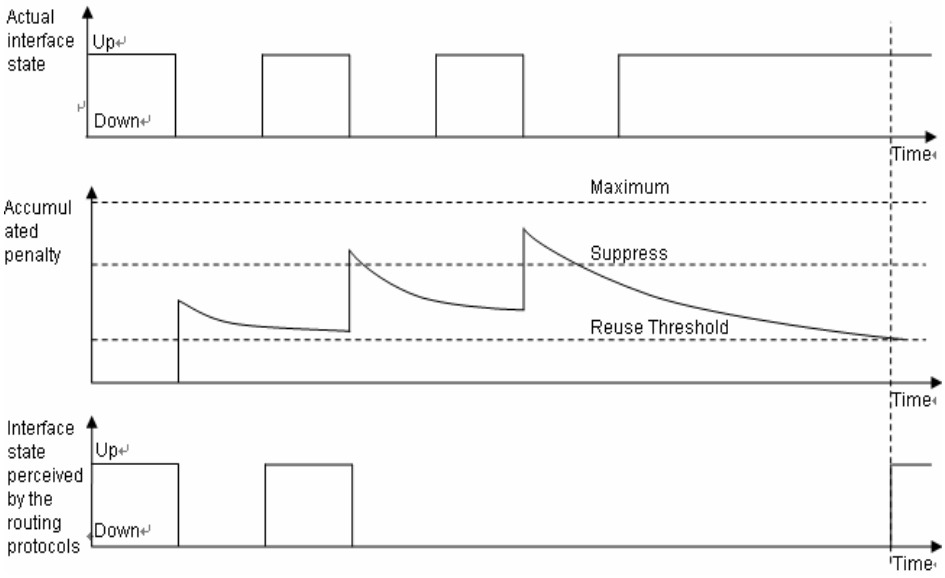


Fig 1 Interface state change event perceived by the routing protocols

1.4.2.3 Reuse Threshold

When the interface stops flapping and the penalty decreases to a certain degree (below the suppress threshold), the interface is considered having recovered to stable state and the interface is hence unsuppressed.

1.4.2.4 Maximum Suppress Time

To avoid that a long-flapping interface cannot be reused due to excessive penalty, the algorithm also defines a maximum suppress time. No matter how long the interface will flap, the duration of interface dampening will exceed this maximum suppress time.

1.4.3 Components Affected

When a layer-3 interface is not configured with dampening, or when an interface is configured with dampening but is not suppressed, the behavior of routing protocol or other layer-3 interface state related protocols will be the same as in normal situations. When an interface is configured with dampening and is suppressed, the upper layer protocol will consider the interface state as down; the routing tables and upper layer routing protocols are immune to any further state transitions of the interface until it is unsuppressed.

Caution

Dampening feature is currently not supported by the sub-interface and interface templates on router products.

1.4.4 Protocol Specification

This is no matching specification, but the suppression algorithm used by this feature is the same as the BGP route flap suppression algorithm described in RFC2439.

1.4.5 Configure Dampening Parameters

Configure as per the following steps:

Command	Function
DES-7200>**enable**	Enter privilege mode
DES-7200# **configure terminal**	Enter global configuration mode

DES-7200(config)# **interface** *type number*	Enter interface configuration mode
DES-7200(config-if)# **dampening** *half-life-period reuse-threshold suppress-threshold max-suppress* **restart** *restart-penalty*	Configure Dampening parameters on the specified interface *half-life-period*: configure the half-life period of suppression penalty *reuse-threshold*: configure the penalty threshold to unsuppress interface *suppress-threshold*: configure the penalty threshold to suppress interface *max-suppress*: configure maximum suppress time **restart** *restart-penalty*: configure the penalty value to start suppression
DES-7200(config-if)# **end**	Exit interface configuration mode and return to privilege mode

If only dampening is configured without any parameter, by default, the half-life period of suppression penalty is 5s, the penalty threshold to suppress interface is 1000, the penalty threshold to suppress interface is 2000 and the maximum suppress time is 20s.

To delete dampening configurations, execute "no dampening" command in the interface configuration mode.

Configuration example:

Configure interface event suppression on switch interface FastEthernet 0/0, with half-life period being 30 seconds, reuse threshold being 1500, suppression threshold being 10000, and maximum suppression time being 120 seconds.

```
DES-7200(config)# interface FastEthernet 0/0
DES-7200(config-if)#no switchport
DES-7200(config-if)# dampening 30 1500 10000 120
```

1.4.6 Display Dampening Information

The following commands are provided to display various configurations and status information. Their descriptions are given below:

Command	Function

show dampening interface	Display the overall statistics of dampening interface
show interface dampening	Display dampening details of all interfaces

1.5 Switch ECMP/WCMP Policy

In the switch, when the hardware forwards and stores ECMP/WCMP routes, load balancing policy is also involved. When the route has multiple next hops, the hardware can select a next hop according to the policy set. The switch will select different fields of the packets as the keyword according to our settings, and send them to the hash as input (there are two algorithms available) to select the appropriate hop. The appropriate packet characteristic fields and hash algorithm means more balanced traffic on the egress direction.

Note

Use the **maximum-paths** command to set the maximum equivalent route number.

1.5.1 Selecting Hash Keyword

you can set the hash keyword to the combination of source IP address, destination IP address, TCP/UDP port number, and user-define (UDF). UDF is a value in the range of 1 to 128 used as the seed value for hash calculation. Among various keywords, SIP is required, while others are optional. Various possible combinations are listed as below:

- SIP
- SIP & DIP
- SIP & TCP/UDP port
- SIP & UDF
- SIP, DIP & TCP/UDP port
- SIP, DIP & UDF
- SIP& TCP/UDP port & UDF
- SIP & DIP & TCP/UDP port & UDF

The default keyword has only SIP and is not configurable. That is, the HASH keyword is source IP at any time.

1.5.2 Selecting the Hash Algorithm

There are two hash algorithms available:

- CRC32_Upper Select the upper bits of the crc32 to determine the next hop
- CRC32_Lower Select the lower bits of the crc32 to determine the next hop

These two kinds of algorithms have different effects for different types of packets. For example, the CRC32_Upper has a good effect on the IP addresses that have the same upper bits but different lower bits. On the other hand, the CRC32_Upper has a good effect on the IP addresses that have the same lower bits but different higher bits.

The default hash algorithm is CRC32_Upper.

1.5.3 Configuration Commands

Command	Function
DES-7200(config)**# ip ref ecmp load-balance** {[**crc32_lower | crc32_upper**] [**dip**] [**port**] [**udf** *number*]}	Use any combination of DIP, Port and UDF to generate a key. And select CRC32_Lower or CRC32_Upper as a Hash algorithm.
DES-7200(config)**# no ip ref ecmp load-balance** {[**crc32_lower | crc32 upper**] [**dip**] [**port**] [**udf** *number*]}	The **no** command will use the keyword stored by the system minus the keyword carried by the **no** command as part of the Key. For example, the keyword stored by the system is SIP & DIP & Port. After the **no ip ref ecmp route dip port** command is executed, the component of the Key is only the SIP. If the member following the **no** command is not in the setting stored by the system, this command works well.

Note

If the existent IPv6 route is equivalent or inequivalent, which may be configured statically, or learned by the IPv6 dynamic routing protocol), the above configurations are valid for the IPv6 packet path selection.

The following configures the hash algorithm as CRC32_Lower, and selects the key of the packet as SIP & DIP:

```
DES-7200(config)# ip ref ecmp load-balance crc32_lower dip
```

1.6 Configuration Examples

1.6.1 Example of Route-map

The route map can be configured very flexibly to be used on the route redistribution and policy-based routing. No matter how the route map is used, the configuration principle is the same, except that different command sets are used. Even if it is used on the route redistribution, different routing protocols can use different commands with the route map.

In the following example, the OSPF routing protocol redistributes only the RIP routes whose hops are 4. In the OSPF routing area, the type of the routes is external route type-1, the initial metric is 40, and the route tag is 40.

Configure OSPF

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# redistribute rip subnets route-map redrip
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
```

Configure the access control list

```
DES-7200(config)# access-list 20 permit 200.168.23.0
```

Configure the route map

```
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# match metric 4
DES-7200(config-route-map)# set metric 40
DES-7200(config-route-map)# set metric-type type-1
DES-7200(config-route-map)# set tag 40
```

In the following configuration example, the RIP routing protocol redistributes only the OSPF routes whose tag is and initial metric is 10.

Configure RIP

```
DES-7200(config)# router rip
DES-7200(config-router)# version 2
DES-7200(config-router)# redistribute ospf 1 route-map redospf
DES-7200(config-router)# network 200.168.23.0
```

Configure route map

```
DES-7200(config)# route-map redospf permit 10
DES-7200(config-route-map)# match tag 10
DES-7200(config-route-map)# set metric 10
```

In the following configuration example, the OSPF routing protocol redistributes the RIP routes. Since the unsupported rule for the route-map application has

been configured, after redistributing the route-map, the printed message prompts that the application not support the corresponding rule.

Configure route-map

```
DES-7200(config)# route-map redrip permit 10
DES-7200(config-route-map)# match length 1 3
DES-7200(config-route-map)# match route-type external
DES-7200(config-route-map)# set level backbone
```

Configure OSPF

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# redistribute rip subnets route-map redrip
% ospf redistribute rip not support match length
% ospf redistribute rip not support match route-type
% ospf redistribute rip not support set level backbone
```

1.6.2 Example of Static Route Redistribution

Configuration requirements

One router exchanges route information with other routers via the RIP. In addition, there are three static routes. The RIP is only allowed to redistribute two routes: 172.16.1.0/24 and 192.168.1.0/24.

Detailed configuration

This is a common distribution list-based route filtering configuration example in practice. Note that the metric is not specified for the routes to be redistributed in the following configuration. Since a static route will be redistributed,the RIP will automatically assign the metric. In the RIP configuration, the version must be specified and the route aggregation must be disabled for the access list allows the 172.16.1.0/24 route. To advertise the route, the RIP protocol must first support the classless route, and the route cannot be aggregated to the 172.16.0.0/16 network.

Configure the static route

```
DES-7200(config)# ip route 172.16.1.0 255.255.255.0 172.200.1.2
DES-7200(config)# ip route 192.168.1.0 255.255.255.0 172.200.1.2
DES-7200(config)# ip route 192.168.2.0 255.255.255.0 172.200.1.4
```

Configure RIP

```
DES-7200(config)# router rip
DES-7200(config-router)# version 2
DES-7200(config-router)# redistribute static
DES-7200(config-router)# network 192.168.34.0
DES-7200(config-router)# distribute-list 10 out static
```

```
DES-7200(config-router)# no auto-summary
```

Configure the extended ACL

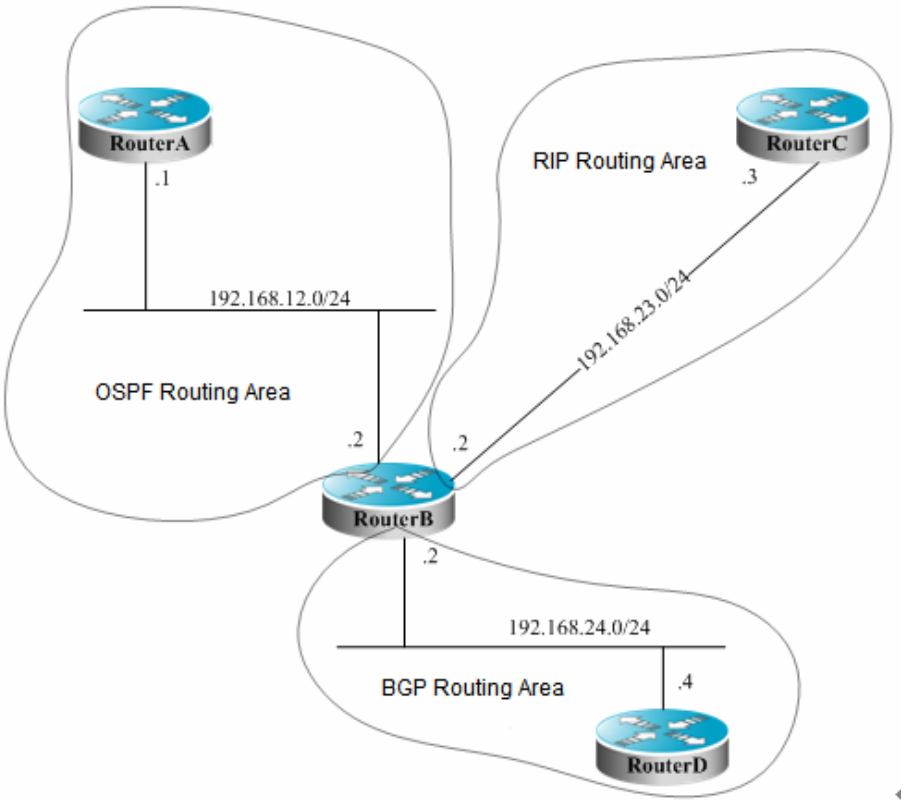
```
DES-7200(config)# access-list 10 permit 192.168.1.0
DES-7200(config)# access-list 10 permit 172.16.1.0
```

1.6.3 Example of Dynamic Route Protocol Redistribution

Configuration requirements

The connection among four routers is shown in the Figure-1. Router A belongs to the OSPF routing area, Router C belongs to the RIP routing area, Router D belongs to the BGP routing area and Router B is connected to three routing areas. Router A advertises the two routes of 192.168.10.0/24 and 192.168.100.1/32, Router C advertises the network routes of 200.168.3.0/24 and 200.168.30.0/24, and Router D advertises the network routes of 192.168.4.0/24、192.168.40.0/24.

Figure-1 Example of Dynamic Routing Protocol Redistribution



On Router B, the OSPF redistributes the RIP routes with the route Type-1, redistributes the BGP routes carrying with the community attribute 11:11. The RIP redistributes the 192.168.10.0/24 route in the OSPF routing area whose metric is 3, amd advertises a default route to the RIP routing area.

Detailed configuration

When the routing protocols redistribute routes among them, the simple route filtering can be controlled by the distribution list. However, different attributes must be set for different routes, and this is not possible for the distribution list, so the route map must be configured for control. The route map provides more control functions than the distribution list, and it is more complex to configure. Therefore, do not use the route map if possible for simple configuration of the router. The following example does not use the route map.

Router A configuration:

Configure the network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.10.1 255.255.255.0
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ip address 192.168.100.1 255.255.255.0
DES-7200(config-if)# no ip directed-broadcast
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.12.55 255.255.255.0
```

Configure the OSPF

```
DES-7200(config)# router ospf 12
DES-7200(config-router)# network 192.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.100.0 0.0.0.255 area 0
```

Router B configuration:

Configure the network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.12.5 255.255.255.0
DES-7200(config)# interface Serial 1/0
DES-7200(config-if)# ip address 192.168.23.2 255.255.255.0
```

#Configure the OSPF and set the redistribution route type

```
DES-7200(config)# router ospf 12
DES-7200(config-router)# redistribute rip metric 100 metric-type 1 subnets
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
```

#Configure the RIP and use the distribution list to filter the redistributed routes

```
DES-7200(config)# router rip
DES-7200(config-router)# redistribute ospf 12 metric 2
DES-7200(config-router)# network 192.168.23.0
DES-7200(config-router)# distribute-list 10 out ospf
DES-7200(config-router)# no auto-summary
```

Configure the BGP

```
DES-7200(config)# router bgp 2
DES-7200(config-router)# neighbor 192.168.24.4 remote-as 4
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 192.168.24.4 activate
DES-7200(config-router-af)# neighbor 192.168.24.4 send-community
```

Configure the route-map

```
DES-7200(config)# route-map ospfrm
DES-7200(config-route-map)# match community cl_110
```

Define the access list

```
DES-7200(config)# access-list 10 permit 192.168.10.0
```

Define the community list

```
DES-7200(config)# ip community-list standard cl_110 permit 11:11
```

Router C configuration:

Configure the network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.30.1 255.255.255.0
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7200(config)# interface serial 1/0
DES-7200(config-if)# ip address 192.168.23.3 255.255.255.0
```

Configure the RIP

```
DES-7200(config)# router rip
DES-7200(config-router)# network 192.168.23.0
DES-7200(config-router)# network 192.168.3.0
DES-7200(config-router)# network 192.168.30.0
```

Router D configuration:

Configure the network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.40.1 255.255.255.0
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.4.1 255.255.255.0
DES-7200(config)# interface serial 1/0
DES-7200(config-if)# ip address 192.168.24.4 255.255.255.0
```

Configure the BGP

```
DES-7200(config)# router bgp 4
```

```
DES-7200(config-router)# neighbor 192.168.24.2 remote-as 2
DES-7200(config-router)# redistribute connected route-map bgprm
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 192.168.24.2 activate
DES-7200(config-router-af)# neighbor 192.168.24.2 send-community
```

Configure the route-map

```
DES-7200(config)# route-map bgprm
DES-7200(config-route-map)# match community 22:22
```

OSPF routes found on router A:

```
O E1 192.168.30.0/24 [110/101] via 192.168.12.5, 00:04:07, FastEthernet0/1
O E1 192.168.3.0/24 [110/101] via 192.168.12.5, 00:04:07, FastEthernet0/1
```

RIP routes found on Router C:

```
R   192.168.10.0/24 [120/2] via 200.168.23.2, 00:00:00, Serial1/0
R   192.168.10.0/24 [120/2] via 200.168.23.2, 00:00:00, Serial1/0
```

1.6.4 Example of IP Event Dampening

Configuration Steps

1) Configure interface event suppression on switch interface FastEthernet 0/0, with half-life period being 30 seconds, reuse threshold being 1500, suppression threshold being 10000, and maximum suppression time being 120 seconds.

```
DES-7200(config)#interface FastEthernet 0/0
DES-7200(config-if)#no switchport
DES-7200(config-if)#dampening 30 1500 10000 100
```

2) Configure interface event suppression on switch interface FastEthernet 0/1, using default dampening parameters.

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#dampening
```

3) Configure interface event suppression on switch interface FastEthernet 0/1, with restart penalty being 500.

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#dampening 5 500 1000 20 restart 500
```

Verification

Execute **"show dampening interface"** to display information related to interface suppression, as shown in the following example:

```
DES-7200#show dampening interface
```

3 interfaces are configured with dampening.

No interface is being suppressed.

Execute **"show interface dampening"** to display the current dampening parameters and state details of interfaces configured IP Event Dampening

```
DES-7200#show interface dampening
FastEthernet 0/1
Flaps Penalty  Supp ReuseTm HalfL ReuseV SuppV MaxSTm  MaxP Restart
0       0   FALSE       0     5   1000   2000     20 16000       0
FastEthernet 0/2
Flaps Penalty  Supp ReuseTm HalfL ReuseV SuppV MaxSTm  MaxP Restart
0       0   FALSE       0     5   1000   2000     20 16000     500
FastEthernet 0/3
Flaps Penalty  Supp ReuseTm HalfL ReuseV SuppV MaxSTm  MaxP Restart
   0       0   FALSE       0     5   1000   2000     20 16000       0
```

2 RIP Configuration

2.1 RIP Overview

The RIP (Routing Information Protocol) is a relatively old routing protocol, which is widely used in small or homogeneous networks. The RIP uses the distance-vector algorithm, and so is a distance-vector protocol. The RIPv1 is defined in RFC 1058 and the RIPv2 is defined in RFC 2453.

The RIP exchanges the routing information by using the UDP packets, with the UDP port number to be 520. Usually, RIPv1 packets are broadcast packets, while RIPv2 packets are multicast packets with the multicast address of 224.0.0.9. The RIP sends the update packet at the interval of 30 seconds. If the device has not received the route update packets from the peer within 180 seconds, it will mark all the routes from that device unreachable. After that, the device will delete these routes from its routing table if it still has not received any update packets from the peer within 120s.

The RIP measures the distance to the destination in hop, known as route metric. As specified in the RIP, Zero hop exists when the router directly connects to the network. One hop exists when the router connects to the network through one device and so on. Up to 16 hops are supported in a network.

The RIP-enabled device can learn the default routes from the neighbors or generate its own default route. When any of the following condition is met, DES-7200 product will generate the default route and advertise it to its neighbors by using the **default-information originate** command:

- IP Default-network is configured.
- The default routes or static default routes learnt by the routing protocol are imported into the RIP protocol.

The RIP-enabled device will send the update packets to the interface of the network it connects. If the network is not associated with the RIP routing process, the interface will not advertise any update packets. The RIP is available in two versions: RIPv1 and RIPv2. The RIPv2 supports plain-text authentication, MD5 cryptographic text and variable length subnet mask.

DES-7200 RIP offers Split Horizon to avoid a loop.

2.2 RIP Configuration Task

2.2.1 Creating the RIP Routing Process

For the router to run the RIP, you must first create the RIP routing process and define the network associated with the RIP routing process.

To create the RIP routing process, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)**# router rip**	Create the RIP routing process.
DES-7200(config-router)**# network** *network-number wildcard*	Define the associated network.

You can configure the *network-number* and *wildcard* parameters at the same time to enable the network segments within the configured address range to run RIP.

Note

There are two meanings for the associated network defined by the **network** command:

1. The RIP only notifies the route information of the associated network.

2. The RIP only notifies and receives route update messages through the interfaces of the associated network.

2.2.2 Advertising the RIP Route Update Message in Unicast Form

The RIP is usually a broadcast or multicast protocol. If the RIP route message needs to be transmitted across the non-broadcast networks, you need to configure the router to advertise the RIP route update message in unicast form.

To advertise the RIP route update message in unicast form, execute the following commands in the RIP routing process configuration mode:

Command	Function
DES-7200(conf-router)**# neighbor** *ip-address*	Advertise the RIP update message in unicast form.

This command allows you to advertise the RIP route update message on a port, or disable advertising the broadcast route update messageon a port. You need to configure the **passive-interface** command in the routing process configuration mode. For related description on the restriction of route message advertisement, see Section *Route Filtering Configuration* of *Protocol Independent Configuration* chapter.

Note

In FR or X.25 environment, if the **broadcast** keyword is specified for address mapping, the **neighbor** command is not necessary, which is mainly used for reducing broadcast packets and filtering routes.

2.2.3 Configuring Split Horizon

Split horizon can be used to avoid loop in the environment where multiple devices running distance-vectortype routing protocols connect to a network in which IP packets are broadcasted. Split horizon can prevent the router from advertising some route information through the port from which it learns such information. This optimizes the route information exchange among multiple routers.

However, split horizon may cause the failure of some routers to learn all the routes in a non-broadcast multi-access network (for example, frame relay, X.25). In this case, you may need to disable split horizon. If a port is configured with the secondary IP address, you also need to pay attention to the split horizon problem.

To enable or disable split horizon, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **no ip split-horizon**	Disable split horizon.
DES-7200(config-if)# **ip split-horizon**	Enable split horizon.

By default, split horizon is enabled on all interfaces.

2.2.4 Defining the RIP Version

DES-7200 product supports RIP version 1 and version 2, where RIPv2 supports authentication, key management, route convergence, CIDR and VLSMs. For the information about the key management and VLSMs, see the *IP Routing Protocol Independent Feature Configuration* chapter.

By default, DES-7200 product can receive RIPv1 and RIPv2 packets, but it can only send RIPv1 packets. You can configure it to receive and send only RIPv1 packets or RIPv2 packets.

To receive and send the packets of a specific version, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **version** {**1** | **2**}	Defining the RIP Version.

The above command allows the software to receive or send only the packets of the specified version. If needed, you can modify the default setting of every port.

To configure a port to send only the packets of a specific version, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip rip send version 1**	Specify to send the packets of only RIPv1
DES-7200(config-if)# **ip rip send version 2**	Send the packets of only RIPv2.
DES-7200(config-if)# **ip rip send version 1 2**	Send the packets of RIPv1 and RIPv2.

To configure a port to receive only the packets of a specific version, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip rip receive version 1**	Receive the packets of only RIPv1.
DES-7200(config-if)# **ip rip receive version 2**	Receive the packets of only RIPv2.
DES-7200(config-if)# **ip rip receive version 1 2**	Receive the packets of RIPv1 and RIPv2.

2.2.5 Configuring Route Aggregation

The automatic route aggregation of the RIP means that the routes of subnets are automatically aggregated into the routes of a classful network when they pass through the border of the classful network. By default, the RIPv2 will automatically perform route aggregation, while the RIPv1 does not support this feature.

The automatic route aggregation function of the RIPv2 enhances the scalability and effectiveness of the network. If there are any aggregated routes, the sub-routes contained in them cannot be seen in the routing table. This greatly reduces the size of the routing table.

It is more efficient to advertise the aggregated routes than the separated routes. There are the following factors:

- Aggregated routes will be handled first when you search the RIP database.
- Any sub-routes will be ignored will you search the RIP database, and thus reducing the processing time.

Sometimes, you want to learn the specific sub-net routes rather than only viewing the aggregated routes. In this case,you should disable the automatic route aggregation function.

To configure automatic route aggregation, execute the following commands in the

RIP routing process mode:

Command	Function
DES-7200(config-router)# **no auto-summary**	Disable automatic route aggregation.
DES-7200(config-router)# **auto-summary**	Enable automatic route aggregation.

After the automatic route aggregation is disabled, you can configure the route aggregation of IP addresses or subnets on an interface by executing the following command in the interface mode:

Command	Function
DES-7200(config-if)# **ip summary-address rip** *ip-address ip-network-mask*	Enable route aggregation on the interface.
DES-7200(config-if)# **no ip summary-address rip** *ip-address ip-network-mask*	Disable route aggregation on the interface.

2.2.6 Configuring RIP Authentication

RIPv1 does not support authentication. If the router is configured with the RIPv2, you can configure authentication on the appropriate interface.

Two RIP authentication modes are supported: plain-text authentication and MD5 authentication. The default is plain-text authentication.

In plain-text authentication mode, you can run the **ip rip authentication text-password** command to configure the plain-text authentication password or associate the key chain to obtain the plain-text authentication password. The latter takes precedence over the former.

In MD5 authenticaiton mode, you should associate the key chain for MD5 authentication.

For the plain-text authentication, no authentication action occurs if the plain-text authentication password string or the key chain association is not configured, or the key chain is not configured although it has been associated. Similarly, for the MD5 authentication, no authentication action occurs if the key chain association is not configured, or the key chain is not configured although it has been associated.

To configure RIP authentication, execute the following commands in the interface configuration mode:

Command	Function

Command	Function
DES-7200(config-if)# **ip rip authentication mode** {**text** | **md5**}	Configure the RIP authentication on the interface. Text: plain-text authentication Md5: MS5 authentication
DES-7200(config-if)# **ip rip authentication text-password** *password-string*	Configure the plain-text authentication password s in the length of 1-16 bytes.
DES-7200(config-if)# **ip rip authentication key-chain** *key-chain-name*	Configure the authentication using key chain.

2.2.7 Adjusting the RIP Timer

The RIP provides the timer adjustment function, which allows you to adjust the timer so that the RIP routing protocol can run in a better way. You can adjust the following timers:

Route update timer: It defines the interval in seconds for the router to send the RIP update packets;

Route invalid timer: It defines the time in seconds after which the routes in the routing table will become invalid if not updated;

Route clearing timer: It defines the time in seconds after which the routes in the routing table will be cleared;

By adjusting the above timers, you can accelerate the aggregation and fault recovery of the routing protocol. To adjust the RIP timers, execute the following commands in the RIP routing process configuration mode:

Command	Function
DES-7200(config-router)# **timers basci** *update invalid flush*	Adjust the RIP timers.

By default, the update interval is 30 seconds, the invalid period is 180 seconds, and the clearing (flush) period is 120 seconds.

Note

The routers connected in the same network must have the same RIP timers.

2.2.8 Configuring the RIP Route Source IP Address Validation

By default, the RIP will validate the source addresses of the incoming route update packets. The RIP will discard the packets from invalid source IP address. Whether a source IP address is valid or not depends on if the source IP address is in the same network as the IP address of the interface. No validation will be performed on the interface of no IP address.

To configure route source IP address validation, execute the following commands in the RIP routing process configuration mode:

Command	Function
DES-7200(config-router)# **no validate-update-source**	Disable the source IP address validation.
DES-7200(config-router)# **validate-update-source**	Enable the source IP address validation.

2.2.9 Configuring RIP Interface Status Control

In some case, it is necessary to configure the RIP flexibly. If you only need to enable the device to learn the RIP routes rather than RIP route advertisement, you can configure the passive interface. Or, if you need to configure the status of some interface individually, you can use a command to control the sending or receiving of the RIP packets on an interface.

To configure some interface as the passive mode, execute the following command in the RIP route processing configuration mode:

Command	Function
DES-7200(config-router)# **passive-interface {default** | *interface-type interface-num*}	Set the interface to passive.
DES-7200(config-router)**#no passive-interface {default** | interface-type interface-num}	Remove the configuration.

Note

The passive interface responds the non-RIP requests (such as the route diagnosis program) rather than the RIP requests, because these request programs hope to understand the routes of all devices.

To disable or allow some interface to receive the RIP message, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# no ip rip receive enable	Disable the interface to receive the RIP message.
DES-7200(config-if)# **ip rip receive enable**	Allow the interface to receive the RIP message.

To disable or allow some interface to send the RIP message, execute the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **no ip rip send enable**	Disable the interface to send the RIP message.
DES-7200(config-if)# **ip rip send enable**	Allow the interface to send the RIP message.

2.2.10 Configuring the Default Route Advertisement on the Interface

Use the following command to generate a default route (0.0.0.0/0) in the update message on a specified interface in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip rip default-information originate** [**metric** *metric-value*]	Advertise the default route and other routes.
DES-7200(config-if)# **no ip rip default-information**	Cancel the default route advertisement on the interface.

In the interface configuration mode, use the following command to generate a default route (0.0.0.0/0) in the update message on a specified interface, and enable only advertising this default route on this interface.

Command	Function
DES-7200(config-if)# **ip rip default-information only** [**metric** *metric-value*]	Advertise the default route only.
DES-7200(config-if)# **no ip rip default-information**	Cancel the default route advertisement on the interface.

Note

With both the **ip rip default-information** command on the interface and the **default-information originate** command in the RIP process configured, only the default route configured on the interface is advertised.

2.2.11 Configuring the Super Network Route Advertisement on the Interface

A super network router is a route whose mask length is less than its natural mask length, for instance, 80.0.0.0/6. 80.0.0.0/6 belongs to Class-A network, but its natural mask legnth is 8, it is a super netowrk route.

When RIPv1-enabled device monitores the response message form RIPv2-enabled device, it will learn wrong route upon receiving a super network route for RIPv1 ignors the mask of the route message. In this case, RIPv2-enabled device needs to disable advertising super network route on its interface.

Use the following command to disable the super network route advertisement in the interface configuration mode:

Command	Function
DES-7200(config-if)**#no ip rip send supernet-routes**	Disable advertising the super network route.
DES-7200(config-if)# **ip rip send supernet-routes**	Enable advertising the super network route.

- Only RIPv1 packets rather than RIPv2 packets and super network routes are received on an interface.
- Super network routes are permitted to be received when RIPv2 packets are allowed to be received on an interface.
- Super network routes are not sent when RIPv1 packets are sent on an interface.

Note

- Super network routes are permitted to be sent by default when RIPv2 packets are allowed to be sent on an interface.
- The **no rip rip send supernet-routes** command prohibits sending super network routes.
- Auto aggregation takes no effect for super network routes.
- When route aggregation is configured on an interface (by the **ip summary rip** command), super network routes are not supported.

2.2.12 Configuring RIP VRF

The RIP supports VRFs. Multiple RIP instances can be created to manage the corresponding VRFs in the RIP process. By default, there is only one RIP instance in the RIP process, which is used to manage the global routing table. After a VRF is created, you can manage the routing table of the VRF by creating a new RIP instance.

Execute the **address-family** command to enter the address family configuration mode (with the prompt (config-router-af)#). When you specify the VRF associated with the sub mode at the first time, the RIP will create the a RIP instance corresponding to the VRF. Under this mode, you can configure the RIP route information of the VRF in the same way as that in global route configuration mode.

To exit the address family configuration sub mode and return to the route configuration mode, execute the **exit-address-family** command or the **exit** command.

To configure the RIP instance managng the VRF, execute the following command in the RIP route processing configuration mode:

Command	Function
DES-7200(config-router)# **address-family ipv4 vrf** *vrf-name*	Create the RIP instance managing the VRF.
DES-7200(config-router)#**no address-family ipv4 vrf** *vrf-name*	Remove the RIP instance managing the VRF.

2.2.13 Configuring RIP BFD

For details on BFD configuration, refer to *BFD Configuration Guide*.

2.2.14 Configuring Triggered RIP

Triggered RIP (TRIP) is a RIP extension on WAN (Wide Area Network), and is mainly used on the on-demand link.

When TRIP is enabled, RIP protocol will no longer send periodic route updates but only send route updates to WAN interface in the following cases:

- When route update request message is received.
- When RIP routing information has changed.
- When interface state has changed.
- Router restart.

Since the periodic RIP update is canceled, an acknowledgement and retransmission mechanism is required to guarantee successful updates transmission on WAN. RIP uses three new types of message which are identified by the value of the command field in RIP header:

- Update request (Type-9): Requests the peer device to send the routing information needed.
- Update response (Type-10): Contains the route updates requested by the peer device.
- Update Acknowledge (Type-11): Acknowledges the received update responses, indicating that the route updates sent by peer device have been received.

Caution

1. This feature can be used in the following cases: 1) the interface is connected to only one neighbor; 2) the interface is connected to multiple neighbors using unicast communication mode. It is suggested to enable this feature on PPP, frame relay, X.25 and similar link layer protocols.

2. It is suggested to enable split horizon with poisoned reverse on TRIP-enabled interface, or else there may be residual invalid routing information.

3. It shall be guaranteed that the feature is enabled on all routers on the same link, or else the feature may fail and routing information cannot be exchanged properly.

4. This feature cannot be used together with BFD for RIP;

5. When this feature is enabled, make sure the RIP configurations on both ends of the link are identical, such as RIP authentication, version of RIP protocol supported by the interface and etc.

To enable or disable this feature, execute the following commands in interface configuration mode:

Command	Function
DES-7200(config-if)# **ip rip triggered**	Enable Triggered RIP.
DES-7200(config-if)# **no ip rip triggered**	Disable Triggered RIP.

2.2.15 Configuring RIP Graceful Restart

RIP Graceful Restart (GR) guarantees non-stop data forwarding during the process of protocol restart. When RIP GR is enabled on the router, the forwarding table will be maintained during the process of RIP restart, and requests will be sent to neighbors to relearn routes in order to complete route re-convergence within the period of graceful restart. Upon expiration of grace period, GR will exit and forwarding table entries will be updated and advertised to neighbors.

Grace period is the maximum duration from RIP GR execution to RIP GR completion. During this period, the forwarding table will be maintained and RIP route recovery will be executed in order to restore RIP to the state before graceful restart. Upon expiration of grace period, RIP will exit GR state and execute common RIP operations.

graceful-restart grace-period Allows the user to explicitly change the restart period. Please note that GR must be completed within the RIP invalid timer and one RIP route update cycle is completed. If this value is not properly configured, non-stop data forwarding cannot be guaranteed during graceful restart. For example: if the grace period is larger than the invalid timer of neighbor and GR is

not completed within such invalid timer, the neighbor's routes won't be sent upon expiration of invalid timer, thus causing the interruption of data forwarding. Therefore, unless otherwise needed, it is not suggested to adjust the grace period. If grace period is adjusted, please refer to the configuration of "timers basic" command and make sure the grace period is larger than the update timer and smaller than the invalid timer.

To enable or disable this feature, execute the following commands in RIP routing process configuration mode:

Command	Function
DES-7200(config-router)# **graceful-restart** [**grace-period** *grace-period*]	Enable RIP Graceful Restart.
DES-7200(config-router)# **no graceful-restart** [**grace-period**]	Disable RIP Graceful Restart.

2.3 RIP configuration examples

2.3.1 Configuring RIP Route and Defining RIP Version

Network Topology

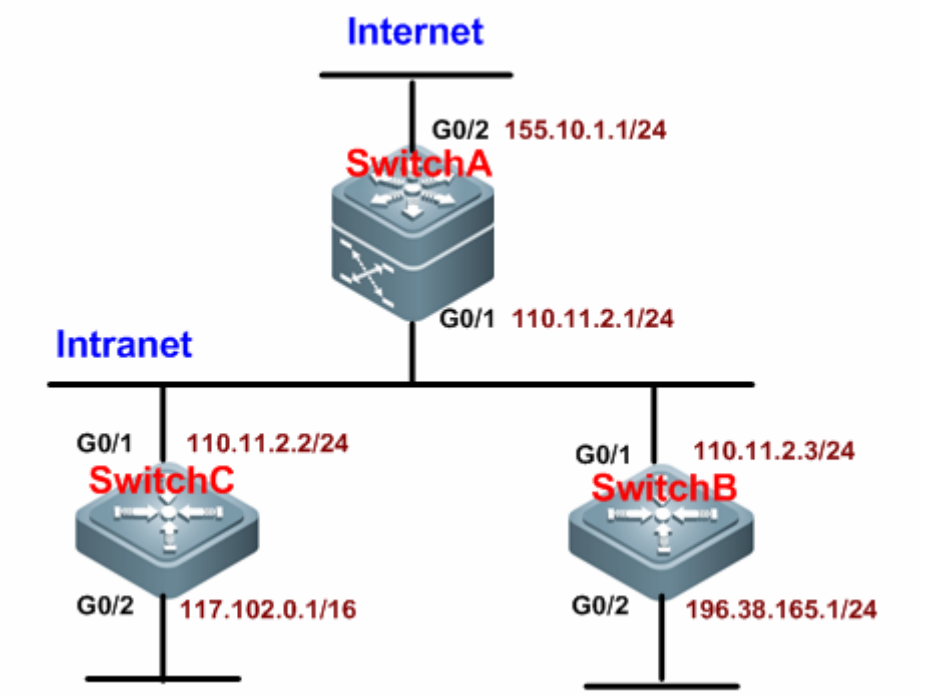


Figure1 Configuring RIP routing and RIP version

Networking Requirements

A small-sized company runs a small office network, and requires network layer

intercommunication can be realized between any two nodes. Networking requirements are shown below:

- The devices shall be able to adapt to the changes in network topology, so as to reduce the workload of manual maintenance;
- Route updates can carry subnet mask;
- Switch A only receives the routing information from external network, but will not advertise routing information of internal network.
- RIP information can be exchanged between Switch A, Switch B and Switch C, so that internal hosts can access Internet.

Configuration Tips

- According to user's requirements and network environment, RIPv2 routing protocol shall be selected to achieve user network intercommunication;
- To allow Switch A to receive routing information sent from external network without advertising the routing information of internal network, the G0/2 port of Switch A shall be configured as a passive interface.

Configuration Steps

Switch A

! Configure the IP address of the corresponding port on Switch A

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 110.11.2.1 255.255.255.0
DES-7200(config-if)#exit
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 155.10.1.1 255.255.255.0
```

! Create RIP routing process

```
DES-7200(config)#router rip
```

! Configure RIP version 2

```
DES-7200(config-router)#version 2
```

! Configure G0/2 as a passive interface

```
DES-7200(config-router)#passive-interface gigabitEthernet 0/2
```

! Disable automatic route summarization

```
DES-7200(config-router)#no auto-summary
```

! Specify the associated network

```
DES-7200(config-router)#network 110.11.2.0 255.255.255.0
DES-7200(config-router)#network 155.10.1.0
```

Switch B

! Configure the IP address of the corresponding port on Switch B

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 110.11.2.2 255.255.255.0
DES-7200(config-if)#exit
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 196.38.165.1 255.255.255.0
DES-7200(config-if)#exit
```

! Create RIP routing process

```
DES-7200(config)#router rip
```

! Configure RIP version 2

```
DES-7200(config-router)#version 2
```

! Disable automatic route summarization

```
DES-7200(config-router)#no auto-summary
```

! Specify the associated network

```
DES-7200(config-router)#network 110.11.2.0
DES-7200(config-router)#network 196.38.165.0
```

Switch C

! Configure the IP address of the corresponding port on Switch C

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 110.11.2.3 255.255.255.0
DES-7200(config-if)#exit
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 117.102.0.1 255.255.0.0
DES-7200(config-if)#exit
```

! Create RIP routing process

```
DES-7200(config)#router rip
```

! Configure RIP version 2

```
DES-7200(config-router)#version 2
```

! Disable automatic route summarization

```
DES-7200(config-router)#no auto-summary
```

! Specify the associated network

```
DES-7200(config-router)#network 110.11.2.0
DES-7200(config-router)#network 117.102.0.0
```

Verification

Display the routing table of each device;

1. View routing table on Switch A, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.1/32 is local host.
R 117.102.0.0/16 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
C    155.10.1.0/24 is directly connected, GigabitEthernet 0/2
C    155.10.1.1/32 is local host.
C    192.168.217.0/24 is directly connected, VLAN 1
C    192.168.217.233/32 is local host.
R  196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

2. View routing table on Switch B, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.2/32 is local host.
R 155.10.1.0/24 [120/1] via 110.11.2.1, 00:15:21, GigabitEthernet 0/1
C    196.38.165.0/24 is directly connected, GigabitEthernet 0/2
C    196.38.165.1/32 is local host.
R 117.102.0.0/16 [120/1] via 110.11.2.2, 00:00:47, GigabitEthernet 0/1
```

3. View routing table on Switch C, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    110.11.2.0/24 is directly connected, GigabitEthernet 0/1
C    110.11.2.3/32 is local host.
C    117.102.0.0/16 is directly connected, GigabitEthernet 0/2
C    117.102.0.1/32 is local host.
R  155.10.1.0/24 [120/1] via 110.11.2.1, 00:20:55, GigabitEthernet 0/1
R  196.38.165.0/24 [120/1] via 110.11.2.3, 00:19:18, GigabitEthernet 0/1
```

2.3.2 RIP Split Horizon

Network Topology

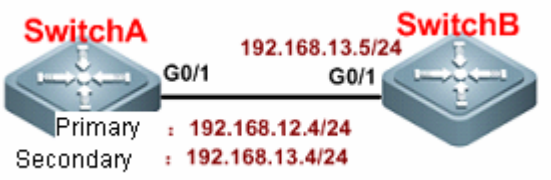


Figure 2 Topological diagram for RIP split horizon

Networking Requirements

There are two devices on the network. Switch A is configured with a secondary

address.

The following requirements shall be met:

- RIP routing protocol is run on both devices;
- Switch B can learn the routes of network segment 192.168.12.0/24.

Configuration Tips

To meet the above requirements, the following configurations shall be made:

- RIPv2 routing protocol is run on both devices;
- Split horizon shall be disabled on SwitchA (by default, split horizon is enabled on all interfaces), or else SwitchA won't advertise network segment 192.168.12.0 to SwitchB.

Configuration Steps

 # SwitchA

! Configure Ethernet interface

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#no switchport
DES-7200(config-if-GigabitEthernet 0/1)#ip address 192.168.12.4 255.255.255.0
DES-7200(config-if-GigabitEthernet 0/1)#ip address 192.168.13.4 255.255.255.0
secondary
```

! Disable split horizon

```
DES-7200(config-if-GigabitEthernet 0/1)#no ip rip split-horizon
```

! Configure RIP routing protocol

```
DES-7200(config)#route rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.12.0
DES-7200(config-router)#network 192.168.13.0
```

! Disable automatic route summarization

```
DES-7200(config-router)#no auto-summary
```

 # SwitchB

! Configure Ethernet interface

```
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#no switchport
DES-7200(config-if-GigabitEthernet 0/1)#ip address 192.168.13.5 255.255.255.0
```

! Configure RIP routing protocol

```
DES-7200(config)#route rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.13.0
```

Verification

View the routing table on SwitchB before and after disabling split horizon

1. Before split horizon is disabled, view the routing table on SwitchB, as shown below:

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C    192.168.13.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.13.5/32 is local host.
```

2. After split horizon is disabled, view the routing table on SwitchB, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
R    192.168.12.0/24 [120/1] via 192.168.13.4, 00:00:10, GigabitEthernet 0/1
C    192.168.13.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.13.5/32 is local host.
```

2.3.3 RIP Unicast Update

Network Topology

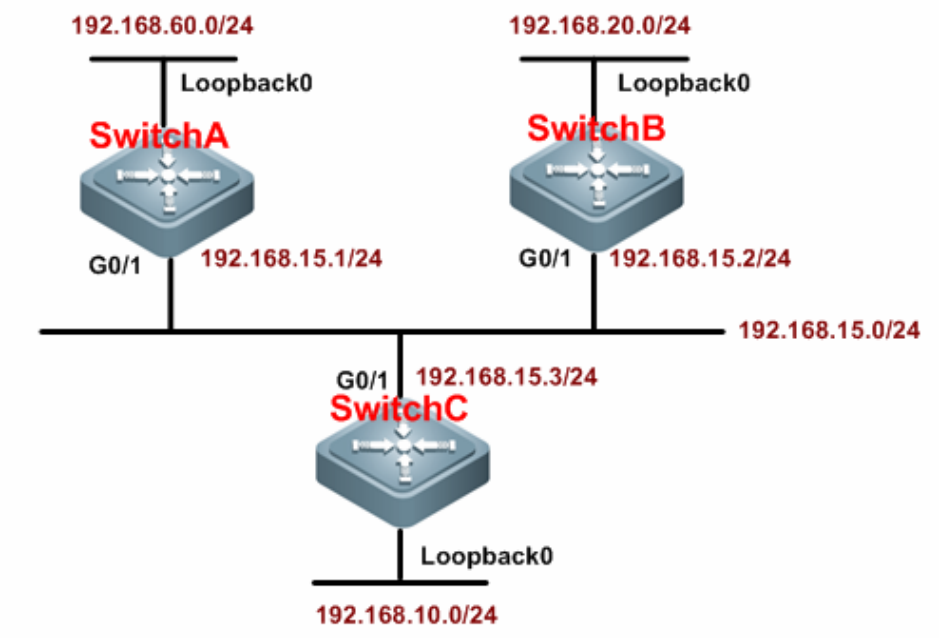


Figure3 Topological diagram for RIP unicast update

Networking Requirements

As shown below, three devices are connected to the LAN and running RIP routing protocol.

- SwitchA can learn the routes advertised by SwitchB and SwitchC;
- SwitchC can learn the routes advertised by SwitchA and SwitchB;
- SwitchB cannot learn the routes advertised by SwitchC.

Configuration Tips

To meet the above configuration requirements, RIP unicast must be configured on SwitchC. Insert the command of "neighbor" during the RIP configuration of SwitchC, so that RIP protocol can send advertisements to the interface of SwitchA in unicast mode. Execute "passive-interface" command on G0/1 interface of SwitchC to avoid route broadcast on this link.

Configuration Steps

 # Switch A

! Configure the IP address of corresponding interface

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.15.1 255.255.255.0
DES-7200(config-if)#exit
```

```
DES-7200(config)#interface Loopback 0
DES-7200(config-if)#ip address 192.168.60.1 255.255.255.0
DES-7200(config-if)#exit
```

! Create RIP routing process

```
DES-7200(config)#router rip
```

! Specify the associated network

```
DES-7200(config-router)#network 192.168.60.0
DES-7200(config-router)#network 192.168.15.0
```

 # Switch B

! Configure the IP address of corresponding interface

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.15.2 255.255.255.0
DES-7200(config-if)#exit
DES-7200(config)#interface Loopback 0
DES-7200(config-if)#ip address 192.168.20.1 255.255.255.0
DES-7200(config-if)#exit
```

! Create RIP routing process

```
DES-7200(config)#router rip
```

! Specify the associated network

```
DES-7200(config-router)#network 192.168.20.0
DES-7200(config-router)#network 192.168.15.0
```

 # Switch C

! Configure the IP address of corresponding interface

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.15.3 255.255.255.0
DES-7200(config-if)#exit
DES-7200(config)#interface Loopback 0
DES-7200(config-if)#ip address 192.168.10.1 255.255.255.0
DES-7200(config-if)#exit
```

! Create RIP routing process

```
DES-7200(config)#router rip
```

! Specify the associated network

```
DES-7200(config-router)#network 192.168.15.0
DES-7200(config-router)#network 192.168.10.0
```

! Configure G0/1 as a passive interface

```
DES-7200(config-router)#passive-interface gigabitEthernet 0/1
```

! Enable unicast update

```
DES-7200(config-router)#neighbor 192.168.15.1
```

Verification

Display the routing table of each device (mainly the routing information on SwitchC and SwitchE):

1. View the routing table on SwitchB, as shown below:

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.20.0/24 is directly connected, Loopback 0
C    192.168.20.1/32 is local host.
C    192.168.15.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.15.2/32 is local host.
R 192.168.60.0/24 [120/1] via 192.168.15.1, 00:15:21, GigabitEthernet 0/1
```

2. View the routing table on SwitchC, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
```

```
Gateway of last resort is no set
C    192.168.10.0 is directly connected, Loopback 0
C    192.168.10.1/32 is local host.
R 192.168.60.0/24 [120/1] via 192.168.15.1, 00:15:21, GigabitEthernet 0/1
C    192.168.15.0/24 is directly connected, GigabitEthernet 0/1
C    192.168.15.3/32 is local host.
R 192.168.20.0 [120/1] via 192.168.15.2, 00:00:47, GigabitEthernet 0/1
```

2.3.4 RIP Authentication

Network Topology

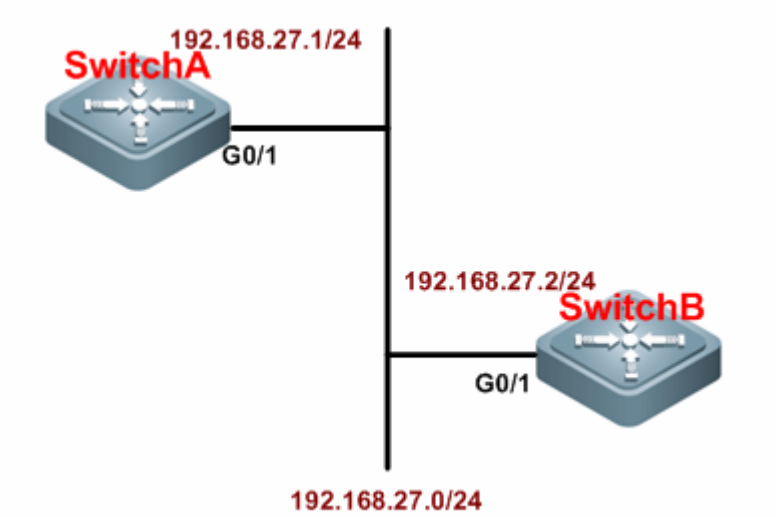


Figure4 Topological diagram for RIP authentication

Networking Requirements

Interconnected through Ethernet, two devices run RIP routing protocol and adopt MD5 authentication. The following requirements must be met:

- The authentication key for Switch A to send RIP packets is "Hello", and Switch A can receive RIP packets with authentication key being "Hello" and "World";
- The authentication key for Switch B to send RIP packets is "World", and Switch B can receive RIP packets with authentication key being "Hello" and "World";
- The first key is used from October 1, 2010 4:30pm for 12 hours (43200s)
- The second key will take effect as of October 2, 2010 4:00am.

Configuration Tips

Authentication is not supported in RIPv1. If RIPv2 routing protocol is configured on the device, the authentication feature can then be configured on the

corresponding interface. The key-string specifies the key set that can be used by this interface. If key-string is not configured, no authentication will take place. Therefore, before configuring authentication, the key chain and the associated key string must be configured first.

There are two RIP authentication modes: plain text and MD5, while plain text is the default authentication mode.

- The authentication key for sending RIP packets must be configured with the first key on keychain;
- When configuring the authentication key that can be received, simply configure any key on the keychain.

Configuration Steps

 # SwitchA:

! Configure the IP address of Ethernet interface

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.27.1 255.255.255.0
DES-7200(config-if)#exit
```

! Configure the key chain named "DES-7200"

```
DES-7200(config)#key chain DES-7200
```

! Configure the first key of "Key 1", which contains the key-string of "Hello", and configure the corresponding time period needed

```
DES-7200(config-keychain)#key 1
DES-7200(config-keychain-key)#key-string Hello
DES-7200(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2010 duration
43200
DES-7200(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2010 duration 43200
DES-7200(config-keychain-key)#exit
```

! Configure the second key of "Key 2", which contains the key-string of "World", and configure the corresponding time period needed

```
DES-7200(config-keychain)#key 2
DES-7200(config-keychain-key)#key-string World
DES-7200(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 2010 infinite
//Beginning time that the key is valid to be received
DES-7200(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2010 infinite
//Beginning time that the key is valid to be sent
DES-7200(config-keychain-key)#end
```

! Configure G0/1 to use MD5 authentication key to authenticate the update messages sent from SwitchB

```
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#ip rip authentication key-chain DES-7200
DES-7200(config-if)#ip rip authentication mode md5
DES-7200(config-if)#exit
```

! Configure RIP routing protocol

```
DES-7200(config)#router rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.27.0
```

SwitchB:

! Configure the IP address of Ethernet interface

```
DES-7200>enable
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.27.2 255.255.255.0
DES-7200(config-if)#exit
```

! Configure key chain

```
DES-7200(config)#key chain DES-7200 //The name of key chain is only valid on
the local device. You can also use other names.
```

! Configure the first key of "Key 1", which contains the key-string of "Hello", and configure the corresponding time period needed

```
DES-7200(config-keychain)#key 1
DES-7200(config-keychain-key)#key-string Hello
DES-7200(config-keychain-key)#accept-lifetime 16:30:00 Oct 1 2010 duration
43200
DES-7200(config-keychain-key)#send-lifetime 16:30:00 Oct 1 2010 duration
43200
DES-7200(config-keychain-key)#exit
```

! Configure the second key of "Key 2", which contains the key-string of "World", and configure the corresponding time period needed

```
DES-7200(config-keychain)#key 2
DES-7200(config-keychain-key)#key-string World
DES-7200(config-keychain-key)#accept-lifetime 04:00:00 Oct 2 010 infinite
DES-7200(config-keychain-key)#send-lifetime 04:00:00 Oct 2 2010 infinite
DES-7200(config-keychain-key)#end
```

! Configure G0/1 to use MD5 authentication key to authenticate the update messages sent from SwitchA

```
DES-7200#configure terminal
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#ip rip authentication key-chain DES-7200
DES-7200(config-if)#ip rip authentication mode md5
DES-7200(config-if)#exit
```

! Configure RIP routing protocol

```
DES-7200(config)#router rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.27.0
```

Verification

Execute "show run" command to verify the correctness of configurations (taking SwitchA as the example):

```
DES-7200#show run

Building configuration...
Current configuration : 1561 bytes

!
vlan 1
!
!
key chain DES-7200
 key 1
  key-string Hello
     accept-lifetime 16:30:00 Oct 01 2010 duration 43200
  send-lifetime 16:30:00 Oct 01 2010 duration 43200
 key 2
  key-string World
     accept-lifetime 04:00:00 Oct 02 2010 infinite
     send-lifetime 04:00:00 Oct 02 2010 infinite
!
no service password-encryption
!
interface GigabitEthernet 0/1
     no switchport
     ip rip authentication mode md5
 ip rip authentication key-chain DES-7200
 no ip proxy-arp
     ip address 192.168.27.1 255.255.255.0
```

```
!
interface GigabitEthernet 0/2
!
interface GigabitEthernet 0/3
!
interface GigabitEthernet 0/4
。。。。。。
!
!
!
router rip
 version 2
 network 192.168.27.0
!
!
!
line con 0
line vty 0 4
 login
!
!
end
```

2.3.5 RIP Redistribution and Default Route

Network Topology

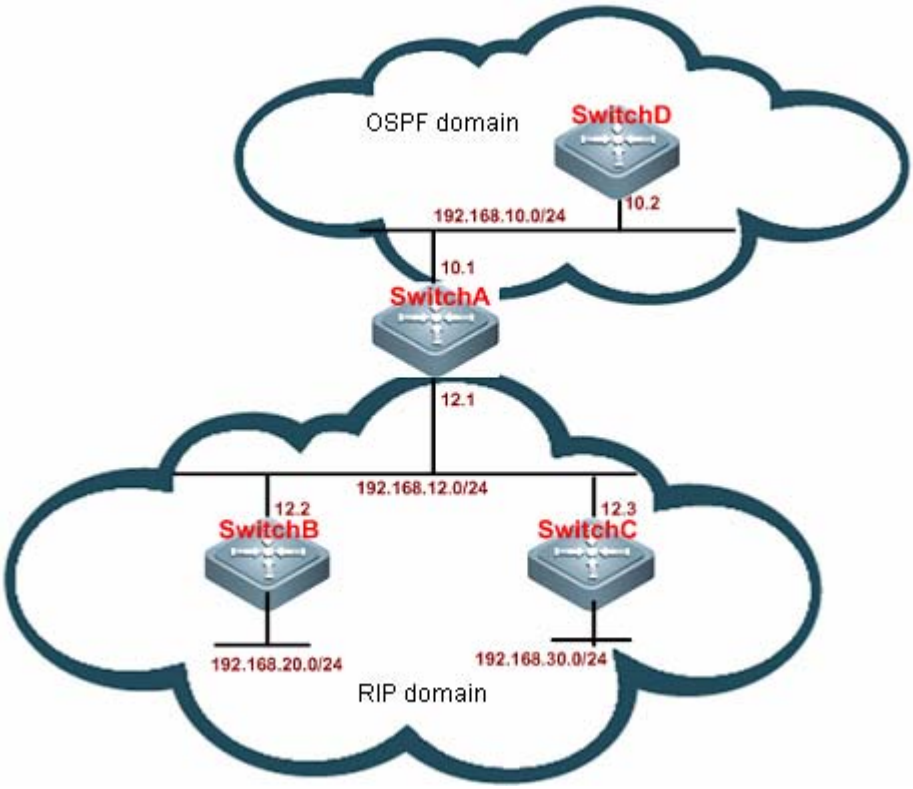


Figure4 Topological diagram for RIP redistribution and default route

Networking Requirements

SwitchA, SwitchB and SwitchC are interconnected in the same network segment and running RIP routing protocol. SwitchA and SwitchD are interconnected in the same network segment and running OSPF routing protocol. Configure these four devices to achieve the following goals:

- SwitchA can learn the OSPF routes advertised by SwitchD;
- SwitchA can redistribute OSPF routes to RIP;
- SwitchA advertises the redistributed routes to SwitchB and SwitchC;
- SwitchC advertise the default route to SwitchA and SwitchB.

Configuration Tips

- Configure to redistribute OSPF routes to RIP in the RIP process of SwitchA;
- Configure to advertise the default route on the corresponding interface of SwitchC;

Configuration Steps

 # SwitchA:

! Configure Ethernet interface

```
DES-7200(config)#interface FastEthernet 0/1
```

```
DES-7200(config-if-FastEthernet 0/1)#no switchport
DES-7200(config-if-FastEthernet 0/1)#ip address 192.168.12.1 255.255.255.0
DES-7200(config-if-FastEthernet 0/1)#exit
DES-7200(config)#interface FastEthernet0/2
DES-7200(config-if-FastEthernet 0/2)#no switchport
DES-7200(config-if-FastEthernet 0/2)#ip address 192.168.10.1 255.255.255.0
```

Configure RIP routing protocol

```
DES-7200(config)#router rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.12.0
DES-7200(config-router)#redistribute ospf 10 metric 3//Redistribute OSPF
routing process in RIP process, with metric value being 3
```

Configure OSPF routing protocol

```
DES-7200(config)#router ospf 10
DES-7200(config-router)#network 192.168.10.0 0.0.0.255 area 0
```

 # SwitchB:

! Configure Ethernet interface

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)#no switchport
DES-7200(config-if-FastEthernet 0/1)#ip address 192.168.12.2 255.255.255.0
DES-7200(config-if-FastEthernet 0/1)#exit
```

! Configure loopback interface

```
DES-7200(config)#interface Loopback 0
DES-7200(config-if-Loopback 0)#ip address 192.168.20.1 255.255.255.0
```

! Configure RIP routing protocol

```
DES-7200(config)#router rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.12.0
DES-7200(config-router)#network 192.168.20.0
```

 # SwitchC：

! Configure Ethernet interface

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)#no switchport
DES-7200(config-if-FastEthernet 0/1)#ip address 192.168.12.3 255.255.255.0
DES-7200(config-if-FastEthernet 0/1)#ip rip default-information originate
metric 5//Advertise default route, with metric value being 5
```

! Configure loopback interface

```
DES-7200(config)#interface Loopback 0
DES-7200(config-if-Loopback 0)#ip address 192.168.30.1 255.255.255.0
```

Configure RIP routing protocol

```
DES-7200(config)#router rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.12.0
DES-7200(config-router)#network 192.168.30.0
```

 # SwitchD:

! Configure Ethernet interface

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)#no switchport
DES-7200(config-if-FastEthernet 0/1)#ip address 192.168.10.2 255.255.255.0
```

! Configure OSPF routing protocol

```
DES-7200(config)#router ospf 10
DES-7200(config-router)#network 192.168.10.0 0.0.0.255 area 0
```

Verification

Display the routing table of each device (mainly the routing information on SwitchA, SwitchB and SwitchC):

1. View routing table on Switch A, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
R*   0.0.0.0/0 [120/5] via 192.168.12.3, 00:00:23, FastEthernet 0/1
C    192.168.10.0/24 is directly connected, FastEthernet 0/2
C    192.168.10.1/32 is local host.
C    192.168.12.0/24 is directly connected, FastEthernet 0/1
C    192.168.12.1/32 is local host.
R    192.168.20.0/24 [120/1] via 192.168.12.2, 00:07:09, FastEthernet 0/1
R    192.168.30.0/24 [120/1] via 192.168.12.3, 00:00:23, FastEthernet 0/1
```

2. View routing table on Switch B, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
R    192.168.10.0/24 [120/3] via 192.168.12.1, 00:00:06, FastEthernet 0/1
C    192.168.12.0/24 is directly connected, FastEthernet 0/1
C    192.168.12.2/32 is local host.
C    192.168.20.0/24 is directly connected, Loopback 0
C    192.168.20.1/32 is local host.
R    192.168.30.0/24 [120/3] via 192.168.12.3, 00:00:06, FastEthernet 0/1
```

3. View routing table on Switch C, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
R    192.168.10.0/24 [120/3] via 192.168.12.1, 00:01:49, FastEthernet 0/1
C    192.168.12.0/24 is directly connected, FastEthernet 0/1
C    192.168.12.3/32 is local host.
C    192.168.30.0/24 is directly connected, Loopback 0
C    192.168.30.1/32 is local host.
R    192.168.20.0/24 [120/3] via 192.168.12.2, 00:01:49, FastEthernet 0/1
```

2.3.6 RIP Supernet Route

Network Topology

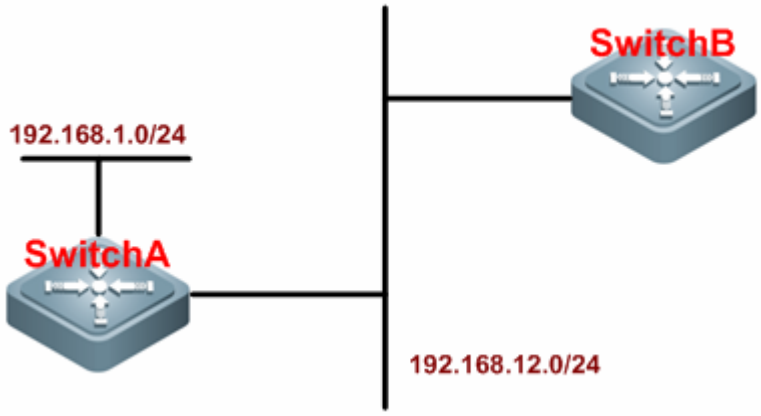


Figure5 Topological diagram for RIP supernet route

Networking Requirements

Two devices are interconnected through Ethernet. SwitchA runs RIPv2, and SwitchB only supports RIPv1 protocol and is unable to learn supernet routes.

Requirements:

- Configure a supernet route of 80.0.0.0/6 on Switch A, with next hop pointing to interface loopback 1 (192.168.1.0);
- Redistribute the aforementioned static route to RIP;
- Prohibit supernet route advertisement on Switch A.

Configuration Tips

Switch B only supports RIPv1 protocol. According to RFC 1058, such device is able to receive update packets of higher-version RIP, but such fields as subnet mask and next hop in the packets must be neglected. Therefore, the route of 80.0.0.0/6 received by Switch B will be treated as 80.0.0.0/8. To prevent Switch B from learning the wrong route, Switch A must be configured to prohibit supernet route advertisement.

Configuration Steps

 # SwitchA:

! Configure Ethernet interface

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)#no switchport
DES-7200(config-if-FastEthernet 0/1)#ip address 192.168.12.1 255.255.255.0
DES-7200(config-if-FastEthernet 0/1)#no ip rip send supernet-routes
//Prohibit supernet route advertisement
```

! Configure loopback interface

```
DES-7200(config)#interface loopback 1
```

```
DES-7200(config-if-Loopback 1)#ip address 192.168.1.1 255.255.255.0
```

! Configure static route

```
DES-7200(config)#ip route 80.0.0.0 252.0.0.0 loopback 1
```

! Configure RIP routing protocol

```
DES-7200(config)#router rip
DES-7200(config-router)#version 2
DES-7200(config-router)#network 192.168.12.0
DES-7200(config-router)#network 192.168.1.0
DES-7200(config-router)#redistribute static//Redistribute static route
```

 # SwitchB (supporting RIPv1 only):

! Configure Ethernet interface

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)#no switchport
DES-7200(config-if-FastEthernet 0/1)#ip address 192.168.12.2 255.255.255.0
```

! Configure RIP routing protocol

```
DES-7200(config)#router rip
DES-7200(config-router)#network 192.168.12.0
```

Verification

Display the routing table of each device;

1. View the routing table on SwitchA, as shown below:

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    80.0.0.0/6 is directly connected, Loopback 1
C    192.168.1.0/24 is directly connected, Loopback 1
C    192.168.1.1/32 is local host.
C    192.168.12.0/24 is directly connected, FastEthernet 0/1
C    192.168.12.1/32 is local host.
```

2. View routing table on SwitchB, as shown below (the bold figures are the routing information learned through RIP):

```
DES-7200#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
R    80.0.0.0/6 [120/1] via 192.168.12.1, 00:00:46, GigabitEthernet 0/1
R    192.168.1.0/24 [120/1] via 192.168.12.1, 00:38:17, FastEthernet 0/1
C    192.168.12.0/24 is directly connected, FastEthernet 0/1
C    192.168.12.2/32 is local host.
```

2.3.7 Example of RIP VRF configuration

Requirements

Two routing devices are interconnected through Ethernet and running RIP routing protocol. The connection layout and IP address distribution are shown in Fig 6.

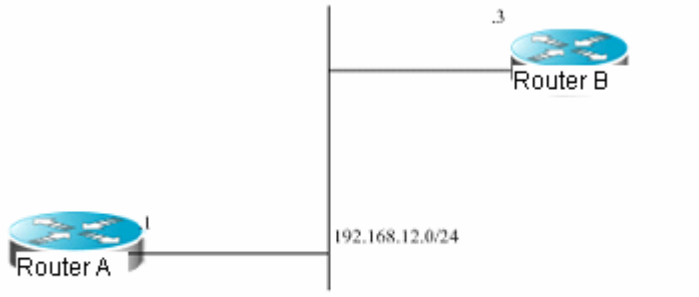


Figure6 Example of RIP VRF configuration

Through RIP, routing information is exchanged between VRF "redvpn" of device A and VRF "bluevpn" of device B.

By enabling RIP graceful restart on device A and setting grace period to 90 seconds, non-stop data forwarding can be realized during main-slave management board switchover carried out on device A. Meanwhile, since the grace period has been changed, "timers basic" shall be configured to a reasonable value.

Detailed Configurations

Device A:

Create VRF

```
ip vrf redvpn
```

Bind the interface to VRF and configure interface address

```
interface FastEthernet 1/0
ip vrf forwarding redvpn
ip address 192.168.12.1 255.255.255.0
```

Configure RIP routing protocol and create RIP instance

```
router rip
address-family ipv4 vrf redvpn
network 192.168.12.0
graceful-restart grace-period 90
timers basic 45 270 180
exit-address-family
```

Device B:

Create VRF

```
ip vrf  bluevpn
```

Bind the interface to VRF and configure interface address

```
interface FastEthernet 1/0
ip vrf forwarding bluevpn
ip address 192.168.12.3 255.255.255.0
```

Configure RIP routing protocol and create RIP instance

```
router rip
address-family ipv4 vrf bluevpn
network 192.168.12.0
timers basic 45 270 180
exit-address-family
```

2.3.8 Example of Triggered RIP configuration

Requirements

Two routers are interconnected through PPP link and running RIP routing protocol. The connection layout and IP address distribution are shown in "Fig 7 Example of Triggered RIP configuration".

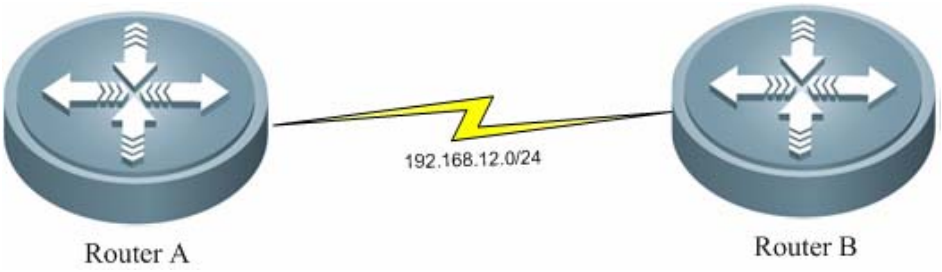


Figure 7 Example of Triggered RIP configuration

By configuring Triggered RIP, routing information can be exchanged between Router A and Router B on WAN link, and split horizon with poisoned reverse shall be enabled.

Detailed Configurations

Device A:

Enable PPP link protocol on the interface and configure interface address; Enable TRIP and split horizon with poisoned reverse.

```
interface Serial 0/0
encapsulation ppp
ip address 192.168.12.1 255.255.255.0
ip rip triggered
ip rip split-horizon poisoned-reverse
```

Configure RIP routing protocol

```
router rip
network 192.168.12.0
```

Device B:

Enable PPP link protocol on the interface and configure interface address; Enable TRIP and split horizon with poisoned reverse.

```
interface Serial 0/0
encapsulation ppp
ip address 192.168.12.2 255.255.255.0
ip rip triggered
ip rip split-horizon poisoned-reverse
# Configure RIP routing protocol
router rip
network 192.168.12.0
```

3 RIPng Configuration

3.1 Overview

Similar to RIP, RIPng is a distance-vector routing protocol using hop count as the routing metric. RIPng is an interior gateway protocol applicable to small- and medium-sized networks. RIPng is the necessary extension of RIP to address the routing requirements of IPv6. Therefore, RIPng and RIP have basic working principles in common. The main differences rise from the format of their address and packet. Based on IPv6, RIPng supports and uses the multicast group address of FF02::9 for update messages. Security authentication used in RIP is also cancelled. Instead, RIPng enables security authentication by the security mechanism of IPv6. 521 port is used. Packet format, mask and maximum packet length are all different. Please refer to RFC2080 and RFC2081 for details. Given the difference from RIP, the corresponding CLI commands are also lesser.

3.2 RIPng Configuration Task

The default configurations of RIPng are given below:

Function	Default setting
Network interface	The default metric-offset is 1.
Redistribution	The route redistribution is disabled by default. If enabled: ● All sub-routes of the routing process are redistributed. ● The metric of redistributed route is the default metric.
Split horizon	Enabled
Poisoned reverse	Disabled
Timer	By default: ● Update time is 30 seconds ● Invalid time is 180 second ● Clearing time is 120 seconds

Default metric	Redistribute the metric used by the routes of other protocols，1 by default.
Administrative distance	120

3.2.1 Create RIPng Routing Process

In order to run RIPng routing protocol, the routing device first needs to create the RIPng routing process and define the network or interface address associated with RIPng routing process.

To create RIPng routing process, input the following command in the global configuration mode:

Command	Function
DES-7200(config)**# ipv6 router rip**	Create RIPng routing process.

3.2.2 Enable RIPng on the Interface

To enable RIPng on the interface, input the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)**# ipv6 rip enable**	Enable RIPng on the interface.

In the following example, enable RIPng on ethernet 0/0. Routes in the range of 2001:db8:6::/64 are converged into 2001:db8:6::/64 for advertisement.

```
DES-7200(config)# interface ethernet 0/0
DES-7200(config-if)# ipv6 address 2001:db8:6::1/64
DES-7200(config-if)# ipv6 rip enable
```

Note

Different from RIP, this command enables RIPng on the interface directly without configuring Network command.

3.2.3 Adjust RIPng Timer

RIPng provides the feature of timer adjustment. You can adjust the timer according to the physical circumstances of the network, so that the RIPng routing protocol can run better. The following timers can be adjusted:

- Route update time (second): defines the interval by which the routing device will send the route update message;
- Route invalid time (second): defines the time by which the route in the

routing table becomes invalid upon no update;

- Route clearing time (second): upon expiration of this time, the route will be removed from the routing table.

By adjusting the aforementioned times, the convergence time and failure recovery time of routing protocol can be accelerated. To adjust RIPng timer, input the following command in the RIPng routing process configuration mode:

Command	Function
DES-7200(config-router)# **times** *update invalid garbage-collection*	Adjust RIPng times.

The following example adjusts the values of three RIPng times:

```
DES-7200(config-router)# timers 10 30 90
```

Caution

Consistency of RIPng times is mandatory for routing devices in the same network.

3.2.4 Configure Split Horizon

When multiple routing devices are linked to the IP broadcast network and running distance-vector routing protocol, it is necessary to adopt the mechanism of split horizon to avoid loop. Split horizon can prevent routing device from sending routing information to the port from which such routing information was learned. Such mechanism optimizes the routing information exchange between multiple routing devices.

However, for non-broadcast multiple-access network (such as frame relay, X.25 network), split horizon may cause disable certain routing devices from learning all routing information. In such a case, the split horizon will need to be disabled.

To disable or enable split horizon, input the following command in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **no split-horizon**	Disable split horizon.
DES-7200(config-router)# **split-horizon**	Enable split horizon.

By default, split horizon is enabled on all RIPng ports.

Note

The current version can only support split horizon configuration in RIPng routing process, i.e., this command will be applied to all RIPng interfaces.

Different from split horizon, when poison reverse is enabled, the routing device will advertise certain route information from the interface from which such route information was learned. Just set the corresponding metric to infinity (16).

To enable or disable poison reverse, input the following command in the routing process configuration mode:

Command	Function
DES-7200(config-router)**#split-horizon poisoned-reverse**	Enable split horizon with poison reverse
DES-7200(config-router)**#no split-horizon poisoned-reverse**	Disable split horizon with poison reverse

Caution

Enabling poison reverse will consume considerable bandwidth.

3.2.5 Configure Default Metric for Redistribution

When a protocol redistributes routes of other protocols, you need to configure the metric for such redistribution for metric varies by protocols. The default metric of RIPng is 1.

To define the default RIPng metric during the redistribution of other routing protocols, please use the routing process configuration command of **default-metric**. Use **no default-metric** command to reset the default value to 1.

Command	Function
DES-7200(config-router)# **default-metric** *metric*	The metric of RIPng is set to *metric*
DES-7200(config-router)# **no default-metric**	Reset the default value to 1

3.2.6 Adjust Interface Metric

Before adding the learned routes into the routing table, you need to add the metric set for the interface to the ones of learned routes. Therefore, you can control the use of routes by configuring the interface metric.

To configure the interface metric, input the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ipv6 rip metric-offset** *value*	Configure interface metric within the scope of 1-16.

The following example sets the metric of ethernet 0/0 to 6:

```
DES-7200(config)# interface ethernet 0/0
DES-7200(config-if)# ipv6 rip metric-offset 6
```

3.2.7 Configure the Advertisement Default Route on the Interface

To generate an IPv6 default route in the update message of this RIPng process (::/0), input the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ipv6 rip default-informaton originate**	Generate a default route to RIPng on the interface and advertise it with other routes.

To generate an IPv6 default route in the update message of this RIPng process (::/0), and advertise only this default route on this interface, input the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ipv6 rip default-informaton only**	Generate a default route to RIPng on the interface and advertise only this default route.

3.2.8 Configure Passive Interface

To prevent other routing devices in the local network from learning the routing information sent by the routing device, configure passive interface to disable sending routing update message from this network interface.

To disable sending update messages from an interface, input the following command in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **passive-interface** {**default** | *interface-type interface-num*}	Disable sending update messages from the interface.

Note

When applying the **default** option, all interfaces will be set to passive mode; when applying the **interface** option, the corresponding interface will set to passive mode.

3.2.9 Configure RIPng Route Filtering

3.2.9.1 Control Route Update Advertisement (RIPng)

To prevent other routing devices in the local network from learning unnecessary routing information, disable the update of specific routes by controlling RIPng route update advertisement.

To disable route update advertisement, input the following command in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **distribute-list prefix-list** *prefix-list-name* **out** [*interface-type interface-name*]	According to the rule of prefix list, enable or disable the advertisement of certain routes.
DES-7200(config-router)# **no distribute-list prefix-list** *prefix-list-name* **out** [*interface-type interface-name*]	Remove the configuration.

In the following example, filtering is only applied to update messages sent from interface eth0, and only update routes included in the prefix-list *outlist* will be sent out.

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# distribute-list prefix-list outlist out eth0
```

3.2.9.2 Control Route Update Processing (RIPng)

This feature can be configured to avoid receiving certain routes in the route update message.

To control route update processing, input the following command in the routing process configuration mode:

Command	Function

DES-7200(config-router)# **distribute-list prefix-list** *prefix-list-name* **in** [*interface-type interface-name*]	According to the rule of access list, enable or disable the receipt of certain routes in the route update.
DES-7200(config-router)# **no distribute-list prefix-list** *prefix-list-name* **in** [*interface-type interface-name*]	Remove the configuration.

In the following example, filtering is only applied to update messages received by interface eth0, and only update routes included in the prefix-list *inlist* will be received.

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# distribute-list prefix-list inlist in eth0
```

3.2.10 Show RIPng Configuration

3.2.10.1 RIPng Debugging Switch

To show the debugging information of RIPng and observe the route processing behaviors of RIPng, input the following command in the privilege configuration mode:

Command	Function
DES-7200# **debug ipv6 rip** [{*interface-type interface-num* | **nsm**}]	Turn on RIPng debugging switch.
DES-7200# **no debug ipv6 rip** [{*interface-type interface-num* | **nsm**}]	Turn off RIPng debugging switch.

3.2.10.2 Show RIPng Routing Table

To show RIPng routing table, input the following command in user mode or privileged EXEC mode:

Command	Function
DES-7200# **show ipv6 rip database**	Display RIPng routing table information.

3.2.10.3 Show RIPng Routing Process

To display the parameters and various statistical data of RIPng routing process,

input the following command in user mode or privilege mode:

Command	Function
DES-7200# **show ipv6 rip**	Display RIPng routing process information.

3.2.10.4 Show RIPng Debugging Information

To display the debugging information of RIPng routing process, input the following command in the privileged EXEC mode or global configuration mode:

Command	Function
DES-7200# **show debugging**	Display the debugging information of RIPng routing process.

3.3 Configuration Examples

3.3.1 Configure Default Route Advertisement

Configuration requirements

There are three devices (see Fig 1 for device connection) running RIPng. The gateway device of Router A advertises the default route to Router B and Router C, with metric being 3. All RIPng interfaces of Router B and Router C are configured to passive mode, so as not to send out RIPng update messages.

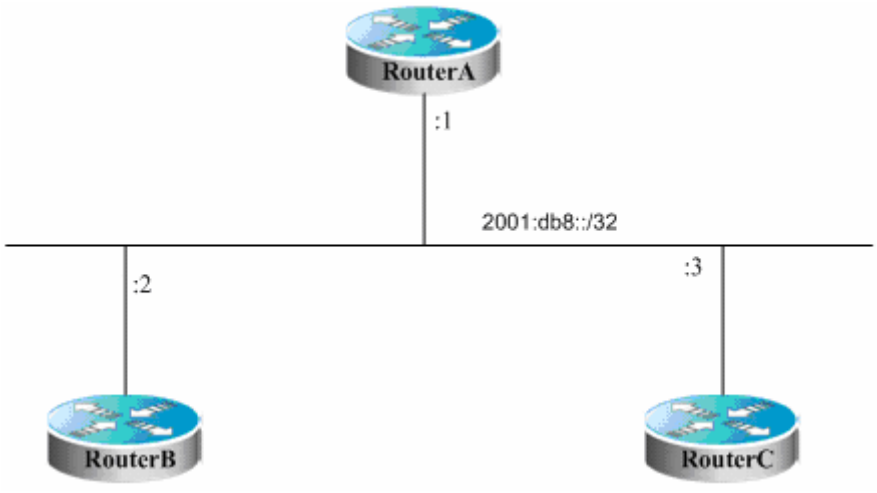


Fig 2 Configuration of default route advertisement

Detailed configuration

Router A:

Configure network interface

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address 2001:db8::1/32
DES-7200(config-if)# ipv6 rip enable
DES-7200(config-if)# ipv6 rip default-information originate
metric 3
```

Configure RIPng

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# exit
```

Router B:

Configure network interface.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address 2001:db8::2/32
DES-7200(config-if)# ipv6 rip enable
```

Configure RIPng.

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# passive-interface default
DES-7200(config-router)# exit
```

Router C:

Configure network interface.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address 2001:db8::3/32
DES-7200(config-if)# ipv6 rip enable
```

Configure RIPng.

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# passive-interface default
DES-7200(config-router)# exit
```

3.3.2 Redistribution configuration

Configuration requirements

There are three devices (see Fig 1 for device connection). Router A runs RIPng; Router C runs BGP and introduces static routes; Router B needs to redistribute the static routes redistributed by Router C to RIPng domain.

In order to meet such requirements, we can configure the specified community

attribute for static routes redistributed to BGP on Router C, while Router B can redistribute BGP routes with specified community attribute to the RIPng domain.

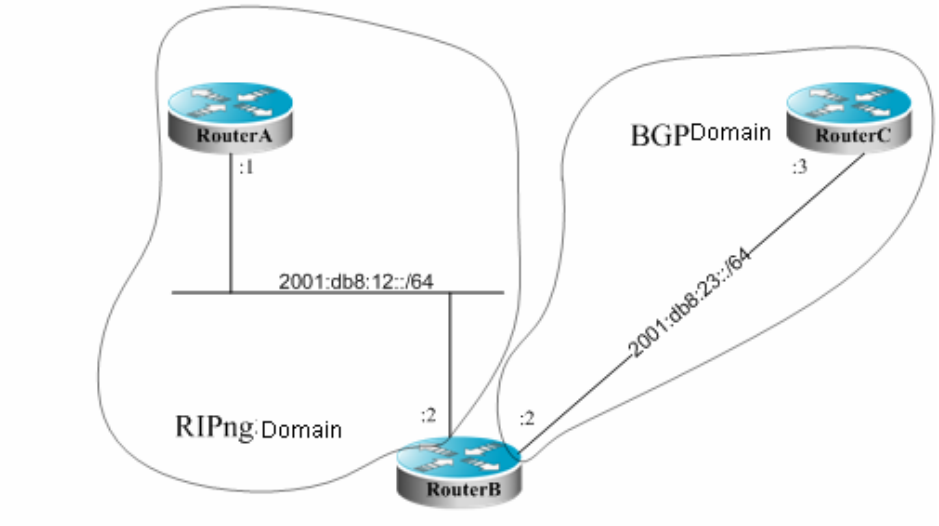


Fig 3 Redistribution configuration

Detailed configuration

Router A:

Configure network interface.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address 2001:db8:12::1/64
DES-7200(config-if)# ipv6 rip enable
```

Configure RIPng.

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# exit
```

Router B:

Configure network interface.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address 2001:db8:12::2/64
DES-7200(config-if)# ipv6 rip enable
DES-7200(config)# interface gigabitEthernet 0/2
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address 2001:db8:23::2/64
```

Configure RIPng.

```
DES-7200(config)# ipv6 router rip
DES-7200(config-router)# redistribute bgp route-map riprm
```

```
DES-7200(config-router)# exit
```

Configure BGP.

```
DES-7200(config)# router bgp 2
DES-7200(config-router)# neighbor 2001:db8:23::3 remote-as 3
DES-7200(config-router)# address-family ipv6
DES-7200(config-router-af)# neighbor 2001:db8:23::3 activate
```

Configure route map.

```
DES-7200(config)# route-map riprm
DES-7200(config-route-map)# match community cl_110
```

Define community list.

```
DES-7200(config)# ip community-list standard cl_110 permit 22:22
```

Router C:

Configure network interface.

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 enable
DES-7200(config-if)# ipv6 address 2001:db8:23::3/64
```

Configure BGP.

```
DES-7200(config)# router bgp 3
DES-7200(config-router)# neighbor 2001:db8:23::2 remote-as 2
DES-7200(config-router)# address-family ipv6
DES-7200(config-router-af)# redistribute static route-map bgprm
DES-7200(config-router-af)# neighbor 2001:db8:23::2 activate
DES-7200(config-router-af)# neighbor 2001:db8:23::2 send-community
```

Configure static route.

```
DES-7200(config)# ipv6 route 2001:db8:88::/64 null 0
DES-7200(config)# ipv6 route 2001:db8:99::/64 null 0
```

Configure route map.

```
DES-7200(config)# route-map bgprm
DES-7200(config-route-map)# set community 22:22
```

4 OSPF Configuration

4.1 OSPF Overview

OSPF (Open Shortest Path First) is an internal gateway routing protocol based on link status developed by the IETF OSPF work group. OSPF, a routing protocol specific for IP, directly runs on the IP layer. Its protocol number is 89. OSPF packets are exchagned in multicast form using the multicast address 224.0.0.5 (for all OSPF routers) and 224.0.0.6 (for specified routers).

The link status algorithm is an algorithm totally different from the Huffman vector algorithm (distance vector algorithm). The RIP is a traditional routing protocol that uses the Huffman vector algorithm, while the OSPF protocol is the typical implementation of the link status algorithm. Compared with the RIP routing protocol, the OSPF uses a different algorithm, and also introduces the new concepts such as route update authentication, VLSMs, and route aggregation. Even if the RIPv2 has made great improvements, and can support the features such as route update authentication and VLSM, the RIP protocol still has two fatal weaknesses: 1) slow convergence; 2) limited network size, with the maximum hot count of no more than 16. The OSPF is developed to overcome these weaknesses of the RIP, making the IGP protocol applicable for large and complicated network environments.

The OSPF protocol establishes and calculates the shortest path to every destination network by using the link status algorithm. This algorithm is complicated. The following briefly describes how the link status algorithm works:

- In the initialization stage, a router will generate a link status notification including the status of all its links.
- All routers exchange the link status message in the multicast way. Upon receiving the link status update message, each router will copy it to its local database and then transmit it to other routers.
- When every router has a complete link status database, the router uses the Dijkstra algorithm to calculate the shortest path trees to all the target networks. The results include destination network, next-hop address, and cost, which are the key parts of the IP routing table.

If there is no link cost or network change, the OSPF will become silent. If any changes occur on the network, the OSPF advertises the changes via the link status message of only the changed links. The routers involved in the changes

will have the Dijkstra algorithm run again, with a new shortest path tree created.

A group of routers running the OSPF protocol form the autonomous domain system of the OSPF routing domain. An autonomous domain system consists of all the routers that are controlled and managed by one organization. Within the autonomous domain system, only one IGP routing protocol is run. However, between multiple such systems, the BGP routing protocol is used for route information exchange. Different autonomous domain systems can use the same IGP routing protocol. To access the Internet, every autonomous system needs to request the related organization for the autonomous system number.

When the OSPF routing domain is large, the hierarchical structure is usually used. In other words, the OSPF routing domain is divided into several areas, which are connected via a backbone area. Every non-backbone area must be directly connected with this backbone area.

There are three roles for the routers in the OSPF routing domain according to their deployment position:

- Area Internal Routers, all interface networks of this router are of this area;
- ABR (Area Border Router): The interfaced networks of this router belong at least to two areas, one of which must be the backbone area;
- ASBR (Autonomous System Boundary Routers): It is the router between which the OSPF route domain exchanges the external route domain.

DES-7200 product implements the OSPF by fully complying with the OSPFv2 defined in RFC 2328. The main features of the OSPF are described as below:

- Support multiple OSPF processes, up to 64 OSPF processes running at the same time.
- Support VRF. You can run OSPF based on different VRFs.
- Support the definition of stubby area.
- Support route redistribution with the static route, directly-connected route and the dynamic route protocol such as RIP, BGP, etc.
- Support plain-text or MD5 authentication between neighbors.
- Support virtual links.
- Support VLSMs.
- Support area division
- Support NSSA (Not So Stubby Area), as defined in RFC 3101.
- Support Graceful Restart, as defined in RFC 3623.

4.2 OSPF Configuration Task

The configuration of OSPF should be cooperated with various routers (including internal routers, area boundary routers and autonomous system boundary routers). When no configuration is performed, the defaults are used for various parameters of the routers. In this case, packets are sent and received without authentication, and an interface does not belong to any area of an autonomous system. When you change the default parameters, you must ensure that the routers have the same configuration settings.

To configure the OSPF, you must perform the following tasks. Among them, activating the OSPF is required, while others are optional, but may be required for particular applications.

The default OSPF configuration is shown as below:

Function	Default setting
Interface parameters	Interface cost: none is preset LSA retransmit interval: 5 seconds. LSA transmit delay: 1 second. Hello message transmit interval : 10 seconds (30 seconds for non-broadcast networks) Failure time of adjacent routers: 4 times the hello interval. Priority: 1 Authentication type: 0 (No authentication). Authentication password: None.
Area	Authentication type: 0 (No authentication). Default metric of aggregated routes to Stub or NSSA area: 1 Inter-area aggregation scope: Undefined Stub area: Undefined NSSA: Undefined
Virtual Link	No virtual link is defined. The default parameters of the virtual link are as below: LSA retransmit interval: 5 seconds. LSA transmit delay: 1 second. Hello message interval: 10 seconds. Failure time of adjacent routers: 4 times the hello interval. Authentication type: No authentication. Authentication password: No password specified.

Automatic cost calculation	Enabled automatically; Default automatic cost is 100Mbps
Default route generation	Disabled The default metric will be 1 and the type is type-2.
Default metric (Default metric)	The default metric is used to redistribute the other routing protocols;
Management Distance	Intra-area route information:110 Inter-area route information:110 External route information:110
Database filter	Disabled. All interfaces can receive the status update message (LSA).
Neighbor change log	Enabled
Neighbor	N/A
Neighbor database filter Disabled.	All outgoing LSAs are sent to the neighbor.
network area (network area)	N/A
Device ID	Undefined; the OSPF protocol does not run by default
Route summarization (summary-address)	Undefined
Changing LSAs Group Pacing	240 seconds
Shortest path first (SPF) timer	The time between the receipt of the topology changes and SPF-holdtime: 5 seconds The least interval between two calculating operations: 10 seconds
Optimal path rule used to calculate the external routes	Using the rules defined in RFC1583
OSPF overflow memory-lack	Enter the overflow state when the memory lacks. GR restarter: disabled. GR helper:enabled.
OSPFv2 MIB binding	In the OSPFv2 process in the smallest process number.
OSPFv2 TRAP sending	Disabled

4.2.1 Creating the OSPF Routing Process

This is to create the OSPF routing process and define the range of the IP

addresses associated with the OSPF routing process and the OSPF area to which these IP addresses belong. The OSPF routing process only sends and receives the OSPF packets at the interface within the IP address range and advertises the link status of the interface to the outside. Currently, 64 OSPF routing process are supported.

To create the OSPF routing process, you can perform the following steps:

Command	Meaning
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config)# **ip routing**	Enable the IP routing (if disabled).
DES-7200(config)**# router ospf** *process-id* [**vrf** *vrf-name*]	Enable OSPF and enter OSPF route configuration mode.
DES-7200 (config-router)# **network** *address wildcard-mask* **area** *area-id*	Define an IP address range for an area.
DES-7200 (config-router)# **End**	Return to the privileged EXEC mode.
DES-7200 # **show ip protocol**	Display the routing protocol that is running currently.
DES-7200 # **write**	Save the configuration.

Note

The parameter vrf *vrf-name* is used to specify the VRF which the OSPF belongs to. If you do not specify the parameter in the OSPF process, it belongs to the default VRF. For the **network** command, 32 bit wildcards are opposed to the mask, where 1 means not to compare the bit and 1 means to compare the bit. However, if you configure the command with mask, DES-7200 products will automatically translate it into a bit wildcard. An interface belongs to the specific area as long as it matches the IP address range defined by the **network** command. When an interface matches more than one IP address range defined by the **network** command in multiple OSPF processes, the OSPF process that the interface takes part in is determined in the way of optimal match.

To disable the OSPF protocol, use the **no router ospf** [*process-id*]command. The example shows how to enable the OSPF protocol:

```
DES-7200(config)# router ospf 1
DES-7200 (config-router)# network 192.168.0.0 255.255.255.0 area 0
DES-7200 (config-router)# end
```

4.2.2 Configuring Interface Parameters

You are allowed to change some particular interface parameters. It should be noted that some parameters must be set to match those of the adjacent router of

the interface. These parameters are set via the **ip ospf hello-interval**, **ip ospf dead-interval**, **ip ospf authentication**, **ip ospf authentication-key** and **ip ospf message-digest-key**. When you use these commands, you should make sure that the adjacent routers have the same configuration.

To configure the OSPF interface parameters, execute the following commands in the interface configuration mode:

Command	Meaning
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config)# **ip routing**	Enable the IP routing (if disabled).
DES-7200 (config)**# interface** *interface-id*	Enter the interface configuration mode.
DES-7200 (config-if)**# ip ospf cost** *cost-value*	(Optional) Define the interface cost.
DES-7200(config-if)**# ip ospf retransmit-interval** *seconds*	(Optional) Set the link status retransmission interval.
DES-7200 (config-if)# **ip ospf transmit-delay** *seconds*	(Optional) Set the transmit delay for the link status update packets.
DES-7200 (config-if)# **ip ospf hello-interval** *seconds*	(Optional) Set the hello message send interval, which must be the same for all the nodes of the entire network.
DES-7200 (config-if)# **ip ospf dead-interval** *seconds*	(Optional) Set the dead interval for the adjacent router, which must be the same for all the nodes of the entire network.
DES-7200 (config-if)# **ip ospf priority** number	(Optional) The priority is used to select the dispatched routers (DR) and backup dispatched routers (BDR).
DES-7200 (config-if)# **ip ospf authentication** [**message-digest | null**]	(Optional) Set the authentication type on the network interface.
DES-7200 (config-if)# **ip ospf authentication-key** *key*	(Optional) Configure the key for text authentication of the interface.
DES-7200 (config-if)**#ip ospf message-digest-key** *keyid* **md5** *key*	(Optional) Configure the key for MD5 authentication of the interface.
DES-7200 (config-if)**#ip ospf database-filter all out**	(Optional) Prevent the interfaces from flooding the LSAs packets. By default, OSPF floods new LSAs over all interfaces in the same area, except the interface on which the LSA arrives.

Command	Meaning
DES-7200 (config-if)**#end**	Return to the privileged EXEC mode.
DES-7200 **#show ip ospf** [*process-id*] **interface** [*interface-id*]	Display the routing protocol that is running currently.
DES-7200 # **write**	(Optional) Save the configuration.

You can use the **no** form of the above commands to cancel or restore the configuration to the default.

4.2.3 Configuring the OSPF to Adapt to Different Physical Networks

According to the transmission nature of different media, the OSPF divides the networks into three types:

- Broadcast network (Ethernet, token network, and FDDI)
- Non-broadcast network (frame relay, X.25)
- Point-to-point network (HDLC, PPP, and SLIP)

The non-broadcast networks include two sub-types according to the operation modes of the OSPF:

- One is the Non-broadcast Multi-access (NBMA) network. The NBMA requires direct communication for all routers interconnected. Only fully meshed networks can meet this requirement. If the SVC (for example, X.25) connection is used, this requirement can be met. However, if the PVC (for example, frame relay) networking is used, there will be some difficulty in meeting this requirement. The operation of the OSPF on the NBMA network is similar to that on the broadcast network: One Designated Router must be elected to advertise the link status of the NBMA network.
- The second is the point-to-multipoint network type. If the network topology is not a fully meshed non-broadcast network, you need to set the network type of the interface to the point-to-multipoint network type for the OSPF. In a point-to-multipoint network type, the OSPF takes the connections between all routers as point-to-point links, so it does not involve the election of the designated router.

Whatever the default network type of the interface, you must set it to the broadcast network type. For example, you can set the non-broadcast multi-access network (frame relay, X.25) to a broadcast network. This spares the step to configure the neighbor when you configure the OSPF routing process. By using the **X.25 map** and **Frame-relay map** commands, you can allow X.25 and frame relay to have the broadcast capability, so that the OSPF can see the networks like X.25 and frame relay as the broadcast networks.

The point-to-multipoint network interface can be seen as the marked point-to-point interface of one or multiple neighbors. When the OSPF is configured as the point-to-multipoint network type, multiple host routes will be created. The point-to-multipoint network has the following advantages over the NBMA network:

- Easy configuration without the configuration of neighbors or the election of the designated router.
- Small cost without the need of fully meshed topology

To configure the network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip ospf network {broadcast | non-broadcast | point-to-point | {point-to-multipoint [non-broadcast]} }**	Configure the OSPF network type.

For different link encapsulation types, the default network type is shown as below:

- Point-to-point network type
  PPP, SLIP, frame relay point-to-point sub-interface, X.25 point-to-point sub-interface encapsulation
- NBMA (non-broadcast) network type
  Frame relay, X.25 encapsulation (except point-to-point sub-interface)
- Broadcast network type
  Ethernet encapsulation

The default type is not the point-to-multipoint network type

It should be noted that the network type should be consistent at both sides. Otherwise, the abnormality will occur, for instance, the neighbor is Full and the calculation of the routing is incorrect.

4.2.3.1 Configuring Point-to-Multipoint Broadcast Network

When routers are connected via X.25 and frame relay networks, if the network is not a fully meshed network or you do not want the election of the designated router, you can set the network type of the OSPF interface as the point-to-multipoint type. Since the point-to-multipoint network sees the link as a point-to-point link, multiple host routes will be created. In addition, all the neighbors have the same cost in the point-to-multiple networks. If you want to make different neighbors have different costs, you can set them by using the **neighbor** command.

To configure the point-to-multipoint network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)**# ip ospf network point-to-multipoint**	Configure the point-to-multipoint network type for an interface.
DES-7200(config-if)**# exit**	Exit to the global configuration mode.
DES-7200(config)**# router ospf 1**	Enter the routing process configuration mode.
DES-7200(config-router)# **neighbor** *ip-address* **cost** *cost*	Specify the cost of the neighbor (optional).

Note

Although the OSPF point-to-point network is a non-broadcast network, it can allow non-broadcast networks to have broadcast capability by using the frame relay, X.25 mapping manual configuration or self-learning. Therefore, you do not need to specify neighbors when you configure the point-to-multipoint network type.

4.2.3.2 Configuring Non-broadcast Network

When the OSPF interface works in the non-broadcast network, you can configure it to the NBMA or the point-to-multipoint non-broadcast type. Since it cannot dynamically discover neighbors without the broadcast capability, you must manually configure neighbors for the OSPF interface working in the non-broadcast network.

You can configure the NBMA network type in the following conditions:

- When a non-broadcast network has the fully meshed topology;
- You can set a broadcast network as the NBMA network type to reduce the generation of the broadcast packets and save the network bandwidth, and also avoid arbitrary reception and transmission of routers by some degree. The configuration of the NBMA network should specify the neighbor. For there is the choice to specify the routers, you should determine which router is the designated router. For this reason, it is necessary for you to prioritize rotuers. The higher the router's pirority is, the higher possibility of being the designated router is.

To configure the NBMA network type, execute the following commands in the interface configuration mode:

Command	Function

Command	Function
DES-7200 (config-if)# **ip ospf network non-broadcast**	Specify the network type of the interface to be the NBMA type.
DES-7200 (config-if)# **exit**	Exit to the global configuration mode.
DES-7200 (config)# **router ospf 1**	Enter the routing process configuration mode.
DES-7200(config-router)# **neighbor** *ip-address* [**priority** *number*] [**poll-interval** *seconds*]	Specify the neighbor, its priority and polling interval of Hello messages.

In a non-broadcast network, if it cannot ensure that any two routers are in direct connection, the better solution is to set the network type of the OSPF to the point-to-multipoint non-broadcast network type.

Whether in a point-to-multipoint broadcast or non-broadcast network, all the neighbors have the same cost, which is the value set by using the **ip ospf cost** command. However, the bandwidths of the neighbors may be actually different, so the costs should be different. Therefore, you can specify the necessary cost for each neighbor by using the **neighbor** command. This only applies to the interfaces of the point-to-multipoint type (broadcast or non-broadcast).

To configure the point-to-multipoint type for the interfaces in a non-broadcast network, execute the following commands in the interface configuration mode:

Command	Function
DES-7200 (config-if)# **ip ospf point-to-multipoint non-broadcast**	Specify the network type of the interface to be the point-to-multipoint non-broadcast type.
DES-7200 (config-if)# **exit**	Exit to the global configuration mode.
DES-7200 (config)# **router ospf 1**	Enter the routing process configuration mode.
DES-7200(config-router)# **neighbor** *ip-address* [**cost** number]	Specify the neighbor and the cost to the neighbor.

Pay attention to step 4. If you have not specified the cost for the neighbor, the cost referenced by the **ip ospf cost** command in the interface configuration mode will be used.

4.2.3.3 Configuring Broadcast Network Type

It is necessary to select the designated router (DR) and backup designated router (BDR) for the broadcast type network of OSPF. The DR will notify the link status of this network to outside. All routers keep the neighbor relationship one another and only the adjacent relationship with the designated routers and backup designated routers. That is to say, each router only switches the link status

packets with the designated router and backup designated routers, and then the designated router notifies all routers. As a result, each router can keep a consistent link status database.

You can control the election of the designated router by setting the OSPF priority. The parameter does not take effect immediately until in the new round of election. The new election of the designated router occurs only when the OSPF neighbor doesn't receive the Hello message from the designated router within the specified time and consider the DR is down.

To configure the broadcast network type, execute the following commands in the interface configuration mode:

Command	Function
DES-7200 (config-if)# **ip ospf network broadcast**	Specify the type of the interface to be the broadcast network type.
DES-7200 (config-if)# **ip ospf priority** *priority*	(Optional) Specify the priority of the interface.

4.2.4 Configuring the OSPF Area Parameters

To configure area authentication, stub area, and default route summary cost, you need to use the command for configuring the areas.

Area authentication is configured to avoid the learning of non-authenticated and invalid routes and the advertisement of invalid routes to the non-authentication routers. In the broadcast-type network, area authentication can also prevent non-authentication routers from becoming the designated routers for the stability and intrusion prevention of the routing system.

When an area is the leaf area of the OSPF area, orthe area neither acts as the transit area nor injects external routes to the OSPF area, you can configure the area as a stub area. The routers in a stub area can only learn about three routes, namely, 1) Routes in the stub area, 2) Routers in other areas, and 3) Default routes advertised by the border router in the stub area. For there is few external routes, the route tables of the rotuers in the stub area are small, saving resources. So the rotuers in the stub area may be low- or middle-level of routers. To reduce the number of the Link Status Advertisements (LSA) messages sent to the stub areas, you can configure the area as the full stub area (configured with the **no-summary** option). The routers in a full stub area can learn two types of routes: 1) routes in the stub area; 2) default routes advertised by the border router in the stub area. The configuration of the full stub area allows the OSPF to occupy the minimized router resources, increasing the network transmission efficiency.

If the routers in a stub area can learn multiple default routes, you need to set the costs of the default routes (by using the **area default-cost** command), so that

they first use the specified default route.

You should pay attention to the following aspects when you configure a stub area:

- The backbone area cannot be configured as a stub area, and the stub area cannot be used as the transmission area of virtual links.
- To set an area as the STUB area, all the routers in the area must be configured with this feature.
- There is no ASBR in stub areas. In other words, the routes outside an autonomous system cannot be propagated in the area.

To configure the OSPF area parameters, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)**#area** *area-id* **authentication**	Set plain-text authentication for the area.
DES-7200 (config-router)**#area** *area-id* **authentication message-digest**	Set MD5 authentication for the area.
DES-7200 (config-router)**#area** *area-id* **stub** [**no-summary**]	Set the area as a stub area. **no-summary:** Set the area as a stub area to prevent the ABR between areas from sending summary-LSAs to the stub area.
DES-7200 (config-router)**#area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the stub area.

Note

For authentication configuration, you need to configure the authentication parameters on an interface. See “Configuring the OSPF Interface Parameters” section in this chapter. You must configure the stub area on all the routers in the area. To configure a full stub area, you also have to configure the full stub area parameters on the border router of the stub area in addition to the basic configuration of stub area. You do not need to change the configuration of other routers.

4.2.5 Configuring the OSPF NSSA

The NSSA (Not-So-Stubby Area) is an expansion of the OSPF stub area. The NSSA also reduces the consumption of the resources of the routers by preventing from flooding the type-5 LSA (AS-external-LSA) to the NSSA. However, unlike the stub area, the NSSA can inject some routes outside the autonomous system to

the routing area of the OSPF.

Through redistribution, the external type-7 routes of the autonomous system are allowed to import to the NSSA. These external type-7 LSAs will be converted into the type-5 LSAs at the border router of the NSSA and flooded to the entire autonomous system. During this process, the external routes can be summarized and filtered.

You should pay attention to the following aspects when you configure the NSSA:

- The backbone area cannot be configured as a NSSA, and the NSSA cannot be used as the transmission area of the virtual links.
- To set an area as the NSSA, all the routers connected to the NSSA must be configured with the NSSA features by using the **area nssa** command.

To configure an area as the NSSA, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)**# area** *area-id* **nssa** [**no-redistribution**] [**no-summary**] [**default-information-originate**[**metric** *metric*][**metric-type** [**1** | **2**]]]	(Optional) Define a NSSA.
DES-7200 (config-router)**#area** *area-id* **default-cost** *cost*	Configure the cost of the default route sent to the NSSA.

The *default-information-originate* parameter is used to generate the default Type-7 LSA. This option varies slightly between the ARR and ASBR of the NSSA. On the ABR, whether there is a default route or not in the routing table, the Type-7 LSA default route will be created. On the other hand, this is only created when there is a default route in the routing table on ASBR.

The **no-redistribution** parameter allows other external routes introduced by using the **redistribute** commands via the OSPF on the ASBR not to be distributed to the NSSA. This option is usually used when the router in the NSSA is both an ASBR and an ABR to prevent external routes from entering the NSSA.

To further reduce the LSAs sent to the NSSA, you can configure the **no-summary** attribute on the ABR to prevent the ABR from sending the **summary LSAs (Type-3 LSA)** to the NSSA.

In addition, the area default-cost is used on the ABR connected to the NSSA. This command configures the cost of the default route sent by the border router to the NSSA. By default, the cost of the default route sent to the NSSA is 1.

4.2.6 Configuring the Route Aggregation

4.2.6.1 Configuring the Route Aggregation between OSPF Areas

The ABR (Area Border Router) has at least two interfaces that belong to different areas, one of which must be the backbone area. The ABR acts as the pivot in the OSPF routing area, and it can advertise the routes of one area to another. If the network addresses of the routes are continual in the area, the border router can advertise only one aggregated route to other areas. The route aggregation between areas greatly reduces the size of the routing table and improves the efficiency of the network.

To configure the route aggregation between areas, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)# **area** *area-id* **range** *ip-address mask* [**advertise** | **not-advertise**] [**cost** *cost*]	Configure route aggregation for the area.

Note

If route aggregation is configured, the detailed routes in this area will not be advertised by the ABR to other areas.

4.2.6.2 Configuring the External Route Aggregation

When the routes are redistributed from other routing process to the OSPF routing process, every route is advertised to the OSPF-enabled router as a separate link status. If the injected route is in the range of continuous IP addresses, the autonomous area border router can advertise only one aggregated route, and thus reducing the size of the routing table.

To configure the external route aggregation, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)# **summary-address** *ip-address mask*[**not-advertise | tag** *tag-id*]	Configure the external route aggregation.

4.2.6.3 Configuring the Control of Adding the Aggregate Route to RIB

The network range after the route aggregation may exceed the actual range in the RIB(Routing Information Base). If the data are sent to the network beyond the aggregation range, it may result in a loop or the greater burden to the router. It needs to add a discard route to the RIB in ABR or ASBR to prevent that problem.

To allow or disalllow to add the discard route to the RIB, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)# **discard-route** {**internal**|**external**}	Allow to add the discard route to the RIB.
DES-7200 (config-router)# **no discard-route** {**internal**|**external**}	Disallow to add the discard route to the RIB.

By default, it allows to add the discard route to the RIB.

4.2.7 Creating the Virtual Links

In the OSPF routing area, the OSPF route updating between non-backbone areas are exchanged via the backbone area to which all the areas are connected. If the backbone area is disconnected, you need to configure the virtual link to connect the backbone area. Otherwise, the network communication will fail. If physical connection cannot be ensured due to the restriction of the network topology, you can also meet this requirement by creating the virtual links.

Virtual links should be created between two ABRs. The common area of the ABRs become the transmit areas. The stub areas and NSSA areas cannot be used as the transit area. The virtual links can be seen as a logical connection channel established between two ABRs via the transit area. On both its ends must be ABRs and configuration must be performed on both ends. The virtual link is identified by the router-id number of the peer router. The area that provides the two ends of a virtual link with an internal non-backbone area route is referred to as the transit area, whose number must be specified at configuration.

The virtual links will be activated after the route in the transit area has been calculated (that is, the route to the other router). You can see it as a point-to-point connection, on which most parameters of the interface can be configured, like a physical interface, for example, **hello-interval** and **dead-interval**.

The “logical channel” means that the multiple routers running the OSPF between the two ABRs only forward packets (If the destination addresses of the protocol packets are not these routers, the packets are transparent to them and are simply

forwarded as common IP packets), and the ABRs exchange route information directly. The route information means the Type-3 LSAs generated by the ABR, and the synchronization mode in the area is not changed as a result.

To create the virtual link, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)# **area** *area-id* **virtual-link** *router-id* [[**hello-interval** *seconds*]| [**retransmit-interval** *seconds*] |[**transmit-delay** *seconds*]|[**dead-interval** *seconds*]| [**authentication** [**message-digest | null**] |[[**authentication-key** *key* | **message-digest-key** *keyid* **md5** *key*]]]	Create a virtual link.

Caution

If the autonomous system is divided into more than one area, one of the areas must be the backbone area to which the other areas must be connected directly or logically. Also, the backbone area must be in good connection.

Note

The *router-id* is the ID of the OSPF neighbor router. If you are not sure of the value of the router-id, you can use the **show ip ospf or show ip ospf neighbor** command to verify it. How to manually configure the router-id, refer to the chapter of *Using the Loopback Address as the Route ID*.

4.2.8 Creating the Default Route

An ASBR can be forced to generate a default route, which is injected to the OSPF routing area. If one router is forced to generate the default route, it will become the ASBR automatically. However, the ASBR will not automatically generate the default route.

To force the ASBR to generate the default route, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)**#default-information**	Generate the default route.

Command	Function
originate [always] [metric *metric-value*] **[metric-type** *type-value*] **[route-map** *map-name*]	

Note

When the stub area is configured, the ABR will generate the default route automatically, and advertise it to all routers within the stub area.

4.2.9 Using the Loopback Address as the Router ID

The OSPF routing process always uses the largest interface IP address as the router ID. If the interface is disabled or the IP address does not exist, the OSPF routing process must calculate the router ID again and send all the route information to the neighbor.

If the loopback (local loop address) is configured, the routing process will select the IP address of the loopback interface as the router ID. If there are multiple loopback interfaces, the largest IP address is selected as the router ID. Since the loopback address always exists, this enhances the stability of the routing table.

To configure the loopback address, execute the following commands in the global configuration mode:

Command	Function
DES-7200 (config)**#interface loopback 1**	Create the loopback interface.
DES-7200 (config-if)**#ip address** *ip-address mask*	Configure the Loopback IP address.

Note

If the OSPF routing process selects the IP address of the common interface as the route identifier, the configuration of the loopback interface will not cause the OSPF process to reselect the identifier.

4.2.10 Changing the Default OSPF Management Distance

The management distance of a route represents the credibility of the source of the route. The management distance ranges from 0 to 255. The greater this value, the smaller the credibility of the source of the route.

The OSPF of DES-7200 product has three types of routes, whose management distances are all 110 by default: intra-area, inter-area, and external. A route belongs to an area is referred to as the intra-area route, and a route to another

area is referred to as the inter-area route. A route to another area (learnt through redistribution) is known as the external route.

To change the OSPF management distance, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200(config-router)# **distance ospf {[inter-area** *dist1*] [**inner-area** *dist2*] [**external** *dist3*]}	Change the OSPF management distance.

4.2.11 Configuring the Route Calculation Timer

When the OSPF routing process receives the route topology change notification, it runs the SPF for route calculation after some time of delay. This delay can be configured, and you can also configure the minimum intervals between two SPF calculations.

To configure the OSPF route calculation timer, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)**#timers throttle spf** *spf-delay spf-holdtime spf-max-waittime*	Configure the route calculation timer.

Spf-delay refers to the delay time from the topology change to SPF calculation. *Spf-holdtime* refers to the minimum time interval between two SPF calculations. The time interval of the consecutive SPF calculations shall at least be twice as the last time interval till the time interval reaches *spf-max-waittime.* If the time interval between two SPF calculations has exceeded the minimum value, then it starts over from the *spf-holdtime* value to calculate the SPF time interval.

Note

Normally, reducing the value of spf-delay and spf-holdtime could speed up the OSPF convergence if the link turbulence occurs occasionally. Setting the spf-max-waittime value can avoid the CPU consumption by the OSPF due to the consecutive link turbulence.

For example: **timers throttle spf** *1000 5,000 100,000.* If the topology changes, the SPF calculations are in the ascend order as follows and do not exceed the *spf-max-waittime*(100,000): 1s，6s，16s，36s，76s，156s，256s，256+100，…

To configure the OSPF route delay time and holdtiime, execute the following commands in the routing process configuration mode:

Command	Function
DES-7200 (config-router)**#timers spf** *spf-delay spf-holdtime*	Configure the route calculation timer, in seconds.

Caution

The configurations of **timers spf** command and **timers throttle spf** command will be overwritten. The latter command configuration takes effect. If neither of the two commands is configured, the default value is the configuration of the **timers throttle spf** command.

The **timers throttle spf** command is more powerful than the **timers spf** command. To this end, it is recommended to use the **timers throttle spf** command.

4.2.12 Changing the LSA Group Pacing Timer

Each LSA has its own refersh and aging time. Calculating the refersh and aging of each LAS respectively consumes lots of CPU. To make full use of CPU, refresh and age the LSAs uniformly.

The default is 4 minutes. This parameter needs not to be adjusted often. The optimum group pacing interval is inversely proportional to the number of LSAs that need to be calculated. For example, if you have approximately 10,000 LSAs in the database, decreasing the pacing interval would be better. If the switch has a small database (40 to 100 LSAs), increasing the pacing interval to 10 to 20 minutes might be better. To configure OSPF LSA pacing, follow these steps in the privileged mode:

Command	Meaning
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200(config)**# router ospf** *1*	Enter the routing protocol configuration mode.
DES-7200 (config-router)**# timers lsa-group-pacing** *seconds*	(Optional) Change the LSAs group pacing.
DES-7200 (config-router)**# end**	Return to the privileged EXEC mode.
DES-7200 **# show running-config**	Verify the configuration.
DES-7200 # **write**	(Optional) Save the configuration.

To restore the settings to the default value, use the **no timers lsa-group-pacing** in the global configuration mode.

4.2.13 Configuring OSPF Interface Cost Value

OSPF calculates the destination route based on the cost, where the route with the least cost is the shortest route. The default route cost is based on network bandwidth. When you configure the OSPF-enabled router, you can set the link cost according to the factors such as link bandwidth, delay or economic cost. The lower its cost, the higher the possibility of that link to be selected as the route. If route aggregation takes place, the maximum cost of all the links are used as the cost of the aggregated route.

Routing configuration includes two parts. In the first place, you set the reference value for the bandwidth generated cost. This value and the interface bandwidth value are used to create the default cost. In the second place, you can set the respective metric of each interface by using the **ip ospf cost** command, so that the default metric is not effective for the interface. For example, the default reference value is 100 Mbps, and an Ethernet interface has the bandwidth of 10Mbps. Other example, the bandwidth is 100Mbps, the bandwidth of an Ethernet interface is 10Mbps, this interface will have the default metric of 100/10 + 0.5 ≈ 10.

The interface cost is selected in the following way in the OSPF protocol. The set interface has the highest priority. If you have set an interface cost, the set value is taken as the interface cost. If you do not set one while the automatic cost generation function is enabled, the interface cost is calculated automatically. If the function is disabled, the default of 10 is taken as the interface cost.

The configuration process is shown as below:

Command	Meaning
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200(config)**# router ospf 1**	Enter the routing protocol configuration mode.
DES-7200(config-router)**#auto-cost [reference-bandwidth** *ref-bw***]**	(Optional) Set the default cost based on the bandwidth on an interface.
DES-7200 (config-router)# **end**	Return to the privileged EXEC mode.
DES-7200 # **show ip protocol**	Display the routing protocol that is running currently.
DES-7200 # **write**	(Optional) Save the configuration.

To remove the setting, use the **no ip ospf cost** or **auto-cost** command.

4.2.14 Configuring OSPF Stub Router

Stub Router is a router that only forwards packets to its directly-connected links. To prevent low-class routers from handling excessive LSAs or to allow routers to

smoothly join/exit the network, we can configure such routers as a Stub Router, which will advertise its maximum metric so that other routers will not preferentially use this device as the transit node during SPF calculation.

After executing "**max-metric router-lsa**" command, the metric of non-stub links carried on the Router LSA generated by the router will be set to the maximum value (0xFFFF). Removing this configuration or timer timeout will restore the links to the default metric.

By default, if this command is enabled, stub links will still advertise the ordinary metric, namely the cost of egress interface. If "**include-stub**" parameter is configured, stub links will advertise the maximum metric.

If an ABR device doesn't want to transmit the traffic of area, use "**summary-lsa**" parameter to configure summary LSA to the maximum metric.

If an ASBR device doesn't want to transmit the external traffic, use "**external-lsa**" parameter to configure external LSA to the maximum metric.

The command of "**max-metric router-lsa**" is generally used in the following circumstances:

- Reload the device. After reloading the device, the IGP protocol will generally converge faster, and other devices will try to forward traffic through the newly reloaded device. If the current device is still building BGP routing tables and certain BGP routes haven't be learned, packets destined for such network will be dropped. In such a case, use "on-startup" parameter to configure a delay timer, so that the device can act as the transmit node after the timer runs out.
- Join the device into network without transmitting traffic. If there are alternate paths, then the current device won't be used to transmit traffic; if there is no alternate path, then the current device will still be used to transmit traffic.
- Gracefully remove the device from the network. By using this command, the current device will advertise a maximum metric value, so that other devices on the network will select the alternate paths to transmit traffic before the device is shut down.

To configure a router to advertise a maximum metric, execute the following commands in routing process configuration mode:

Command	Meaning
DES-7200 **# configure terminal**	Enter the global configuration mode.
DES-7200 (config)**# router ospf** *1*	Enable the OSPF and enter the OSPF configuration mode.
DES-7200 (config-router)# **max-metric router-lsa** [**external-lsa**	(Optional) Configure the router to advertise a maximum metric.

Command	Meaning
[*max-metric-value*]] [**include-stub**] [**on-startup** [*seconds*]] [**summary-lsa** [*max-metric-value*]]	
DES-7200 (config-router)# **end**	Return to the privileged EXEC mode.
DES-7200 # **show ip protocol**	Display the routing protocol that is running currently.
DES-7200 # **write**	(Optional) Save the configuration.

Caution

In the older versions of OSPF (RFC 1247 or earlier versions), links with maximum metric (0xFFFF) in LSA won't participate in SPF calculation, namely no traffic is sent to routers originating these LSAs.

4.2.15 Configuring OSPF MTU-Ignore

When the OSPF receives the database description packet, it will check the MTU of the neighbor against its own. If the interface indicated in the received database description packet has a MTU greater than that of the receiving interface, the neighborhood relationship cannot be established. In this case, you can disable MTU check as a solution.

To disable the MTU check on an interface, you can execute the following command in the interface configuration mode;

Command	Meaning
DES-7200 (config-if)# **ip ospf mtu-ignore**	Configure not to check the MTU value when the interface receives the database description packets.

By default, the MTU check is enabled on an interface.

4.2.16 Disabling Sending the OSPF Packets on the Interface

To prevent other routers in the network from dynamically learning the route information of the router, you can set the specified network interface of the router as a passive interface by using the **passive-interface** command to prevent from sending OSPF packets on the interface.

In the privileged mode, you can configure an interface as a passive interface by performing the following steps:

Command	Meaning
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200(config)**# router ospf 1**	Enter the routing protocol configuration mode (currently RIP and OSPF are supported)
DES-7200 (config-router)# **passive-interface** *interface-name*	(Optional) Set the specified interface as a passive interface.
DES-7200 (config-router)# **passive-interface default**	(Optional) Set all the network interfaces as the passive interfaces
DES-7200 (config-router)**# end**	Return to the privileged EXEC mode.
DES-7200 (config-router)**# write**	Save the configuration.

By default, all interfaces are allowed to receive/send the OSPF packets. To re-enable the network interface to send the route information, you can use the **no passive-interface** *interface-id* command. To re-enable all network interfaces, use the keyword **default.**

4.2.17 Configuring the OSPF Fast Convergence

4.2.17.1 Configuring the OSPF Fast Hello

Enabling OSPF Fast Hello will accelerate OSPF neighbor detection and allow quick detection of lost neighbors. OSPF Fast Hello can be enabled by specifying *"minimal*" and "**hello-multiplier**" key words and "**multiplier**" parameter. "**Minimal**" key word configures the dead interval to 1s, and "**hello-multiplier**" configures the number of hello packets sent during that 1 second, thus providing sub-second hello packets.

When Fast Hello feature is configured on the interface, the hello interval advertised in the hello packets that are sent out this interface is set to 0. The hello interval in the hello packets received over this interface is ignored.

No matter Fast Hello feature is enabled or not, the dead interval must be consistent on a network segment. The hello-multiplier needs not to be the same for the entire segment as long as at least one hello packet is received within the dead interval.

Configure Fast Hello feature on the interface:

Command	Function
DES-7200**# configure terminal**	Enter global configuration mode.
DES-7200(config)**# ip routing**	Enable routing (if it is disabled)
DES-7200(config)# **interface**	Enter interface configuration mode.

Command	Function
interface-id	
DES-7200(config-if)# **ip ospf dead-interval minimal hello-multiplier** *multiplier*	(Optional) Enable OSPF Fast Hello.
DES-7200 (config-if)# **end**	Return to privileged mode.
DES-7200 # **show ip ospf** [*process-id*]**interface** [*interface-id*]	Display OSPF interface information.
DES-7200 # **write**	Save configurations.

Configure Fast Hello feature on the virtual link:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200 (config)# **ip routing**	Enable routing (if it is disabled)
DES-7200 (config)# **router ospf** *process_id* [**vrf** *vrf-name*]	Enable OSPF and enter OSPF configuration mode.
DES-7200 (config-router)# **area** *area-id* **virtual-link** *router-id* [**dead-interval** | **minimal hello-multiplier** *multiplier*]	Configure Fast Hello feature on the virtual link
DES-7200 (config-router)# **end**	Return to privileged mode.
DES-7200 # **write**	Save configurations.

Caution

While configuring Fast Hello, "**dead-interval minimal hello-multiplier**" parameter and "**hello-interval**" parameter must not be configured at the same time.

4.2.17.2 Configuring the OSPF Two-way Maintenance

In a large-sized network, substantive packets may be received and transmitted, thus occupying excessive CPU and memory resources and causing the delay or drop of certain packets. If the processing time of Hello packets exceeds the dead interval, the corresponding neighbor will be disconnected. After enabling the feature of two-way maintenance, besides hello packets, DD, LSU, LSR and LSAck packets from a specific neighbor can also be used to maintain the two-way adjacency of this neighbor if there are substantive packets on the network, thus avoiding the loss of neighbors caused by the delay or drop of hello packets.

OSPF two-way maintenance is enabled by default. In routing process configuration mode, execute the following commands to disable OSPF two-way maintenance:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **router ospf** *1*	Enter routing protocol configuration mode.
DES-7200(config-router)# **no two-way-maintain**	(Optional) Disable OSPF two-way maintenance.
DES-7200 (config-if)# **end**	Return to privileged mode.
DES-7200 # **write**	Save configurations.

4.2.17.3 Configuring the Interval of Accepting the Same LSA

In a broadcasting network or the environment featured by frequent network oscillation, the device may receive the same LSA updates from different neighbors on one or multiple interfaces. If the same LSAs received are handled every time, excessive system resources may be wasted. OSPF protocol requires that the same LSAs received will only be considered valid after a period of time. The same LSAs received within a short periods of time will be ignored. This time interval is the constant MinLSArrival with value being 1s.

Different types of networks will have different requirements on the interval for handling LSA changes. The user can configure this parameter according to different network planning and performance requirements in order to optimize the network.

In routing process configuration mode, the user can execute the following commands to configure the interval of accepting the same LSA:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **router ospf** *1*	Enter routing protocol configuration mode.
DES-7200(config-router)# **timers lsa arrival** *arrival-time*	(Optional) Configure the interval of accepting the same LSA. The default value is 1000 milliseconds.
DES-7200 (config-if)# **end**	Return to privileged mode.
DES-7200 # **write**	Save configurations.

4.2.17.4 Configuring the LSA to Send the packet updates

To avoid the impacts on network devices caused by the flooding of a number of update packets, the feature of LSP packet update is introduced. By controlling the inter-packet spacing between substantive update packets, the LSAs to be flooded during this period can be collected, so that these LSAs can be sent with the least number of packets. Meanwhile, the CPU resources can be saved to handle other tasks and the system performance can be optimized.

When there are excessive LSAs on the network and the device is suffering from excessive loads, the "transmit-time" and "transmit-count" shall be properly configured to control the number of LS-UPD packets flooded on the network. When the load of CPU and network bandwidth is not too high, you can reduce "transmit-time" and increase "transmit-count" in order to accelerate network convergence. In routing process configuration mode, the user can execute the following commands to configure LSA to send packet updates:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **router ospf** *1*	Enter routing protocol configuration mode.
DES-7200(config-router)# **timers pacing lsa-transmit** *transmit-time transmit-count*	(Optional) Configure LSA to send packet updates.
DES-7200 (config-if)# **end**	Return to privileged mode.
DES-7200 # **write**	Save configurations.

4.2.17.5 Configuring the LSA to Send the packet updates

To prevent multiple events from triggering the same LSAs within a short time and consuming excess CPU resources, OSPF protocol has defined the minimum time interval of "MinLSInterval" for LSA generation, with default value being 5 seconds. During this time, the same LSA instances cannot be generated repeatedly. The purpose for configuring this interval is to prevent frequent LSA oscillation from causing impacts to the network. However, such a limit will slow down LSA generation and fail to advertise the changes in network topology.

To quickly respond to the changes in network topology and avoid excessively frequent route calculation, we can use rate-limiting algorithm to dynamically change the interval for LSA generation. The command of "timers throttle lsa all" has three parameters: initial interval, hold interval and maximum interval, which allow the system to automatically adjust the interval for LSA generation according to the extent of frequent changes in network topology. Generally, "delay-time" is

set to 0 or a small value, so that LSA instances can be generated immediately when the network topology is comparatively stable; when the network topology changes frequently, the interval for LSA generation will increase from "hold-time" following the algorithm of hold-time×2n-1. N refers to the number of changes. With the increase in the number of repeated LSA generation, the interval for generation will become larger and larger until the "maximum interval" is reached. When the interval for LSA generation is larger than the "max-wait-time", the "delay-time" for generating this LSA will restore to the initial interval.

By default, the initial interval is 0 millisecond, the hold time is 5000 milliseconds, and the maximum interval is 5000 milliseconds. In this way, the shortest interval for consecutively generating the same LSA is MinLSInterval, which complies with RFC 2328.

In routing process configuration mode, the user can execute the following commands to configure LSA generation rate-limiting algorithm:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **router ospf** *1*	Enter routing protocol configuration mode.
DES-7200(config-router)# **timers throttle lsa all** *delay-time hold-time max-wait-time*	(Optional) Configure LSA generation rate-limiting algorithm. By default, the initial interval is 0 millisecond, the hold time is 5000 milliseconds, and the maximum interval is 5000 milliseconds.
DES-7200 (config-if)# **end**	Return to privileged mode.
DES-7200 # **write**	Save configurations.

Caution

While configuring this command, the "hold-time" cannot be smaller than the "delay-time", and the "max-wait-time" cannot be smaller than "hold-time".

4.2.18 Configuring OSPF Load Protection

When the memory lacks, OSPF enters the overflow state. In the overflow state, OSPF protocol will:

- For the learned LSA: receive the Inter-Area/Intra-Area LSA; receive the external LSA if the destination route address represented by LSA is for the non-default learned route; not receive other LSAs.
- For the external LSA generated by itself: clear the external LSAs except for the default route.

- The incompletemess of route learning and advertisement may lead to the route loop in the network. OSPF will generate a default route that is destined to the NULL port to prevent the route loop. The generated default route exists in the overflow state all the time.

You can configure the overflow memory-lack in the OSPF configuration mode:

Command	Function
DES-7200(config)**#router ospf** *process-id*	Enter the OSPF configuration mode.
DES-7200(config-router)**#overflow memory-lack**	When the memory lacks, OSPF enters the overflow state.

Note

By default, OSPF enters the overflow state automatically when the memory lacks. Use the **no overflow memory-lack** command to disable OSPF to enter the overflow state.

Caution

To exit from the overflow state, you must use the **clear ip ospf process** command, or restart the OSPF protocol.

4.2.19 Configuring the OSPF Network Management

4.2.19.1 Configuring the OSPFv2 MIB Binding

The user can only operate a sole OSPFv2 process by SNMP since the OSPFv2 MIB itself does not have the OSPFv2 process information. By default, OSPFv2 MIB is binded with the OSPFv2 process in the smallest number, and all user operations take effect for this process.

The user can bind OSPFv2 MIB to the process manually if he/she wants to operate the specified OSPFv2 process by SNMP.

In the routing process configuration mode, execute the following command:

Command	Function
DES-7200 (config-router)**#enable mib-binding**	Bind the OSPFv2 MIB to the specified OSPFv2 process.

4.2.19.2 Configuring the OSPFv2 TRAP Message

The OSPFv2 protocol defines several types of the OSPF TRAP messages, which are used to send the TRAP message to the SNMP server when part of the network configuration changes and some OPSF event occurs for the network management. Sending OSPFv2 TRAP messages is not limited by binding the OSPFv2 process and OSPFv2 MIB. The TRAP switch can be enabled by different processes at the same time.

In the global configuration mode, execute the following command:

Command	Function
DES-7200 # configure terminal	Enter the global configuration mode.
DES-7200 (config)# **snmp-server host** *host-ip* **version** *version-no string* **[ospf**]	Configure the SNMP server to receive the TRAP. *host-ip:* the address corresponding to the SNMP server. *version-no*: the SNMP version corresponding to the SNMP server. *string*: the communication authentication code of SNMP, which is generally public. The optional parameter ospf means that the SNMP server receives the OSPF TRAP message (by default, the SNMP server receives all types of TRAP messages).
DES-7200 (config)# **snmp-server enable traps ospf**	Enable the OSPF TRAP sending switch.
DES-7200 (config)**#router ospf** *process_id* [**vrf** *vrf-name*]	Enable OSPF, enter the OSPF configuration mode.
DES-7200 (config-router)# **enable traps** [**error** [**ifauthfailure | ifconfigerror | ifrxbadpacket | virtifauthfailure | virtifconfigerror | virtifrxbadpacket**] | **lsa** [**lsdbapproachoverflow | lsdboverflow | maxagelsa | originatelsa**] | **retransmit** [**iftxretransmit | virtiftxretransmit**] | **state-change** [**ifstatechange | nbrstatechange | virtifstatechange | virtnbrstatechange**]]	Enable the specified OSPF TRAP switch.

Command	Function
DES-7200 (config)**# end**	Return to the privileged mode.
DES-7200**# write**	Save the configuration.

4.2.20 Configuring the OSPF GR

4.2.20.1 Principles of OSPF GR

OSPF GR standard:

RFC3623: Graceful OSPF Restart

RFC3623 principles:

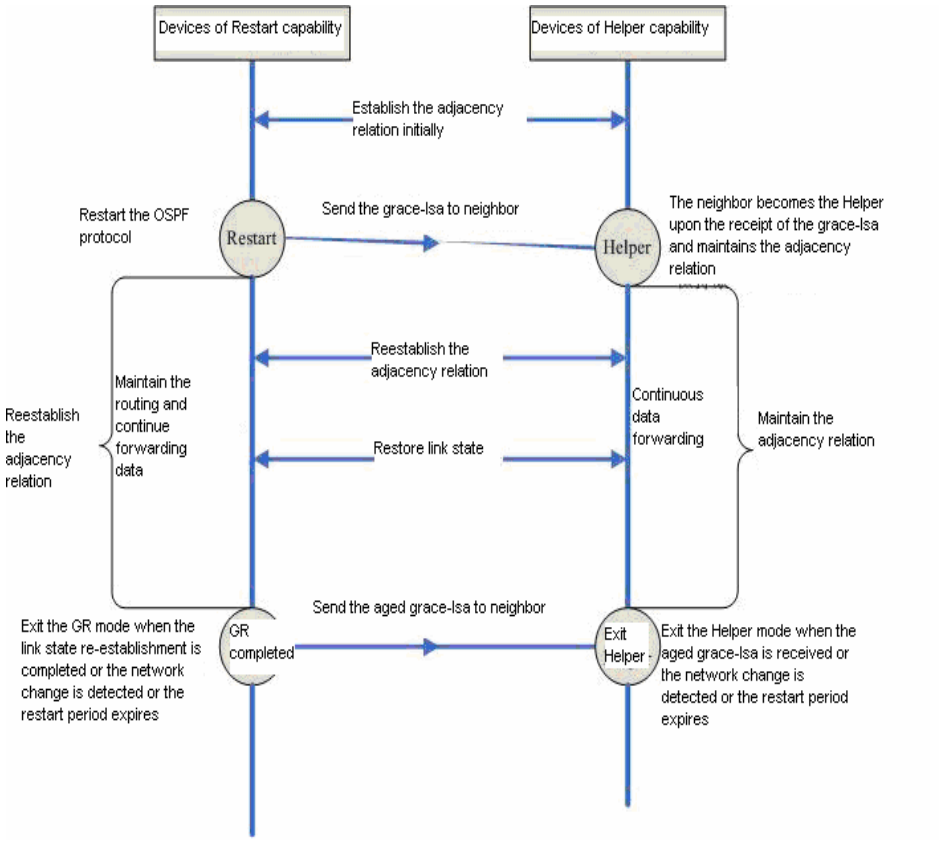
As the standard GR protocol that IETF defines for OSPF, RFC3623 defines the conditions, operations and precautions need to meet for the execution of Graceful Restart. As specified in RFC3623, two GR principles are curcial. Namely, network topology should be stable and the router can maintain the routing table during restarting OSPF.

The execution of OSPF GR is not an independent process. Functionally, it falls into GR Restart capability and GR Help capability. The device of GR Restart capability can autonomously execute graceful restart, and the device of GR Help capability can receive Grace_LSA and heop its neighbors to execue graceful restart.

The GR Restart capability depends on products. The GR of routing protocol generally is used to enhance the availability of the system where the control panel and the forwarding panel are separated for continous forwarding.

The GR Help capability depends on software. If the software supports OSPF GR, then the device is of the GR Help capability.

Generally, the device of the GR Restart capability that is executing GR is refered to the GR Restarter, and the one of the GR Help capability that is helping the GR Restarter to execute GR is called the GR Helper. The GR process begins by the GR Restarter’s sending the Grace LSA. The neighbor becomes the GR Helper upon the receipt of the Grace LSA and assists the GR Restarter to reestablish the adjacency relation. Meanwhile, the neighbor maintains the adjacency relation with the GR Restarter for continous data forwarding.



The above figure briefly outlines the execution of OSPF GR. The GR period is the longest time of establishing link status. When the link is reestablished or the graceful restart period times out, the GR Restater exits the execution of GR.

4.2.20.2 Configuring the OSPF GR Restarter

To configure the GR period, execute the **graceful-restart** command:

Command	Function
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config)# **router ospf** *1*	Enter the OSPF configuration mode.
DES-7200 (config-router)# **graceful-restart**	Enable OSPF GR.
DES-7200 (config-router)# **end**	Exit to the privileged EXEC mode.
DES-7200 # **show running-config**	View the configuration.
DES-7200# **write**	(Optional) Save the configuration.

By default, the GR period is 120s. To modify the GR period, execute the **graceful-restart grace-period** command:

Command	Function
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config)# **router ospf** *1*	Enter the OSPF configuration mode.
DES-7200 (config-router)# **graceful-restart grace-period** *100*	Enable OSPF GR and set its GR period to 100s.
DES-7200 (config-router)# **end**	Exit to the privileged EXEC mode.
DES-7200 # **show running-config**	View the configuration.
DES-7200# **write**	(Optional) Save the configuration.

4.2.20.3 Configuring the OSPF GR Helper

By default, the OSPF GR Helper is enabled. You are allowed to disable the GR Helper capabiltiy and configure the GR Helper to detect network change:

Command	Function
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config)# **router ospf** *1*	Enter the OSPF configuration mode.
DES-7200 (config-router)# **graceful-restart helper disable**	Disable the OSPF GR Helper.
DES-7200 (config-router)# **no graceful-restart helper disable**	Enable the GR Helper again.
DES-7200 (config-router)# **graceful-restart helper** {**strict-lsa-checking** | **internal-lsa-checking**}	Enable the OSPF GR Helper to check the change of LSA. If the network changes, exit the GR Helper. By default, the changes of network are not detected during the GR Helper. **strict-lsa-checking**: check the changes of types1 to 5 and type 7 LSAs **internal-lsa-checking**: check the changes of types1 to 3 LSAs
DES-7200 (config-router)# **end**	Exit to the privileged EXEC mode.
DES-7200 # **show running-config**	View the configuration.
DES-7200# **write**	(Optional) Save the configuration.

4.2.21 Configuring OSPF BFD

For details, refer to *BFD Configuration Guide*.

4.2.22 Configuring the OSPF VPN

Please refer to *Configure OSPF VPN extension* for details about OSPF VPN configuration.

4.3 Monitoring and Maintaining OSPF

You can show the data such as the routing table, cache, and database of the OSPF. The following table lists some of that data that can be shown for your reference.

Command	Meaning
DES-7200# **show ip ospf** [*process-id*]	Show the general information of the OSPF protocol for corresponding processes. It will display all processes if the process number is not specified.
DES-7200# **show ip ospf** [*process-id area-id*] **database** [**adv-router** *ip-address* | {**asbr-summary** | **external** | **network** | **nssa-external | opaque-area | opaque-as | opaque-link | router** | **summary**} [*link-state-id*] [{**adv-router** *ip-address* | **self-originate}**] | **database-summary** | **max-age** | **self-originate**]	Show OSPF database information. Show the information of each type of LSAs of the specified process.
DES-7200# **show ip ospf** [*process-id*] **border-routers**	Show the route information when the specified process reaches the ABR and ASBR.
DES-7200# **show ip ospf interface** [*interface-name*]	Show the information on the interface participating in the OSPF routing.
DES-7200# **show ip ospf** [*process-id*] **neighbor**[*interface-name*] [*neighbor-id*] **[detail]**	Show the information of the adjacent routers of the interface. *interface-name*: The local interface connected to the neighbor *neighbor-id*: The router ID of the neighbor.
DES-7200# **show ip ospf** [*process-id*] **virtual-links**	View the virtual link information of the specified process.
DES-7200# **show ip ospf** [*process-id*] **route [count]**	Show the routes of the OSPF routing table.

For the explanations of the commands, see *IP Routing Protocol Configuration Command Reference*. There are the following common monitoring and

maintenance commands:

1. Show the status of the OSPF neighbor

Use the **show ip ospf** [*process-id*] **neighbor** to show all neighbor information of the OSPF process, including the status of neighbor, role, router ID and IP address, BFD state, ect.

```
DES-7200# show ip ospf neighbor

 OSPF process 1:
 Neighbor ID  Pri State  BFD State Dead Time Address:     Interface
 10.10.10.50 1 Full/DR  UP 00:00:38     10.10.10.50  eth0/0
 OSPF process 100:
 Neighbor ID  Pri State  BFD State  Dead Time    Address I    interface
 10.10.11.50 1    Full/Backup  DOWN 00:00:31    10.10.11.50  eth0/1

DES-7200# show ip ospf 1 neighbor

 OSPF process 1:
 Neighbor ID  Pri State  BFD State Dead Time Address:     Interface
 10.10.10.50 1    Full/DR      UP 00:00:38  10.10.10.50  eth0/0

DES-7200# show ip ospf 100 neighbor

 OSPF process 100:
 Neighbor ID  Pri State    BFD State Dead Time   Address:     Interface
 10.10.11.50 1    Full/Backup  DOWN 00:00:31    10.10.11.50  eth0/1
```

2. Show the OSPF interface status

The following message shows that the F0/1 port belongs to area 0 of the OSPF, and the router ID is 172.16.120.1. The network type is “BROADCAST”-broadcast type. You must pay special attention to the parameters such as Area, Network Type, Hello and Dead. If these parameters are different from the neighbor, no neighborhood relationship will be established.

```
DES-7200# sh ip ospf interface fastEthernet 1/0
FastEthernet 1/0 is up, line protocol is up
Internet Address 192.168.1.1/24, Ifindex: 2 Area 0.0.0.0, MTU 1500
Matching network config: 192.168.1.0/24,
Process ID 1, Router ID 192.168.1.1, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State DR, Priority 1
Designated Router (ID) 192.168.1.1, Interface Address 192.168.1.1
Backup Designated Router (ID) 192.168.1.2, Interface Address 192.168.1.2
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 00:00:04
Neighbor Count is 1, Adjacent neighbor count is 1
Crypt Sequence Number is 30
Hello received 972 sent 990, DD received 3 sent 4
LS-Req received 1 sent 1, LS-Upd received 10 sent 26
LS-Ack received 25 sent 7, Discarded 0
```

3. Show the information of the OSPF routing process

The following command shows the route ID, router type, area information, area summary, and other related information.

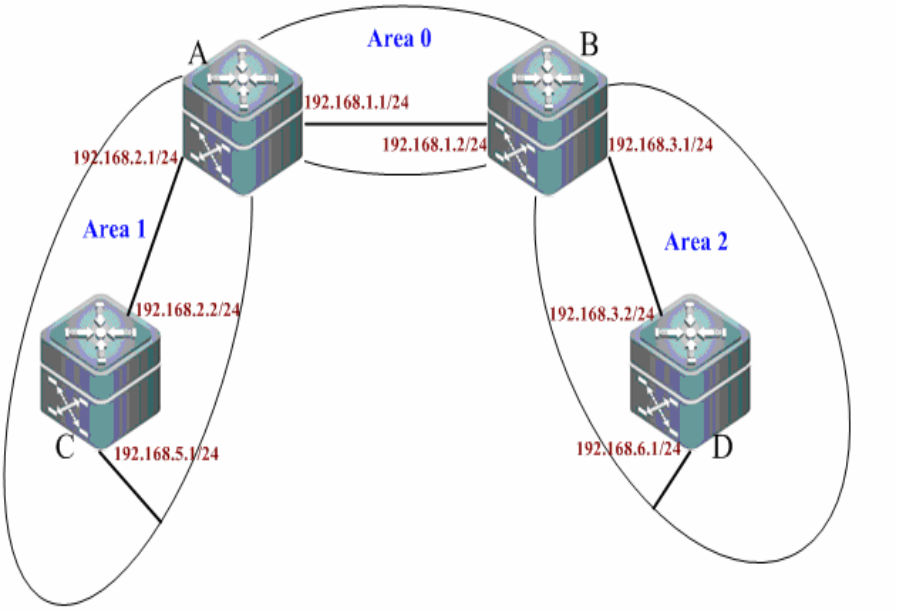
```
DES-7200 # show ip ospf

 Routing Process "ospf 1" with ID 1.1.1.1
 Process uptime is 4 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 This router is an ASBR (injecting external route information)
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 LsaGroupPacing: 240 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 4. Checksum 0x0278E0
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 4
 External LSA database is unlimited.
 Number of LSA originated 6
 Number of LSA received 2
 Log Neighbor Adjency Changes : Enabled
 Number of areas attached to this router: 1
 rea 0 (BACKBONE)
 Number of interfaces in this area is 1(1)
 Number of fully adjacent neighbors in this area is 1
 Area has no authentication
 SPF algorithm last executed 00:01:26.640 ago
 SPF algorithm executed 4 times
 Number of LSA 3. Checksum 0x0204bf
 Routing Process "ospf 20" with ID 2.2.2.2
 Process uptime is 4 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 LsaGroupPacing: 240 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 umber of non-default external LSA 0
 External LSA database is unlimited.
 umber of LSA originated 0
 Number of LSA received 0
 Log Neighbor Adjency Changes : Enabled
 Number of areas attached to this router: 0
```

4.4 OSPF Configuration Examples

4.4.1 Multi-area OSPF Configuration Example

Topological diagram

The following figure shows the networking diagram for OSPF autonomous system. The entire autonomous system is divided into three areas: area 0, area 1 and area 2. OSPF protocol is running on respective devices.



- **Networking diagram for multi-area OSPF configuration**

Application needs

Configure Switch C and Switch B as area border routers (ABR) and Switch C and Switch D as intra-AS devices. Through OSPF basic configurations, every switch can successfully learn the routes to all network segments.

Configuration tips

- Configure the IP address of respective interfaces
- Enable routing (disabled by default)
- Create OSPF routing process
- Specify the IP address range associated with this routing process and the OPPF area to which these IP addresses belong.

Configuration Steps

- Configure A

Step 1: Configure IP address of the interface

```
A(config)#interface gigabitEthernet 0/1
A(config-if-GigabitEthernet 0/1)#ip address 192.168.1.1 255.255.255.0
A(config-if-GigabitEthernet 0/1)#exit
A(config)#interface gigabitEthernet 0/2
A(config-if-GigabitEthernet 0/2)#ip address 192.168.2.1 255.255.255.0
A(config-if-GigabitEthernet 0/2)#exit
```

Step 2: Configure OSPF basic features

```
A(config)#router ospf 1
A(config-router)#network 192.168.1.0 0.0.0.255 area 0
A(config-router)#network 192.168.2.0 0.0.0.255 area 1
```

- Configure B

Step 1: Configure IP address of the interface

```
B(config)#interface gigabitEthernet 0/1
B(config-if-GigabitEthernet 0/1)#ip address 192.168.1.2 255.255.255.0
B(config-if-GigabitEthernet 0/1)#exit
B(config)#interface gigabitEthernet 0/2
B(config-if-GigabitEthernet 0/2)#ip address 192.168.3.1 255.255.255.0
B(config-if-GigabitEthernet 0/2)#exit
```

Step 2: Configure OSPF basic features

```
B(config)#router ospf 1
B(config-router)#network 192.168.1.0 0.0.0.255 area 0
B(config-router)#network 192.168.3.0 0.0.0.255 area 2
```

- Configure C

Step 1: Configure IP address of the interface

```
C(config)#interface gigabitEthernet 0/3
C(config-if-GigabitEthernet 0/3)#ip address 192.168.2.2 255.255.255.0
C(config-if-GigabitEthernet 0/3)#exit
C(config)#interface gigabitEthernet 0/4
C(config-if-GigabitEthernet 0/4)#ip address 192.168.5.1 255.255.255.0
C(config-if-GigabitEthernet 0/4)#exit
```

Step 2: Configure OSPF basic features

```
C(config)#router ospf 1
C(config-router)#network 192.168.2.0 0.0.0.255 area 1
C(config-router)#network 192.168.5.0 0.0.0.255 area 1
```

- Configure D

Step 1: Configure IP address of the interface

```
D(config)#interface gigabitEthernet 0/3
D(config-if-GigabitEthernet 0/3)#ip address 192.168.3.2 255.255.255.0
D(config-if-GigabitEthernet 0/3)#exit
D(config)#interface gigabitEthernet 0/4
D(config-if-GigabitEthernet 0/4)#ip address 192.168.6.1 255.255.255.0
D(config-if-GigabitEthernet 0/4)#exit
```

Step 2: Configure OSPF basic features

```
D(config)#router ospf 1
D(config-router)#network 192.168.3.0 0.0.0.255 area 2
D(config-router)#network 192.168.6.0 0.0.0.255 area 2
```

Verify configurations

Step 1: Display information about neighbors (taking A/B as the example)

```
A#show ip ospf neighbor

OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID  Pri  State   Dead Time  Address        Interface
192.168.1.2 1  Full/DR  00:00:40 192.168.1.2 GigabitEthernet 0/1
192.168.2.2 1 Full/BDR  00:00:34 192.168.2.2  GigabitEthernet 0/2

B#show ip ospf neighbor

OSPF process 1, 2 Neighbors, 2 is Full:
Neighbor ID Pri  State Dead Time  Address        Interface
192.168.1.1 1 Full/BDR  00:00:32 192.168.1.1  GigabitEthernet 0/1
192.168.3.2 1 Full/BDR  00:00:30 192.168.3.2  GigabitEthernet 0/2
```

Step 2: Display OSPF routing information of A

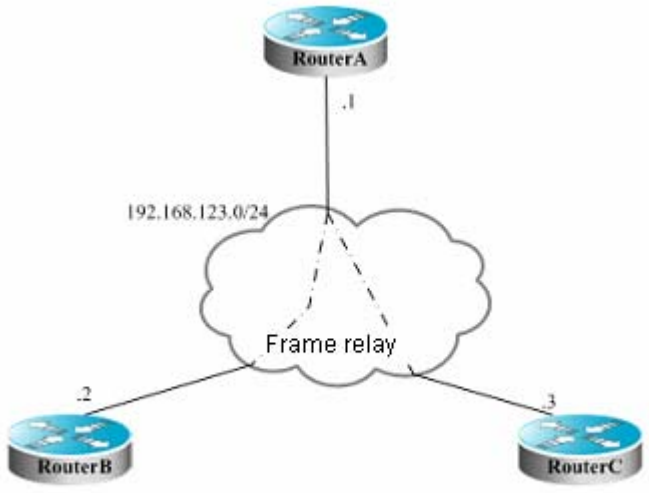
```
SwitchA#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C   192.168.1.0/24 is directly connected, GigabitEthernet 0/1
```

```
C    192.168.1.1/32 is local host.
C    192.168.2.0/24 is directly connected, GigabitEthernet 0/2
C    192.168.2.1/32 is local host.
O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 00:18:03, GigabitEthernet 0/1
//inter-AS route
O    192.168.5.0/24 [110/2] via 192.168.2.2, 00:00:02, GigabitEthernet 0/2
O IA 192.168.6.0/24 [110/3] via 192.168.1.2, 00:01:02, GigabitEthernet 0/1
//inter-AS route

Switch#show ip route

Gateway of last resort is no set
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
//inter-AS route
C    192.168.2.0/24 is directly connected, GigabitEthernet 0/3
C    192.168.2.2/32 is local host.
O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:19:05, GigabitEthernet 0/3
C    192.168.5.0/24 is directly connected, GigabitEthernet 0/4
C    192.168.5.1/32 is local host.
O IA 192.168.6.0/24 [110/4] via 192.168.2.1, 00:03:19, GigabitEthernet 0/3
//inter-AS route
```

4.4.2 OSPF NBMA Network Type Configuration Example

Requirements

Full mesh connection of three devices needs to be realized through frame relay network. Every device has only one frame relay link. The link bandwidth is the same as PVC rate. IP address assignment and device connections are shown in Fig 2.



OSPF NBMA network type configuration example

Requirements:

Configure NBMA network between A, B and C;

Device A is the designated router, and Device B is the backup designated router;

All networks are in the same area;

Quicken topological convergence.

Detailed configurations

Since there is no special configuration about OSPF, we will use multicasting to detect neighbors. If the interface is configured with the network type of NBMA, then the interface won't send OSPF multicast packets. Therefore, the IP addresses of neighbors shall be specified. You can configure shorter SPF hold-time to quicken topological convergence.

Configurations on Device A:

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 10
```

Configure OSPF routing protocol; the cost to reach device B is smaller.

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.2     priority 5
neighbor 192.168.123.3
timers throttle spf 500 1000 10000
```

Configurations on device B:

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
ip ospf priority 5
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
```

```
neighbor 192.168.123.1 priority 10
neighbor 192.168.123.3
timers throttle spf 500 1000 10000
```

Configurations on device C:

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
ip ospf network non-broadcast
```

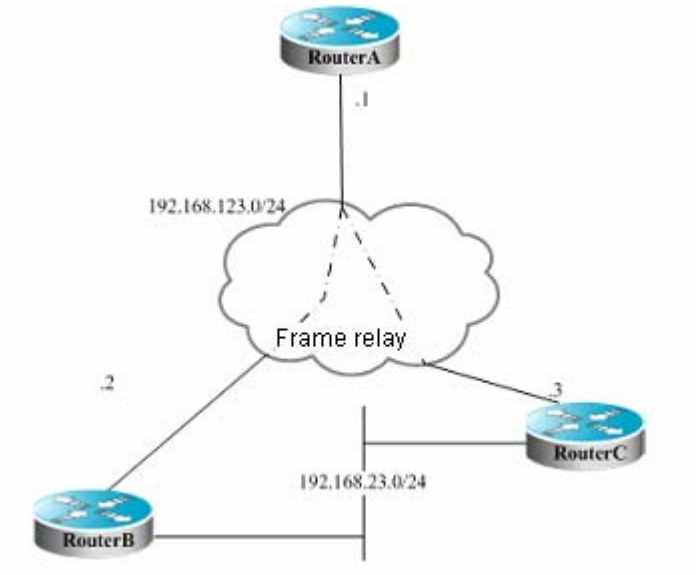
Configure OSPF routing protocol

```
router ospf 1
network 192.168.123.0 0.0.0.255 area 0
neighbor 192.168.123.1 10
neighbor 192.168.123.2 5
timers throttle spf 500 1000 10000
```

4.4.3 OSPF Point-to-multipoint Broadcasting Network type Configuration Example

Requirements

Three devices need to be interconnected through frame relay. Every device has only one frame relay link. The link bandwidth is the same as PVC rate. IP address assignment and device connections are shown in Fig 3.



- **OSPF point-to-multipoint network type configuration example**

Requirements:

Configure point-to-multipoint network between A, B and C.

Detailed configurations

If the interface is configured with point-to-multipoint network type, and there is no process of designed router election, than OSPF operations are very similar to the behaviors of point-to-point network type.

Configurations on Device A:

Configure Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.12.1 255.255.255.0
```

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.123.1 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

Configurations on device B:

Configure Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.23.2 255.255.255.0
```

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.123.2 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

Configurations on device C:

Configure Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.23.3 255.255.255.0
```

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.123.3 255.255.255.0
encapsulation frame-relay
ip ospf network point-to-multipoint
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.123.0 0.0.0.255 area 0
```

Assuming that there is another requirement for the above figure:

Device A shall give preference to device B to reach the destination network of 192.168.23.0/24. To achieve this goal, the cost of neighbor shall be specified while configuring this neighbor.

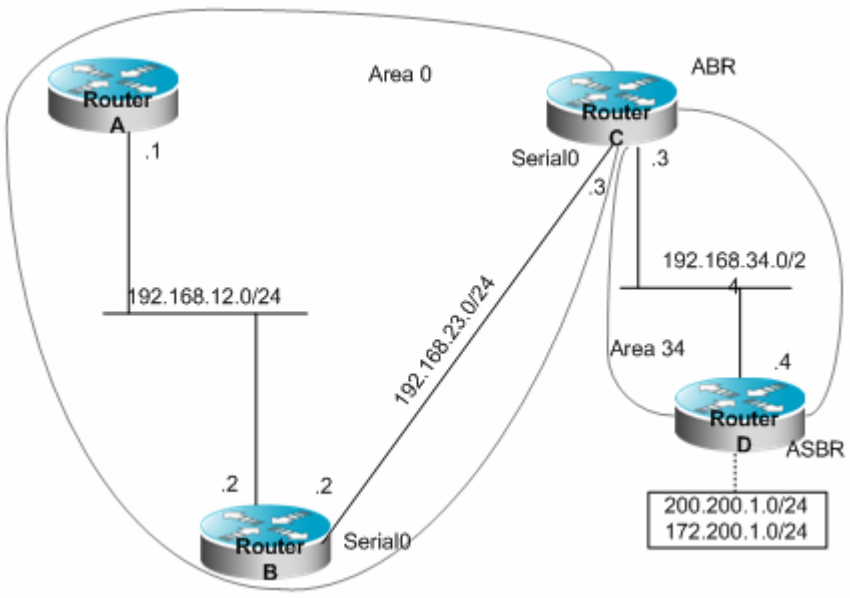
Execute the following commands on device A:

```
router ospf 1
neighbor 192.168.123.2 cost 100
neighbor 192.168.123.3 cost 200
```

4.4.4 OSPF ABR/ASBR Configuration Example

Requirements

Four devices form a OSPF routing domain. Network 192.168.12.0/24 and 192.168.23.0/24 belong to area 0, and network 192.168.34.0/24 belongs to area 34. Details about IP address assignment and device connection are shown in Fig 6.



OSPF ABR/ASBR configuration example

As shown above, device A and device B are intra-area routers; device C is an area border router; device D is a AS boundary router. 200.200.1.0/24 and 172.200.1.0/24 are network segments outside the OSPF routing domain. All OSPF devices shall be able to learn external routes after configuration. External routes shall type 1 routes carry "34" tag.

Detailed configurations

While OSPF redistributes routes from other sources, it will by default redistribute type-II routes carrying no tag.

Configurations on Device A:

Configure Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.1 255.255.255.0
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
```

Configurations on device B:

Configure Ethernet interface

```
interface FastEthernet0/0
ip address 192.168.12.2 255.255.255.0
```

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.23.2 255.255.255.0
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.12.0 0.0.0.255 area 0
network 192.168.23.0 0.0.0.255 area 0
```

Configurations on device C:

Configure Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.34.3 255.255.255.0
```

Configure WAN interface

```
interface Serial 1/0
ip address 192.168.23.3 255.255.255.0
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.23.0 0.0.0.255 area 0
network 192.168.34.0 0.0.0.255 area 34
```

Configurations on Switch D:

Configure Ethernet interface

```
interface FastEthernet 0/0
ip address 192.168.34.4 255.255.255.0
```

Configure ports on Ethernet adapter

```
interface FastEthernet 1/0
ip address 200.200.1.1 255.255.255.0
interface FastEthernet 1/1
ip address 172.200.1.1 255.255.255.0
```

Configure OSPF routing protocol and redistribute RIP routes

```
router ospf 1
network 192.168.34.0 0.0.0.255 area 34
redistribute rip metric-type 1 subnets tag 34
```

Configure RIP routing protocol

```
router rip
network 200.200.1.0
network 172.200.0.0
```

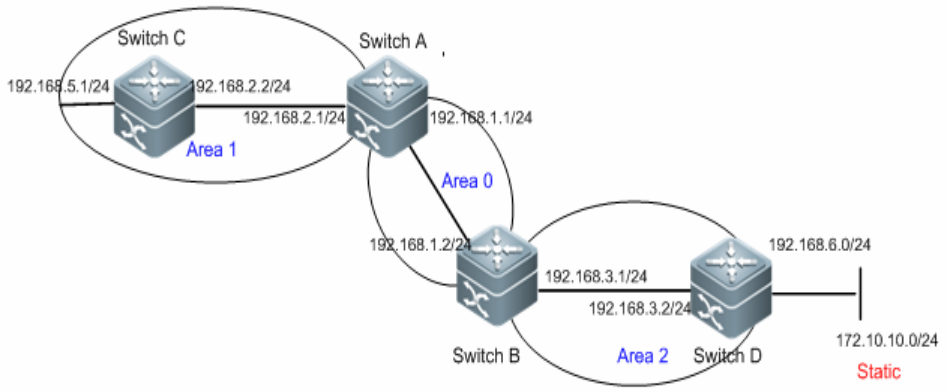
The OSPF routes generated on device B are shown below. Please note that the type of external routes has changed to E1.

```
O E1 200.200.1.0/24 [110/85] via 192.168.23.3,00:00:33,Serial1/0
O IA 192.168.34.0/24 [110/65] via 192.168.23.3,00:00:33,Serial1/0
O E1 172.200.1.0 [110/85] via 192.168.23.3,00:00:33,Serial1/0
```

4.4.5 OSPF Static Route Redistribution Configuration Example

Topological diagram

The following figure shows the networking diagram for OSPF autonomous system. The entire autonomous system is divided into three areas: area 0, area 1 and area 2. Segment 172.10.10.0 is outside the routing domain.



Networking diagram for OSPF static route redistribution configuration

Application needs

Configure Switch A and Switch B as area border routers (ABR) and Switch C as intra-area device. Configure Switch D as ASBR and introduce one external static route, so that all OSPF devices in non-stub area can successfully learn this external route.

Configuration tips

Configure the IP address of respective interfaces (omitted)

Configure OSPF basic features (see "Multi-area OSPF configuration example")

Configure to introduce external static route

Configuration Steps

Step 1: On Switch D, configure a static route to the destination network segment of 172.10.10.0

```
SwitchD(config)#ip route 172.10.10.0 255.255.255.0 192.168.6.2
```

Step 2: Display the routing table of Switch A

```
SwitchA#show ip route ospf
O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 15:33:00, GigabitEthernet 0/1
O    192.168.5.0/24 [110/2] via 192.168.2.2, 15:14:59, GigabitEthernet 0/2
O IA 192.168.6.0/24 [110/3] via 192.168.1.2, 00:17:58, GigabitEthernet 0/1
```

From the above information, we can see that there is no route to the network segment of 172.10.10.0

Step 3: Configure static route redistribution on Switch D

```
SwitchD(config)#router ospf 1
SwitchD(config-router)# redistribute static subnets
```

Verify configurations

Step 1: Display routing table of Switch D

```
SwitchD#show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    172.10.10.0/24 [1/0] via 192.168.6.2  //static route
O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 15:25:19, GigabitEthernet 0/3
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 15:25:19, GigabitEthernet 0/3
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/3
C    192.168.3.2/32 is local host.
O IA 192.168.5.0/24 [110/4] via 192.168.3.1, 15:11:56, GigabitEthernet 0/3
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/4
C    192.168.6.1/32 is local host.
```

Step 2: View OSPF information of Switch D. Key point: Switch D is a AS boundary router (ASBR).

```
SwitchD#show ip ospf
 Routing Process "ospf 1" with ID 192.168.3.2
 Process uptime is 15 hours 27 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Enable two-way-maintain
 This router is an ASBR (injecting external routing information)
 Initial SPF schedule delay 1000 msecs
 Minimum hold time between two consecutive SPFs 5000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 0 msecs
 Minimum hold time for LSA throttle 5000 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Lsa Transmit Pacing timer 40 msecs, 10 LS-Upd
 Minimum LSA arrival 1000 msecs
 Pacing lsa-group: 240 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 1. Checksum 0x006DB0
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 1
```

```
External LSA database is unlimited.
Number of LSA originated 2
Number of LSA received 173
Log Neighbor Adjency Changes : Enabled
 Number of areas attached to this router: 1: 1 normal 0 stub 0 nssa
   Area 2
      Number of interfaces in this area is 2(2)
      Number of fully adjacent neighbors in this area is 1
      Number of fully adjacent virtual neighbors through this area is 0
      Area has no authentication
      SPF algorithm last executed 00:06:27.540 ago
      SPF algorithm executed 9 times
      Number of LSA 6. Checksum 0x0212ff
```

Step 3: Display the routing table of Switch A

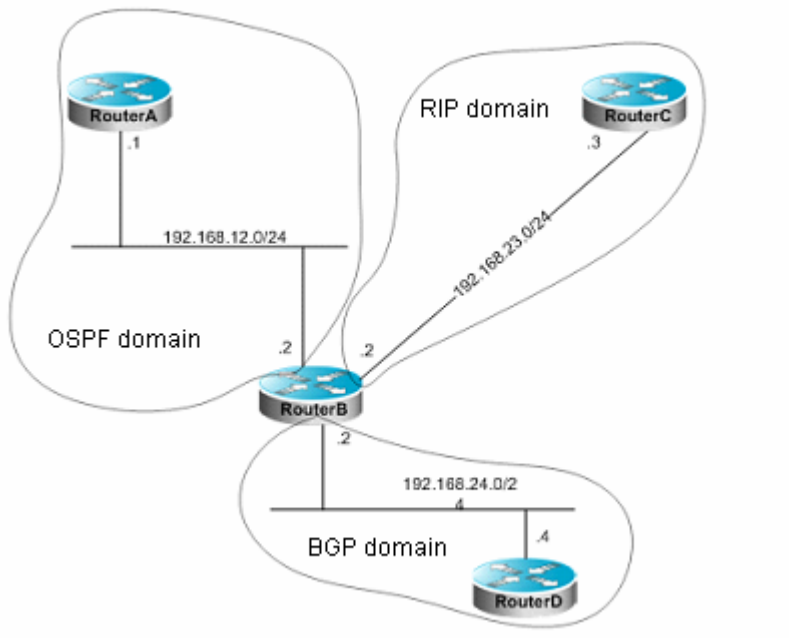
```
SwitchA#show ip route ospf
O E2 172.10.10.0/24 [110/20] via 192.168.1.2, 00:07:37, GigabitEthernet 0/1
O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 15:33:00, GigabitEthernet 0/1
O    192.168.5.0/24 [110/2] via 192.168.2.2, 15:14:59, GigabitEthernet 0/2
O IA 192.168.6.0/24 [110/3] via 192.168.1.2, 00:17:58, GigabitEthernet 0/1
```

From the above information, we can see that Switch A has successfully learned the route to the network segment of 172.10.10.0.

4.4.6 OSPF Dynamic Route Redistribution Configuration Example

Requirements

There are four devices which are connected as per following figure. Router A belongs to OSPF routing domain; router C belongs to RIP routing domain; router D belongs to BGP routing domain; router B is connected with three routing domains. Router A advertises the following two routes: 192.168.10.0/24 and 192.168.100.1/32; router C advertises the following two routes of 192.168.3.0/24 and 192.168.30.0/24; router D advertises the following two routes: 192.168.4.0/24 and 192.168.40.0/24.



Dynamic routing protocol redistribution

On Router B, OSPF will redistribute routes in the RIP routing domain (type-1) and BGP routes carrying the community attribute of 11:11 in BGP routing domain. RIP will redistribute a static route of 192.168.10.0/24 in OSPF routing domain, set the metric to 2 and advertise a default route to RIP domain.

Detailed configuration of routing devices

While redistributing routes between routing protocols, simple route filtering can be controlled by the distribute list, which, however, cannot configure different attributes for different routes; it will only be done by the route map. Route map provides greater control capability than the distribution list, but the configurations are comparatively complicated as well. Generally, the route map shall be avoided as best as possible, so that device configurations can be simplified. This example configures the route map to match the community attribute of BGP routes.

Configurations on Router A:

Configure network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.10.1 255.255.255.0
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ip address 192.168.100.1 255.255.255.0
DES-7200(config-if)# no ip directed-broadcast
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.12.55 255.255.255.0
```

Configure OSPF

```
DES-7200(config)# router ospf 12
```

```
DES-7200(config-router)# network 192.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.100.0 0.0.0.255 area 0
```

Configurations on Router B:

Configure network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.12.5 255.255.255.0
DES-7200(config)# interface Serial 1/0
DES-7200(config-if)# ip address 192.168.23.2 255.255.255.0
```

Configure OSPF and the type of routes to be redistributed

```
DES-7200(config)# router ospf 12
DES-7200(config-router)# redistribute rip metric 100 metric-type 1 subnets
DES-7200(config-router)# redistribute bgp route-map ospfrm subnets
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 0
```

Configure RIP and distribute list to filter the redistributed routes

```
DES-7200(config)# router rip
DES-7200(config-router)# redistribute ospf 12 metric 2
DES-7200(config-router)# network 192.168.23.0
DES-7200(config-router)# distribute-list 10 out ospf
DES-7200(config-router)# default-information originate always
DES-7200(config-router)# no auto-summary
```

Configure BGP

```
DES-7200(config)# router bgp 2
DES-7200(config-router)# neighbor 192.168.24.4 remote-as 4
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 192.168.24.4 activate
DES-7200(config-router-af)# neighbor 192.168.24.4  send-community
```

Configure route map

```
DES-7200(config)# route-map ospfrm
DES-7200(config-route-map)# match community cl_110
```

Define access list

```
DES-7200(config)# access-list 10 permit 192.168.10.0
```

Define community list

```
DES-7200(config)# ip community-list standard cl_110 permit 11:11
```

Configurations on Router C:

Configure network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.30.1 255.255.255.0
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7200(config)# interface Serial 1/0
DES-7200(config-if)# ip address 192.168.23.3 255.255.255.0
```

Configure RIP

```
DES-7200(config)# router rip
DES-7200(config-router)# network 192.168.23.0
DES-7200(config-router)# network 192.168.3.0
DES-7200(config-router)# network 192.168.30.0
```

Configurations on Router D:

Configure network interface

```
DES-7200(config)# interface gigabitEthernet 0/0
DES-7200(config-if)# ip address 192.168.40.1 255.255.255.0
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.4.1 255.255.255.0
DES-7200(config)# interface gigabitEthernet 1/0
DES-7200(config-if)# ip address 192.168.24.4 255.255.255.0
```

Configure BGP

```
DES-7200(config)# router bgp 4
DES-7200(config-router)# neighbor 192.168.24.2 remote-as 2
DES-7200(config-router)# redistribute connected route-map bgprm
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 192.168.24.2 activate
DES-7200(config-router-af)# neighbor 192.168.24.2  send-community
```

Configure route map

```
DES-7200(config)# route-map bgprm
DES-7200(config-route-map)# set community 22:22
```

OSPF routes learned by Router A:

```
O E1 192.168.30.0/24[110/101]via 192.168.12.5,00:04:07,FastEthernet0/1
O E1 192.168.3.0/24[110/101]via 192.168.12.5,00:04:07,FastEthernet0/1
```

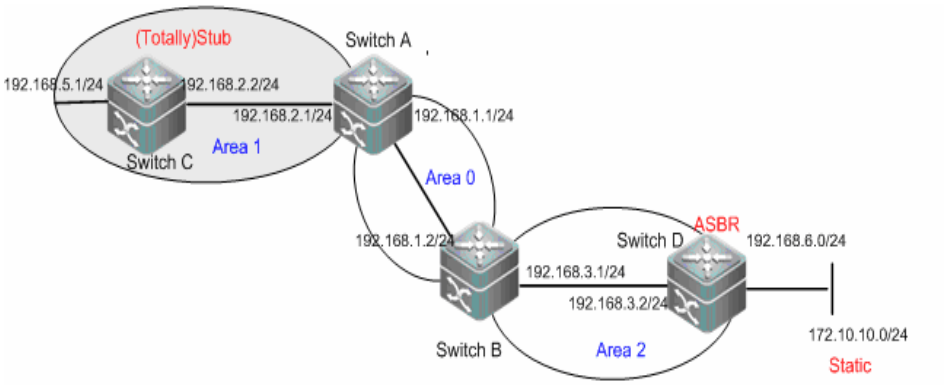
RIP routes learned by Router C:

```
R    0.0.0.0/0 [120/1] via 200.168.23.2, 00:00:00, Serial1/0
R    192.168.10.0/24 [120/2] via 200.168.23.2, 00:00:00, Serial1/0
```

4.4.7 OSPF (Totally) Stub Area Configuration Example

Topological diagram

The following figure shows the networking diagram for OSPF autonomous system. The entire autonomous system is divided into three areas: area 0, area 1 and area 2. Segment 172.10.10.0 is outside the routing domain.



Networking diagram for OSPF (Totally) Stub area configuration

Application needs

- Configure Switch A and Switch B as area border routers (ABR) and Switch C as intra-area device. Configure Switch D as ASBR and introduce one external static route.
- To reduce the size of routing table inside AS border and the number of routes exchanged, configure the specific area to a (Totally) Stub area.
- Routing information can be correctly propagated in OSPF autonomous system.

Configuration tips

- The backbone area (Area 0) cannot be configured as (Totally) Stub area, and there must be no ASBR in the (Totally) Stub area, namely the external routes of autonomous system cannot be propagated in this area. In this example, Area 1 can be configured as a (Totally) Stub area.
- To configure an area into Stub area, you must configure "**stub**" command on all devices in this area. This example needs to configure this attribute on Switch A and Switch C.
- To configure an area into Totally Stub area, you must configure "**stub**" command on all devices in this area (Switch C) and "**stub [no-summary]**" command on the ABR device (Switch A).

Configuration Steps

The following information only shows the steps to configure OSPF (Totally) Stub area. For other configurations, please refer to the examples shown in "Multi-area OSPF Configuration" and "OSPF Static Route Redistribution".

Step 1: Display the routing table of Switch C when its native area is a normal area.

```
SwitchC#show ip route  ospf
O E2 172.10.10.0/24 [110/20] via 192.168.2.1, 4d,02:28:07, GigabitEthernet
0/3                          //AS external route
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 4d,17:52:14, GigabitEthernet 0/3
O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 4d,17:52:14, GigabitEthernet 0/3
O IA 192.168.6.0/24 [110/4] via 192.168.2.1, 4d,02:38:27, GigabitEthernet 0/3
```

From the above information, we can see that the routing table contains AS external route when the native area of Switch C is a normal area.

Step 2: Configure Stub area

Configurations on Switch A

```
SwitchA(config)#router ospf 1
SwitchA(config-router)#area 1 stub
```

Configurations on Switch C

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#area 1 stub
```

Display the routing table of Switch C when its native area is a stub area.

```
SwitchC#show ip route ospf
O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:00:32, GigabitEthernet 0/3
//default route
O IA 192.168.1.0/24 [110/2] via 192.168.2.1, 00:00:32, GigabitEthernet 0/3
O IA 192.168.3.0/24 [110/3] via 192.168.2.1, 00:00:32, GigabitEthernet 0/3
O IA 192.168.6.0/24 [110/4] via 192.168.2.1, 00:00:32, GigabitEthernet 0/3
```

From the above information, we can see that the AS external route is gone when the native area of Switch C is a stub area. The AS external route in the original routing table has been replaced by a default route.

Step 3: Configure Totally Stub area

Configurations on Switch A

```
SwitchA(config)#router ospf 1
SwitchA(config-router)#area 1 stub stub no-summary
```

Configurations on Switch C

```
SwitchC(config)#router ospf 1
```

```
SwitchC(config-router)#area 1 stub
```

Display the routing table of Switch C when its native area is a totally stub area.

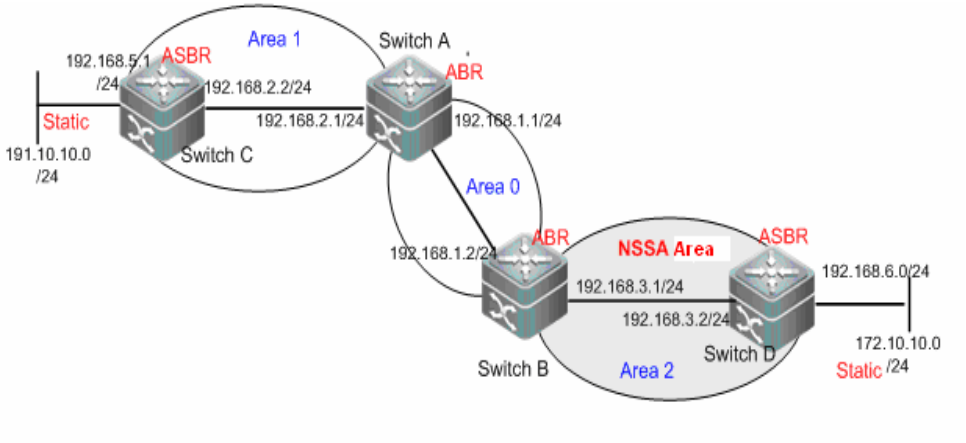
```
SwitchC#show ip route ospf
O*IA 0.0.0.0/0 [110/2] via 192.168.2.1, 00:30:53, GigabitEthernet 0/3
```

From the above information, we can see that the routing table entries are further reduced to only one default route to the external area when the native area of Switch C is a totally stub area.

4.4.8 OSPF NSSA Area Configuration Example

Topological diagram

The following figure shows the networking diagram for OSPF autonomous system. The entire autonomous system is divided into three areas: area 0, area 1 and area 2. Segment 192.10.10.0 and segment 172.10.10.0 are outside the OSPF routing domain.



Networking diagram for OSPF NSSA area configuration

Application needs

Configure Switch A and Switch B as area border routers (ABR) and Switch C as intra-area device. Configure Switch C and Switch D as ASBR and introduce one AS external static route respectively.

Area 2 shall be configured as a NSSA area in order to reduce the size of routing table of intra-area devices and the number of routes exchanged. Meanwhile, prohibit Switch B from sending summary LSAs (Type-3 LSA) to NSSA area.

Routing information can be correctly propagated in OSPF autonomous system.

Configuration tips

Steps to configure NSSA area are shown below:

The backbone area (Area 0) cannot be configured as a NSSA area;

ASBR can exist in NSSA area, and certain number of AS external routes can be imported to OSPF routing domain.

1、 To configure this area into NSSA area, you must configure "**area nssa**" command on all devices (Switch B/D) connected to NSSA area.

Configuration Steps

The following information only shows the steps to configure NSSA area. For OSPF basic configurations, please refer to the examples shown above.

Step 1: Configure static route redistribution

Configurations on Switch C

! Configure static route

```
SwitchC(config)#ip route 191.10.10.0 255.255.255.0 192.168.5.2
```

! OSPF static route redistribution

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#redistribute static subnets
```

Configurations on Switch D

! Configure static route

```
SwitchD(config)#ip route 172.10.10.0 255.255.255.0 192.168.6.2
```

! OSPF static route redistribution

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#redistribute static subnets
```

Step 2: Configure NSSA

Configurations on Switch B (ABR)

```
SwitchB(config)#router ospf 1
```

! Define NSSA area and prohibit ABR device from sending summary LSAs (Type-3 LSA) to NSSA area.

```
SwitchB(config-router)#area 2 nssa no-summary
```

Configurations on Switch D (ASBR)

```
SwitchD(config)#router ospf 1
SwitchD(config-router)#area 2 nssa
```

Verify configurations

Step 1: Display the routing information when Area 2 is a normal area.

Display the routing table of Switch D (ASBR)

```
SwitchD#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    172.10.10.0/24 [1/0] via 192.168.6.2
O E2 191.10.10.0/24 [110/20] via 192.168.3.1, 00:00:21, GigabitEthernet 0/3
O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:00:21, GigabitEthernet 0/3
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:00:21, GigabitEthernet 0/3
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/3
C    192.168.3.2/32 is local host.
O IA 192.168.5.0/24 [110/4] via 192.168.3.1, 00:00:21, GigabitEthernet 0/3
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/4
C    192.168.6.1/32 is local host.
```

Display OSPF routing table of Switch B (ABR)

```
SwitchB#show ip route ospf
O E2 172.10.10.0/24 [110/20] via 192.168.3.2, 17:53:35, GigabitEthernet 0/2
Type7 LSA on ASBR
O E2 191.10.10.0/24 [110/20] via 192.168.1.1, 00:57:46, GigabitEthernet 0/1
O IA 192.168.2.0/24 [110/2] via 192.168.1.1, 5d,15:39:01, GigabitEthernet 0/1
O IA 192.168.5.0/24 [110/3] via 192.168.1.1, 01:10:34, GigabitEthernet 0/1
O    192.168.6.0/24 [110/2] via 192.168.3.2, 17:53:36, GigabitEthernet 0/2
```

Step 2: Display the routing tables of respective devices in NSSA area when Area 2 is configured as NSSA area.

Display OSPF routing table of Switch B (ABR)

```
SwitchB#show ip route ospf
O N2 172.10.10.0/24 [110/20] via 192.168.3.2, 00:01:00, GigabitEthernet 0/2
O E2 191.10.10.0/24 [110/20] via 192.168.1.1, 01:11:26, GigabitEthernet 0/1
O IA 192.168.2.0/24 [110/2] via 192.168.1.1, 5d,15:52:41, GigabitEthernet 0/1
O IA 192.168.5.0/24 [110/3] via 192.168.1.1, 01:24:14, GigabitEthernet 0/1
O    192.168.6.0/24 [110/2] via 192.168.3.2, 00:01:01, GigabitEthernet 0/2
```

From the above information, we can see that the ABR in NSSA area has translated the external routes imported by this area into N2 (OSPF NSSA external type 2) routes for distributing into other areas.

Display the routing table of Switch D (ASBR)

```
SwitchD#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
S    172.10.10.0/24 [1/0] via 192.168.6.2
O IA 192.168.1.0/24 [110/2] via 192.168.3.1, 00:03:20, GigabitEthernet 0/3
O IA 192.168.2.0/24 [110/3] via 192.168.3.1, 00:03:20, GigabitEthernet 0/3
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/3
C    192.168.3.2/32 is local host.
O IA 192.168.5.0/24 [110/4] via 192.168.3.1, 00:03:20, GigabitEthernet 0/3
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/4
C    192.168.6.1/32 is local host.
```

From the above information, we can see that the AS external routes imported by other areas cannot reach this area when the native area of Switch D is a NSSA area.

Step 3: Display the routing information of NSSA area while configuring the "no-summary" attribute of NSSA area on Switch B (ABR).

```
SwitchD#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is 192.168.3.1 to network 0.0.0.0
O*IA 0.0.0.0/0 [110/2] via 192.168.3.1, 00:00:40, GigabitEthernet 0/3
S    172.10.10.0/24 [1/0] via 192.168.6.2
C    192.168.3.0/24 is directly connected, GigabitEthernet 0/3
C    192.168.3.2/32 is local host.
C    192.168.6.0/24 is directly connected, GigabitEthernet 0/4
C    192.168.6.1/32 is local host.
```

From the above information, we can see that after configuring "no-summary" attribute on the ABR of NSSA area, the routing table entries are further reduced, and the inter-area routes are replaced by one default route.

Step 4: Display OSPF routing information on devices in other areas. Key point: whether there is any AS external route imported by NSSA area.

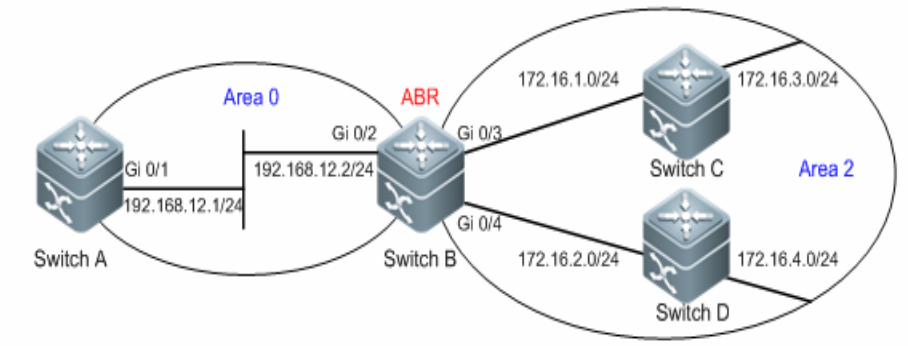
```
SwitchA#show ip route ospf
O E2 172.10.10.0/24 [110/20] via 192.168.1.2, 02:08:08, GigabitEthernet 0/1
O E2 191.10.10.0/24 [110/20] via 192.168.2.2, 03:18:35, GigabitEthernet 0/2
O IA 192.168.3.0/24 [110/2] via 192.168.1.2, 5d,17:59:01, GigabitEthernet 0/1
O    192.168.5.0/24 [110/2] via 192.168.2.2, 03:31:25, GigabitEthernet 0/2
O IA 192.168.6.0/24 [110/3] via 192.168.1.2, 02:08:09, GigabitEthernet 0/1
```

From the above information, we can see that an AS external route imported by NSSA area is contained in the routing table of Switch A.

4.4.9 OSPF Inter-area Route Summarization Configuration Example

Topological diagram

The following figure shows the topological diagram for OSPF autonomous system, in which segment 192.168.12.0/24 belongs to Area 0 and segments 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24 and 172.16.4.0/24 belong to Area 2.



OSPF inter-area route summarization configuration example

Application needs

To reduce the size of routing table, configure Switch B so that it will only advertise the summary route of four network segments (172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24 and 172.16.4.0/24) instead of advertising the routes of these four segments.

Configuration tips

1. Since segments 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24 and 172.16.4.0/24 are consecutive address ranges, we can configure route summarization on the area border device (Switch B) to alleviate route computation. The command for configuring OSPF inter-area route summarization is "area range".

2. During route summarization, the summarized range may exceed the actual network range in the routing table. Routing loop may incur or the burden of router may be increased if packets are sent to a nonexistent network. To avoid this, we need to add a "discard" route to the routing table of ABR (Switch B) or ASBR, so as to add the "discard" routes generated by the inter-area route summarization command of "area range". This feature is enabled by default.

3. The summary address of 172.16.1.0/24, 172.16.2.0/24, 172.16.3.0/24 and 172.16.4.0/24 is 172.16.0.0/21. Routes falling within this range won't be advertised to other areas by ABR.

Configuration Steps

Step 1: Configure the IP address of respective interfaces (omitted)

Step 2: Configure OSPF basic features

Configure Switch A

```
SwitchA(config)#router ospf 1
SwitchA(config)# network 192.168.12.0 0.0.0.255 area 0
```

Configure Switch B

```
SwitchB(config)#router ospf 1
SwitchB(config-router)#network 192.168.12.0 0.0.0.255 area 0
SwitchB(config-router)#network 172.16.1.0 0.0.0.255 area 2
SwitchB(config-router)#network 172.16.2.0 0.0.0.255 area 2
```

Configure Switch C

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#network 172.16.1.0 0.0.0.255 area 2
SwitchC(config-router)#network 172.16.3.0 0.0.0.255 area 2
```

Configure Switch D

```
SwitchD(config)#router ospf 1
SwitchD(config-router)#network 172.16.2.0 0.0.0.255 area 2
SwitchD(config-router)#network 172.16.4.0 0.0.0.255 area 2
```

Display OSPF routing table of Switch A

```
SwitchA#show ip route ospf
O IA 172.16.1.0/24 [110/2] via 192.168.12.2, 00:06:47, GigabitEthernet 0/1
O IA 172.16.2.0/24 [110/2] via 192.168.12.2, 00:06:47, GigabitEthernet 0/1
O IA 172.16.3.0/24 [110/3] via 192.168.12.2, 00:06:47, GigabitEthernet 0/1
O IA 172.16.4.0/24 [110/3] via 192.168.12.2, 00:06:19, GigabitEthernet 0/1
```

From the above information, we can see that the detailed routes of area 2 are advertised to area 0.

Step 3: Configure inter-area route summarization on ABR (Switch B)

```
SwitchB(config)#router ospf 1
SwitchB(config-router)#area 2 range 172.16.0.0 255.255.248.0
```

Step 4: On ABR (Switch B), add the summary route entry into the core routing table. This feature is enabled by default.

```
SwitchB(config-router)# discard-route internal
```

Verify configurations

After configuring route summarization, display OSPF routing table of Switch A

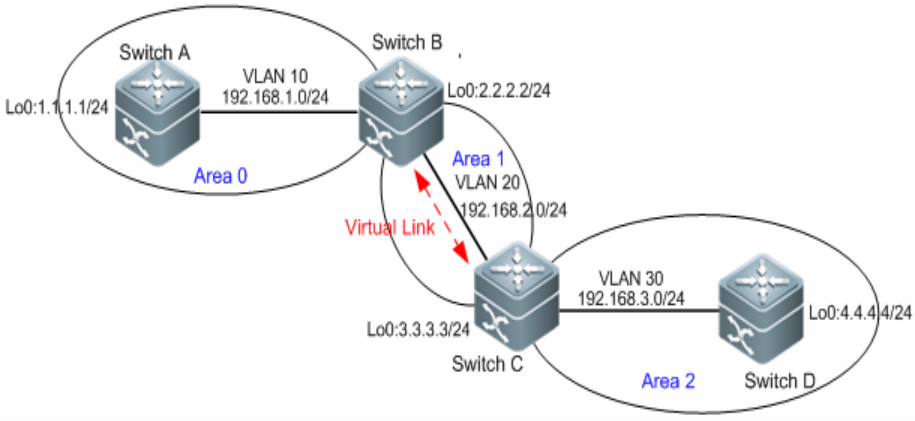
```
SwitchA#show ip route ospf
O IA 172.16.0.0/21 [110/2] via 192.168.12.2, 00:01:04, GigabitEthernet 0/1
```

From the above information, we can see that only the summary route is advertised. Specific routes won't be advertised by the ABR to other areas. The size of routing table is decreased substantially.

4.4.10 OSPF Virtual Link Configuration Example

Topological diagram

The following figure shows an OSPF routing domain. Segment 192.168.1.0 belongs to area 0; segment 192.168.2.0 belongs to area 1; segment 192.168.3.0 belongs to area 2. Due to the limitations in physical conditions, we cannot physically deploy other specific areas nearby the backbone area. As shown below, area 2 is not directly connected with area 0.



Networking diagram for OSPF virtual link configuration

Application needs

Through configuration, Switch D shall be able to receive routes of 192.168.1.0/24 (area 0) and 192.168.2.0/24 (area 1). Meanwhile, Switch B shall also be able to learn the routes of segment 192.168.3.0/24 (area 2).

IP address assignment details are shown below:

Device name	Device ID	Interface address
Switch A	1.1.1.1	VLAN 10（Gi0/1）: 192.168.1.1/24
Switch B	2.2.2.2	VLAN 10（Gi0/1）: 192.168.1.2/24 VLAN 20（Gi0/3）: 192.168.2.1/24
Switch C	3.3.3.3	VLAN 20（Gi0/3）: 192.168.2.2/24 VLAN 30（Gi0/5）: 192.168.3.1/24
Switch D	4.4.4.4	VLAN 30（Gi0/5）: 192.168.3.2/24

Configuration tips

When OSPF routing domain is composed of multiple areas, each area must be directly connected with the backbone area (area 0), or else areas cannot be interconnected. If there is no direct physical link, we can create virtual link to logically connect the area to the backbone area. Configuration tips are shown below:

Configure the IP address of respective interfaces (omitted)

Enable OSPF basic features

Configure OSPF virtual link

- The virtual link must be configured on ABR. This example configures virtual link on Switch B and Switch C.
- Execute "**area** *area-id* **virtual-link** *router-id*" command to configure virtual link on ABR. Router-id refers to the identifier of peer device.

Configuration Steps

Step 1: Configure OSPF basic features

Configure Switch A

! Create OSPF process and specify the IP address range associated with this routing process and the OPPF area to which these IP addresses belong.

```
SwitchA(config)#router ospf 1
SwitchA(config-router)#network 192.168.1.0 0.0.0.255 area 0
SwitchA(config-router)#exit
```

! Configure loopback IP of 1.1.1.1 as the device ID of Switch A

```
SwitchA(config)#interface loopback 0
```

```
SwitchA(config-Loopback 0)#ip address 1.1.1.1 255.255.255.0
```

Configure Switch B

! Create OSPF process and specify the IP address range associated with this routing process and the OPPF area to which these IP addresses belong.

```
SwitchB(config)#router ospf 1
SwitchB(config-router)#network 192.168.1.0 0.0.0.255 area 0
SwitchB(config-router)#network 192.168.2.0 0.0.0.255 area 1
SwitchB(config-router)#exit
```

! Configure loopback IP of 2.2.2.2 as the device ID of Switch B

```
SwitchB(config)#interface loopback 0
SwitchB (config-Loopback 0)#ip address 2.2.2.2 255.255.255.0
```

Configure Switch C

! Create OSPF process and specify the IP address range associated with this routing process and the OPPF area to which these IP addresses belong.

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#network 192.168.2.0 0.0.0.255 area 1
SwitchC(config-router)#network 192.168.3.0 0.0.0.255 area 2
SwitchC(config-router)#exit
```

! Configure loopback IP of 3.3.3.3 as the device ID of Switch C

```
SwitchC(config)#interface loopback 0
SwitchC(config-Loopback 0)#ip address 3.3.3.3 255.255.255.0
```

Configure Switch D

! Create OSPF process and specify the IP address range associated with this routing process and the OPPF area to which these IP addresses belong.

```
SwitchD(config)#router ospf 1
SwitchD(config-router)#network 192.168.3.0 0.0.0.255 area 2
SwitchD(config-router)#exit
```

! Configure loopback IP of 4.4.4.4 as the device ID of Switch D

```
SwitchD(config)#interface loopback 0
SwitchD(config-Loopback 0)#ip address 4.4.4.4 255.255.255.0
```

Display OSPF routing table of Switch A

```
SwitchA#show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:32:48, VLAN 10
```

Since Area 2 is not directly connected with Area 0, there is no routing information about Area 2 in the routing table of Switch A.

Step 2: Configure OSPF virtual link

Configure Switch B

```
SwitchB(config)#router ospf 1
SwitchB(config-router)#area 1 virtual-link 3.3.3.3
```

Configure Switch C

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#area 1 virtual-link 2.2.2.2
```

Verify configurations

Display OSPF routing table of Switch B

```
SwitchB#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
Gateway of last resort is no set
C    2.2.2.0/24 is directly connected, Loopback 0
C    2.2.2.2/32 is local host.
C    192.168.1.0/24 is directly connected, VLAN 10
C    192.168.1.2/32 is local host.
C    192.168.2.0/24 is directly connected, VLAN 20
C    192.168.2.1/32 is local host.
O IA 192.168.3.0/24 [110/2] via 192.168.2.2, 00:02:49, VLAN 20
```

From the above information, we can see that after configuring the virtual link, Switch B has successfully learned the route from segment 192.168.3.0/24 (area 2).

Display OSPF routing table of Switch D

```
SwitchD#show ip route

Codes:  C - connected, S - static, R - RIP, B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
```

```
C    4.4.4.0/24 is directly connected, Loopback 0
C    4.4.4.4/32 is local host.
O IA 192.168.1.0/24 [110/3] via 192.168.3.1, 00:04:45, VLAN 30
O IA 192.168.2.0/24 [110/2] via 192.168.3.1, 00:05:02, VLAN 30
C    192.168.3.0/24 is directly connected, VLAN 30
C    192.168.3.2/32 is local host.
```

From the above information, we can see that after configuring the virtual link, Switch D has successfully learned the routes from segments 192.168.1.0/24 (area 0) and 192.168.2.0/24 (area 1).

Display OSPF routing table of Switch A

```
SwitchA#show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:51:22, VLAN 10
O IA 192.168.3.0/24 [110/3] via 192.168.1.2, 00:07:58, VLAN 10
```

From the above information, we can see that after configuring the virtual link, Switch A has successfully learned the route from segment 192.168.3.0/24 (area 2).

Display OSPF virtual link information of Switch B

```
SwitchB#show ip ospf 1 virtual-links
Virtual Link VLINK0 to router 3.3.3.3 is up
  Transit area 0.0.0.1 via interface GigabitEthernet 0/3
  Local address 192.168.2.1/32
  Remote address 192.168.2.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Adjacency state Full
```

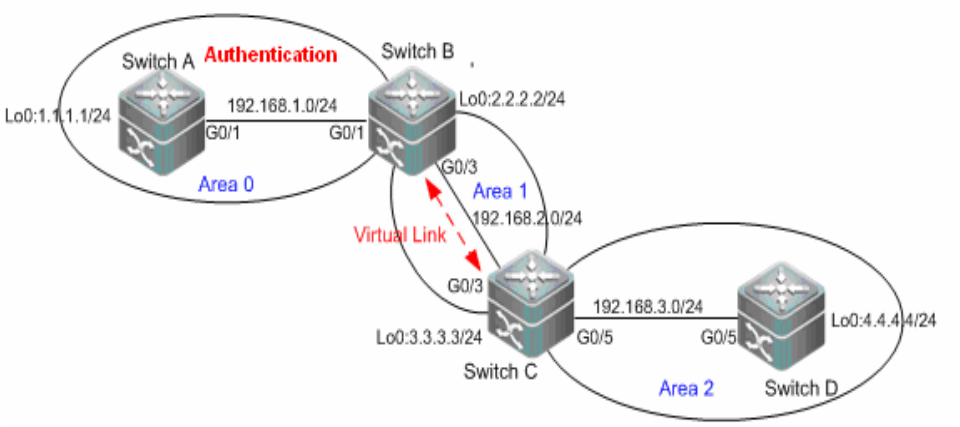
Display OSPF virtual link information of Switch C

```
SwitchC#show ip ospf 1 virtual-links
Virtual Link VLINK0 to router 2.2.2.2 is up
  Transit area 0.0.0.1 via interface GigabitEthernet 0/3
  Local address 192.168.2.2/32
  Remote address 192.168.2.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
    Adjacency state Full
```

4.4.11 OSPF Authentication Configuration Example

Topological diagram

The following figure shows an OSPF routing domain. Segment 192.168.1.0 belongs to area 0; segment 192.168.2.0 belongs to area 1; segment 192.168.3.0 belongs to area 2. Due to the limitations in network structure, area 2 is connected to area 0 through virtual link.



Networking diagram for OSPF authentication configuration

Application needs

1. To prevent the device from learning unauthenticated and invalid routes and advertising valid routes to unauthenticated devices, it is required to configure area authentication in the backbone area (area 0), with authentication type being MD5.

2. Switch D shall be able to learn routes from 192.168.1.0/24 (area 0) and 192.168.2.0/24 (area 1). Meanwhile, Switch B shall also be able to learn the routes from segment 192.168.3.0/24 (area 2).

Configuration tips

To configure OSPF area authentication, we must configure area authentication on all devices in the same area using the same authentication type. This example requires enabling area authentication in Area 0, namely all devices (Switch A and Switch B) in Area 0 shall be configured with the same authentication type.

While using OSPF virtual link to connect non-backbone area (Area 2) with backbone area, if ID authentication is enabled in the backbone area (Area 0), then backbone area ID authentication shall also be configured on the ABR of non-backbone area (Switch C).

Major steps of OSPF area authentication are shown below:

In OSPF router configuration mode, specify the authentication type for the area.

Configure authentication type and authentication key on the interface.

Configuration Steps

The following information only shows the steps to configure OSPF area authentication. For other configurations, please refer to the examples shown in "OSPF Virtual Link".

Configure Switch A

Step 1: In OSPF router configuration mode, specify Area 0 to enable MD5 authentication

```
SwitchA(config)#router ospf 1
SwitchA(config-router)#area 0 authentication message-digest
SwitchA(config-router)#exit
```

Step 2: Configure authentication type and authentication key on the interface.

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#ip ospf message-digest-key 1 md5
hello
```

Configure Switch B

Step 1: In OSPF router configuration mode, specify Area 0 to enable MD5 authentication

```
SwitchB(config)#router ospf 1
SwitchB(config-router)#area 0 authentication message-digest
SwitchB(config-router)#exit
```

Step 2: Configure authentication type and authentication key on the interface.

```
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#ip ospf message-digest-key 1 md5
hello
```

Configure Switch C

! Enable backbone area (Area 0) authentication on Switch C

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#area 0 authentication message-digest
```

Verify configurations

Step 1: Display the OSPF information of respective devices when authentication is only enabled on Switch A and Switch B (not enabled on Switch C).

! Display the virtual link configurations of Switch B

```
SwitchB#show ip ospf virtual-links
Virtual Link VLINK0 to router 3.3.3.3 is up
  Transit area 0.0.0.1 via interface GigabitEthernet 0/3
  Local address 192.168.2.1/32
  Remote address 192.168.2.2/32
```

```
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
Adjacency state Down
```

From the above information, we can see that the adjacency state is down.

! Display the virtual link configurations of Switch C

```
SwitchC#show ip ospf virtual-links
Virtual Link VLINK0 to router 2.2.2.2 is up
  Transit area 0.0.0.1 via interface GigabitEthernet 0/3
  Local address 192.168.2.2/32
  Remote address 192.168.2.1/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
Adjacency state Down
```

From the above information, we can see that the adjacency state is down.

! Display OSPF routing information of Switch A

```
SwitchA#show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:10:59, GigabitEthernet 0/1
```

From the above information, we can see that Switch A has failed to learn the route from area 2.

Step 1: Display the OSPF information of respective devices after authentication is enabled on Switch A and Switch B and area 0 authentication is configured on Switch C.

! Display the virtual link configurations of Switch B

```
SwitchB#show ip ospf virtual-links
Virtual Link VLINK0 to router 3.3.3.3 is up
  Transit area 0.0.0.1 via interface GigabitEthernet 0/3
  Local address 192.168.2.1/32
  Remote address 192.168.2.2/32
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:01
Adjacency state Full
```

From the above information, we can see that the adjacency state is full.

! Display the virtual link configurations of Switch C

```
   SwitchC#show ip ospf virtual-links
Virtual Link VLINK0 to router 2.2.2.2 is up
```

```
Transit area 0.0.0.1 via interface GigabitEthernet 0/3
Local address 192.168.2.2/32
Remote address 192.168.2.1/32
Transmit Delay is 1 sec, State Point-To-Point,
    Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:00
    Adjacency state Full
```

From the above information, we can see that the adjacency state is full.

! Display OSPF routing information of Switch A

```
SwitchA#show ip route ospf
O IA 192.168.2.0/24 [110/2] via 192.168.1.2, 00:21:30, GigabitEthernet 0/1
O IA 192.168.3.0/24 [110/3] via 192.168.1.2, 00:03:18, GigabitEthernet 0/1
```

From the above information, we can see that Switch A has successfully learned the route from area 2.

Step 3: Display general OSPF information of Switch A.

```
SwitchA#show ip ospf
 Routing Process "ospf 1" with ID 1.1.1.1
 Process uptime is 18 hours 22 minutes
 Process bound to VRF default
 Conforms to RFC2328, and RFC1583Compatibility flag is enabled
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 Enable two-way-maintain
 Initial SPF schedule delay 1000 msecs
 Minimum hold time between two consecutive SPFs 5000 msecs
 Maximum wait time between two consecutive SPFs 10000 msecs
 Initial LSA throttle delay 0 msecs
 Minimum hold time for LSA throttle 5000 msecs
 Maximum wait time for LSA throttle 5000 msecs
 Lsa Transmit Pacing timer 40 msecs, 10 LS-Upd
 Minimum LSA arrival 1000 msecs
 Pacing lsa-group: 240 secs
 Number of incomming current DD exchange neighbors 0/5
 Number of outgoing current DD exchange neighbors 0/5
 Number of external LSA 0. Checksum 0x000000
 Number of opaque AS LSA 0. Checksum 0x000000
 Number of non-default external LSA 0
 External LSA database is unlimited.
 Number of LSA originated 2
 Number of LSA received 244
 Log Neighbor Adjency Changes : Enabled
```

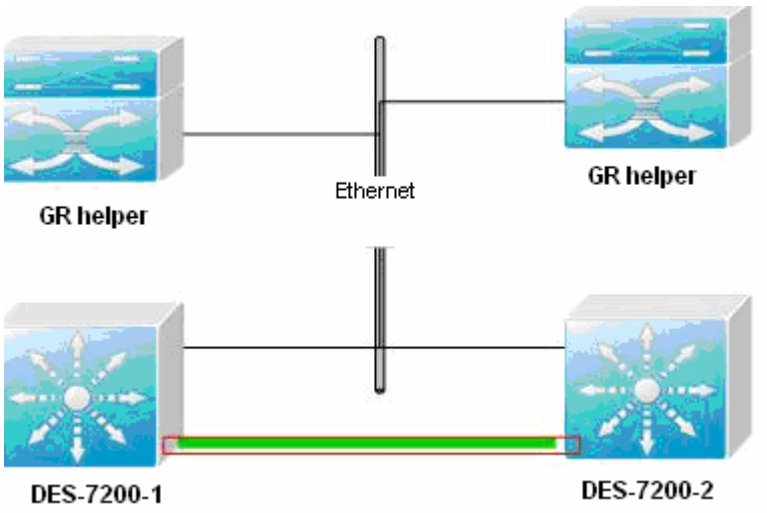
```
Number of areas attached to this router: 1: 1 normal 0 stub 0 nssa
 Area 0 (BACKBONE)
    Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 1
    Area has message digest authentication
    SPF algorithm last executed 17:24:38.030 ago
    SPF algorithm executed 11 times
    Number of LSA 7. Checksum 0x032955
```

The above information shows that area authentication has been enabled.

4.4.12 OSPF GR Configuration Example

Requirements

As shown below, two DES-7200 high-end switches have GR Restart capability, and both devices are equipped with primary and secondary engines to allow redundant backup at the control plane. DES-7200-1 builds OSPF adjacencies with DES-7200-2and other GR helpers, and OSPF GR capability is supported by all devices. The connection layout is shown below:



OSPF GR configuration example

It is required that two DES-7200 devices shall allow non-stop packet forwarding in order to enhance the high reliability of core devices.

Specific configurations

Configure DES-7200-1:

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# graceful-restart
DES-7200(config-router)# graceful-restart helper strict-lsa-checking
```

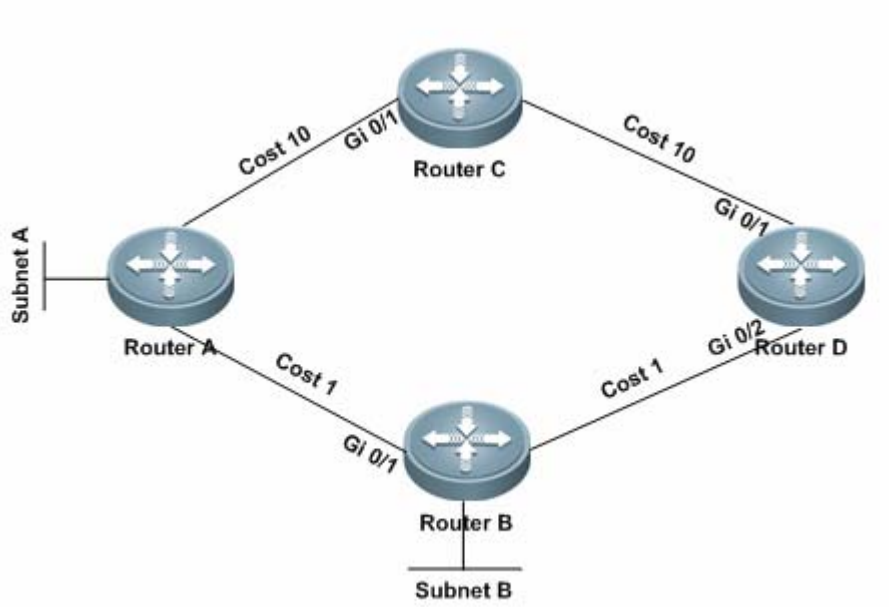
Configure DES-7200-2:

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# graceful-restart
DES-7200(config-router)# graceful-restart helper strict-lsa-checking
```

4.4.13 OSPF Stub Router Configuration Example

Requirements

For four devices form a OSPF routing domain. The connection layout is shown below. According to the rule for best route selection, the path from Router D to subnet A must pass Router B. It is expected the route can pass Router C instead by configuring Router B only.



OSPF Stub Router configuration example

It is required that Router B only advertise the route to Subnet B, and other routes shall be advertised by Router C.

Detailed configurations

Configure IP addresses and OSPF processes on four devices, and execute the following configurations after adjacencies have been established successfully.

Configurations on Switch D:

Configure Ethernet interface

```
interface gigabitEthernet 0/1
ip ospf cost 10
interface gigabitEthernet 0/2
ip ospf cost 1
```

Configurations on device C:

Configure Ethernet interface

```
interface gigabitEthernet 0/1
ip ospf cost 10
```

Configurations on device B:

Configure Ethernet interface

```
interface gigabitEthernet 0/1
ip ospf cost 1
```

Configure OSPF routing protocol

```
router ospf 1
max-metric router-lsa
```

4.4.14 OSPF Fast Convergence Configuration Example

Requirements

Router A and Router B are interconnected throuhg layer-2 switch, and OSPF protocol is running on devices to establish routes. IP address assignment and connection layout are shown in the following figure.

OSPF fast convergence configuration example

After the link between Router B and layer-2 switch fails, Router A shall be able to detect adjacency change within 1 second and quickly respond to the change in network information.

Detailed configurations

Enabling "Fast Hello" will reduce adjacency change detection time to less than 1 second. Meanwhile, LSA fast convergence shall also be enabled to adapt to the swift change in network.

Configure Router A:

Configure Ethernet interface

```
interface gigabitEthernet 0/1
ip address 192.168.1.1 255.255.255.0
interface gigabitEthernet 0/2
ip address 192.168.2.1 255.255.255.0
ip ospf dead-interval minimal hello-multiplier 5
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
network 192.168.2.0 0.0.0.255 area 0
timers arrival-time 100
timers throttle lsa all 0 100 500
```

Configure Router B:

Configure Ethernet interface

```
interface gigabitEthernet 0/1
ip address 192.168.3.1 255.255.255.0
interface gigabitEthernet 0/2
ip address 192.168.2.2 255.255.255.0
ip ospf dead-interval minimal hello-multiplier 5
```

Configure OSPF routing protocol

```
router ospf 1
network 192.168.2.0 0.0.0.255 area 0
network 192.168.3.0 0.0.0.255 area 0
timers arrival-time 100
timers throttle lsa all 0 100 500
```

5 OSPFv3 Configuration

OSPFV2 (RFC2328) runs under the IPv4. The RFC5340 describes OSPFV3, the extension of OSPFv2 that provides support for IPv6 routes. This document briefly describes the OSPFv3 protocol and its configuration.

Caution

Before learning this document, you must know the OSPFv2 protocol and related configuration.

The OSPFv3 protocol extends the OSPFv2 protocol with the same operation mechanisms and most configurations as the OSPFv2.

5.1 Overview

As an Interior Gateway Protocol (IGP), the OSPF runs among the layer 3 devices in a same Autonomous System (AS).

Unlike a vector distance protocol, the OSPF is a link-state protocol. By exchanging various types of link-state advertisements (LSAs) recording link state between devices, it synchronizes link state information between devices and then calculates OSPF route entries through the Dijkstra algorithm.

The OSPFv3 is described in the RFC5340 and supports the IPv6. This section describes the different implementation than OSPFv2.

- LSA Association Change
- Interface Configuration
- Router ID Configuration
- Authentication Mechanism Configuration

5.1.1 LSA Association Change

Just as described above, the OSPF is a link-state protocol and its implementation is based on LSAs. Through LSAs, we can know the topologies of networks and address information. In contrast to the IPv4, the IPv6 uses a 128-bit IP address. The design of LSAs is modified accordingly. The types of LSAs are described as follows:

- Router-LSAs (Type 1)

Each device generates this type of LSAs by itself. They describe the states of its links in specified areas and the cost spent on reaching the links.In contrast to the OSPFv2, the Router-LSAs of the OSPFv3 only indicate the state information of links. They do not record the information about the network addresses connected to routers. The information will be acquired by newly added types of LSAs. Additionaly, in the OSPFv2, only one Router-LSA is allowed to be generated for each device in each area. While in the OSPFv3, multiple Router-LSAs are allowed to be generated. Thus, when performing the SPF calculation, we must consider all the Router-LSAs generated by the device. Router-LSAs and Network-LSAs describe the link topology of areas together.

Caution

Through the flag bits on Router-LSAs, we can know whether the routers are Area Border Routers (ABR), AS boundary routers (ASBR) or those at one end of a virtual link.

- Network-LSAs (Type 2)

Network-LSAs only exist in broadcast networks or NBMA networks and are generated by DRs (Designated Routers) in a network. They describe the information about all the routers connected in specified areas on a network. Like Router-LSAs, Network-LSAs also only indicate link-state information and do not record network address information. Network-LSAs and Router-LSAs describe the link topology of areas together.

- Inter-Area-Prefix-LSAs (Type 3)

Generated for an area by the ABRs in the area and used to describe the network information about reaching other areas. They replace type 3 summary-LSAs in OSPFv2. In contrast to the OSPFv2, they use a prefix structure to describe destination network information.

- Inter-Area-Router-LSAs (Type 4)

Generated for an area by the ABRs in the area, used to describe the path information about reaching the ASBRs in other areas, and replacing type 4 summary-LSAs in the OSPFv2.

- AS-external-LSAs (Type 5)

This type of LSAs are generated by ASBRs and used to describe the network information about reaching outside AS. Usually, the network information is generated through other route protocols. In contrast to the OSPFv2, it uses a prefix structure to describe destination network information.

- NSSA-LSA (Type 7)

Their function is same to that of type 5 AS-external-LSAs. However, they are generated by ASBRs in the NSSA area.

- Link-LSAs (Type 8)

In the OSPFv3, the newly added LSA type is generated by each device for each connected link and describes the local link address of the device in the current link and all set IPv6 address prefix information.

- Intra-Area-Prefix-LSAs (Type 9)

In the OSPFv3, the newly added LSA type provides additional address information for Router-LSAs or Network-LSAs. Therefore, it has two effects:

1） Associate network-LSAs and record the prefix information of a transit network.

2） Associate router-LSAs and record the prefix information on all Loopback interfaces, point-to-point links, point-to-multipoint links, virtual links and stub networks of the router in the current area.

Other main change of LSA association:

- LSA flooding scope

In the OSPFv2, the LSA flooding occurs inside areas and ASs. In the OSPFv3, flooding occurs in local link. Type 8 Link-LSAs is the type that can flood only inside a locla link.

- Handling an unknown LSA type

This is an improvement made by the OSPFv3 based on the OSPFv2.

In the OSPFv2, database synchronization is necessary in the initial establishment of adjacency relationship. If there is an unrecognizable LSA type in the database description message, this relationship cannot be established properly. If there is an unrecognizable LSA type in a link-state updating message, then the type of LSAs will be discarded.

In the OSPFv3, it is allowed to receive an unknown LSA type. By using the information recorded in the LSA header, we can determine how to handle the received unrecognizable LSA type.

5.1.2 Interface Configuration

In the OSPFv3, the change based on interface configuration is as follows:

- In order for an interface to run OSPFv3, enable the OSPFv3 directly in the interface configuration mode. For OSPFv2, however, run the **network** command in the OSPF route configuration mode.
- If an interface runs OSPFv3, all the addresses on the interface will run IPv6. In the OSPFv2,however, all the addresses are enabled via a **network** command.

In the environment where the OSPFv3 runs, a link can support multiple OSPF entities and different devices connecting this link can run one of these OSPF entities. The OSPFv2 does not support this function.

5.1.3 Router ID Configuration

RFC5340 specifies the OSPFv3 Router ID is in the format of 32-bit IPv4 address but not the IPv6 address.

By default, the methods of electing the OSPFv3 Router ID and the OSPFv3 process are the same. The automatic election method is adopted. Firstly, select the maximum IPv4 address for the loopback interface as the Router ID, if the loopback interface has not been configured, OSPFv3 process will select the maximum IPv4 address for other interface as the Router ID. With multiple OSPFv3 processes running in the device, OSPFv3 process select the Router ID with the highest priority from the unselected IPv4 addresses. Different Router IDs are for the different processes.

If the IPv4 addresses for the Router ID selection are insufficient, OSPFv3 process will fail to auto-obtain the Router ID. You can use the **router-id** command to configure a Router ID to enable the OSPFv3 process.

Caution

The Router ID for each router in the AS must be sole. With multiple OSPFv3 processes running in the same device, the Router ID for each process must also be sole.

5.1.4 Authentication Mechanism Configuration

The OSPFv2 itself supports two authentication modes: plain text authentication and key authentication based on MD5. The OSPFv3 itself does not provide any authentication. Instead, it uses the IPSec authentication mechanism. In future, we will support the IPSec authentication mechanism.

5.2 Basic OSPFv3 Configuration

Default OSPFv3 configuration:

Router ID		Undefined
Interface Configuration	Interface type	Broadcast network
	Interface cost	Undefined
	Hello message sending interval	10 seconds
	Dead interval of adjacent device	4 times the hello interval.
	LSA sending delay	1 seconds

Router ID		Undefined
	LSA retransmit interval	5 seconds
	Priority	1
	MTU check of database description messages	Enabled
Virtual Link	Virtual Link	Undefined
	Hello message sending interval	10 seconds
	Dead interval of adjacent device	4 times the hello interval.
	LSA sending delay	1 seconds
	LSA retransmit interval.	5 seconds
Area Configuration	Area	Undefined
	Default router cost for stub and NSSA area	1
Route Information Aggregation	Inter-area route aggregation	Off
	External route aggregation	Off
Management Distance	Intra-area route	110
	Inter-area route	110
	External route	110
Auto cost		Enabled The default cost reference is 100 Mbps.
Changing LSAs Group Pacing		240 seconds
Shortest path first (SPF) timer		Time from receiving the topology change to running SPF at the next time :5 seconds The least interval between two calculations:
Route redistribution		Off
Route filtering		Off
Passive interface		Off

5.2.1 Enabling OSPFv3

To run the OSPFv3, execute the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
ipv6 router ospf *process-id*	Start the OSPFv3 route process and enter the OSPFv3 configuration mode.
router-id *router-id*	Configure the Router ID for running the OSPFv3.
interface *interface-type interface-id*	Enter the interface configuration mode.
ipv6 ospf *process-id* **area** *area-id* **[instance-id** *instance-id***]**	Enable the OSPFv3 on an interface. *instance-id:* The OSPFv3 entity number that the interface participates in. The interfaces of different devices connecting a network select to participate in different OSPFv3 entities.
copy running-config startup-config	Save the configuration.

Note

The OSPFv3 instance ID and process ID are different. OSPFv3 process ID is valid for the device itself only, not influencing the interaction with other router devices. While the OSPFv3 instance ID influences the interaction with other router devices. Only the devices with the same instance ID can set up the OSPFv3 neighbor relationship.

Caution

In the interface configuration mode, first enable the interface to participate in OSPFv3 and then configure the OSPFv3 process. After you configure the OSPFv3 process, the interface will automatically participate in the appropriate process.

DES-7200 product support up to 32 OSPFv3 processes.

5.2.2 Configuring OSPF Parameters on the Interface

In the interface configuration mode, you can modify the OSPF parameters of an interface to meet practice application needs.

To configure OSPF parameters on the interface, execute the following commands in the interface configuration mode:

Command	Function
ipv6 ospf *process-id* **area** *area-id*	Configure the interface to participate in the

Command	Function
[instance-id *instance-id***]**	OSPFv3 routing process.
ipv6 ospf network {**broadcast** | **non-broadcast** | **point-to-point** | **point-to-multipoint** [**non-broadcast**]} [**instance** *instance-id*]	Set the network type of an interface. The default is the broadcast network type.
ipv6 ospf neighbor *ipv6-address* {[**cost** <*1-65535*>] | [**poll-interval** <*0-2147483647*> | **priority** <*0-255*>]} [**instance** *instance-id*]	(Optional) Set the OSPFv3 neighbor.
ipv6 ospf cost *cost* [**instance** *instance-id*]	(Optional) Define the cost of an interface.
ipv6 ospf hello-interval *seconds* [**instance** *instance-id*]	(Optional) Set the time interval to send the Hello message on an interface. For all nodes in the whole network, the value must be same.
ipv6 ospf dead-interval *seconds* [**instance** *instance-id*]	(Optional) Set the adjacency dead-interval on an interface. For all nodes in the whole network, the value must be same.
ipv6 ospf transmit-delay *seconds* [**instance** *instance-id*]	(Optional) Set the interval of transmitting link state.
ipv6 ospf retransmit-interval *seconds* [**instance** *instance-id*]	(Optional) Set the LSA transmit delay on an interface.
ipv6 ospf priority *number* [**instance** *instance-id*]	(Optional) Set the priority of an interface. The priority is used to select Designated Routers (DR) and Backup Designated Routers (BDR).

To remove the configuration, use the **no** form of the above commands.

Caution

You can modify the parameter setting of an interface based on actual needs. However, be sure that the settings of some parameters must be identical to those of neighbors. Otherwise, it will be impossible to establish the adjacency relationship. These parameters include the following: **instance, hello-interval and dead-interval.**

5.2.3 Configuring OSPFv3 Area Parameter

The OSPF protocol applies the concept of “hierarchical structure”, allowing a network to be divided into a group of parts connected through a “backbone” in

mutual independence way. These parts are called Areas. The backbone part is called Backbone Area and always indicated by the numerical value 0 (or 0.0.0.0).

By using this hierarchical structure, each device is allowed to keep the link state database in the area where it resides and the topology inside the area is invisible to outside. In this way, the link state database of each device can be always in a reasonable size, route calculation time is not too much and the number of messages is not too big.

In the OSPF, the following types of special areas have been defined to meet actual needs:

- stub Area.

If an area is at the end part of the whole network, then we can design the area as a stub area.

A stub area cannot learn the external route information of an AS (type 5 LSAs). In practical application, external route information is very important in the linkstate database. Therefore, the devices inside a stub area will learn little route information, reducing the system resources for running the OSPF protocol.

When a device inside a stub area wants to access outside of an AS, use the default route entrie (type3 LSA) generated from the default route information published by Area Border Routers in the stub area.

- NSSA area (Not-So-Stubby Area)

NSSA extends the stub area. By preventing from flooding type 5 LSAs to the devices in the NSSA, it reduce the consumption of device resources. However, unlike a stub area, it allows a certain amount of external route information of the AS to enter an NSSA in other ways, namely, inject into the NSSA in the form of type 7 LSAs.

To configure OSPFv3 area parameters, execute the following command in the OSPFv3 configuration mode:

Command	Function
area *area-id* **stub** [**no-summary**]	Configure a stub area. no-summary: configure the area to a totally stub area, preventing the area border router in the stub area from sending type3 and type4 LSAs to the stub area.
area *area-id* **default-cost** *cost*	Configure the cost of the default route sent to a stub area or NSSA.

To remove the configuration, use the **no** form of the above commands.

Caution

After configured an area as the stub area, you can configure the default-cost parameter. If this area is changed as an ordinary area, the default-cost configuration will be deleted automatically.

5.2.4 Configuring OSPFv3 Virtual Link

In the OSPF, all areas must connect to the backbone area to ensure the communication with other areas.If some areas cannot connect to the backbone area, they must use virtual links to connect the backbone area.

To establish a virtual link, execute the following command in the OSPFv3 configuration mode:

Command	Function
area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**dead-interval** *seconds*] [**transmit-delay** *seconds*] [**retransmit-interval** *seconds*] [**instance** *instance-id*]	Configure a virtual link. By default, the virtual link is not configured. *area-id:* the ID for the area where the virtual link is. *router-id:* the router-id for the virtual link neighbor. Other parameters are the same as the interface parameters.

To remove the configuration, use the **no** form of the above commands.

Caution

1. It is not allowed to create a virtual link in the stub area and NSSA.
2. A virtual link can be taken as a special interface, so its configuration is same to that of a normal interface. You must ensure that the configurations of **instance, hello-interval** and **dead-interval** configured at the two ends of the virtual link are identical.

5.2.5 Configuring OSPFv3 Route Aggregation

Without route aggregation, every device in a network must maintain the routeing information of the whole network. By aggrgating some information together, route aggregation can alleviate the burden on the L3 equipment and network bandwidth. As the size of a network is growing, route aggregation becomes more and more important.

5.2.5.1 Configuring Inter-area Route Aggregation

The ABR in an area needs to advertise the routes in the area to other areas. If the route addresses are continuous, the ABR aggregates these routes and then advertises it.

To configure inter-area route aggregation, execute the following command in the OSPFv3 configuration mode:

Command	Function
area *area-id* **range** *ipv6-prefix*/*prefix-length* [**advertise** | **not-advertise**]	Configure inter-area route aggregation. *area-id*: Set the aggregated area id. *ipv6-prefix/prefixlength*: Set the ipv6 prefix of the aggregated route. **advertise|not-advertise**: Advertise or not advertise the aggregated summary-LSA.

Use the **no area** *area-id* **range** {*ipv6-prefix* /*prefix-length*} command to disable the inter-area route aggregation.

5.2.5.2 Configuring Outer-area Route Aggregation

The route aggregation is allowed to take place when redistributing the generated Type-5 LSA on the ASBR.

To configure outer-area route aggregation, execute the following command in the OSPFv3 configuration mode:

Command	Function
summary-prefix *ipv6-prefix* / *prefix-length* [**not-advertise** | **tag** *tag-value*]	Configure outer-area route aggregation. *ipv6-prefix/prefixlength*: Set the ipv6 prefix of the aggregated route. **not-advertise**: Not advertise the aggregated LSA. *tag-value*: The valid range is <*0-4294967295*>, used to specify the tag value for the aggregated LSA.

Use the **no summary-prefix** *ipv6-prefix*/*prefix-length* command to disable the outer-area route aggregation.

5.2.6 Configuring Bandwidth Reference Value of OSPFv3 Interface Metric

The metric for the OSPF protocol is a bandwidth value based on an interface. The

cost value of the interface is calculated based on its bandwidth.

For example, if the bandwidth reference value of an interfaces is 100 Mbps and the bandwidth of theinterfaces is 10Mbps, the automatically calculated interface cost is 100/10=10.

Currently, the interface refernece value of network interfaces is defaulted to 100 Mbps.

To change the bandwidth reference value, execute the following command in the OSPFv3 configuration mode:

Command	Function
auto-cost [**reference-bandwidth** *ref-bw*]	Configure the bandwidth reference value for interface metric, in Mbps.

Caution

You can run the **ipv6 ospf cost** *cost-value* command in the interface configuration mode to set the cost for a specified interface, which takes precedence over the one calculated based on bandwidth reference value.

5.2.7 Configuring Whether to Check the MTU when DD Packets are Received on the OSPFv3 Interface

When the OSPFv3 receives the DD(Database Description) packets, it checks whether the MTU for the neighbor interface is the same as the MTU for the interface itself. If the former one is larger than the latter one, it fails to set up the neighbor relationship. To solve the problem, you can disable the MTU checksum function or modify the MTU for the IPv6 interface.

To disable the MTU checksum function on an interface, use the following command in the interface configuration mode:

Command	**Function**
ipv6 ospf mtu-ignore [**instance** *instance-id*]	Disable the MTU checksum function when the DD packets are received on an interface.

By default, the MTU checksum on the interface is enabled.

5.2.8 Configuring OSPFv3 Default Route

In the OSPFv3 protocol, you can generate default route in many ways. For example, the default route represented by Type-3 LSA will be automatically generated in a stub area. For details, refer to Configuring OSPFv3 Area Parameters. In addition, you can configure a default route represented by Type 5

LSA and advertise it to the whole OSPF AS.

To configure a default rotue, execute the following commands in the OSPFv3 configuration mode:

Command	Function
default-information originate [always] [metric *metric-value*] **[metric-type** *type-value*] **[route-map** *map-name*]	Configure a default route. **always**：With this parameter configured, no matter what the condition the system routing is, a default LSA originates always. Without this parameter configured, only does the default routing exist in the core routing list, the default LSA originates and is advertised. *metric:* The valid range is 0-16777214. **metric-type**：The external routing type of the corresponding default routing. **route-map**：Set the corresponding route-map rule for the originated LSA.

Execute the **no default-information originate** command to remove the generated default route.

Caution

1. This command cannot be configured on the devices in a stub area.
2. Once configured, the device automatically becomes ASBR.

5.2.9 Configuring OSPFv3 Route Redistribution

Route redistribution allows you to redistribute the routes of one routing protocol to another routing protocol.

To configure the OSPFv3 route redistribution, execute the following commands in the OSPFv3 configuration mode:

Command	Function
redistribute {**bgp** | **connected** | **isis** [*area-tag*] | **ospf** *process-id* | **rip** | **static**} [{**level-1** | **level-1-2** | **level-2**} |	Redistribute the routes of one routing protocol to another routing protocol. You can set the conditions of redistribution.

Command	Function
match {**internal** | **external** [**1**|**2**]} | **metric** *metric-value* | **metric-type** {*1*|*2*} | **route-map** *route-map-name* | **tag** *tag-value*]	At present, the OSPFv3 supports redistribution of static, connect, rip, bgp, isis and ospf route redistribution. When redistributing ISIS routes, you can configure the level parameter to redistribute the ISIS routes of the specified level. When redistributing OSPF routes, you can configure the match parameter to redistribute the OSPF routes of the specific sub type.
default-metric *number*	Configure the default metric for route redistribution.

You can use the **no redistribute** *protocol* mode to disable route redistribution.

5.2.10 Configuring OSPFv3 Timer

The OSPFv3 protocol belongs to link-state protocols. When the link state changes, the OSPFv3 process will trigger the SPF calculation. The SPF calculation delay is configurable, you can also use the command to configure the minumum and maximum interval between two SPF calculations.

To configure the OSPFv3 timer, use the following command in the routing process configuration mode:

Command	Function
timers throttle spf *spf-delay spf-holdtime spf-max-waittime*	Configure the OSPFv3 timer, in ms.

The parameter *spf-delay* refers to the delay time from the topology change to the beginning of the SPF calculation.

The parameter *spf-holdtime* refers to the minimum interval of two SPF calculations. It is worth mentioning that the next SFP holdtime shall at least be twice as the last one till the interval reaches the configured *spf-max-waittime*. If the SPF calculation intervals have exceeded the minimum value, it will re-calculate the SPF calculation interval from the

spf-holdtime.

Note

In normal conditions, when the link changes, reducing the *spf-delay* and *spf-holdtime* value can improve the OSPF convergence speed. Setting the maximum *spf-max-waittime* avoid the CPU consumption due to the continuous link turbulance.

For example, **timers throttle spf** *1000 5,000 100,000*

If the topology keeps changing, the SPF calucation intervals(cannot exceed the max-wait-time) are 1s, 6s, 16s, 36s, 76s, 156s, 256s, 256+100, ……

To configure the OSPFv3 timer SPF delay and holdtime, use the following command in the routing process configuration mode:

Command	Function
DES-7200 (config-router)# **timers spf** *spf-delay spf-holdtime*	Configure the OSPFv3 timer, in seconds.

Caution

The **timers spf** and **timers throttle spf** commands are overwritten, and the latter-configured one is valid. With both commands not configured, the default value is **timers throttle spf.**

It is recommended to use the **timer throttle spf** command.

5.2.11 Configuring OSPFv3 Passive Interface

To prevent other Layer 3 devices in the network from learning the route information of this device, you can set a network interface to a passive interface in the routing protocol configuration mode

For the OSPFv3 protocol, if a network interface is configured as a passive network interface, then this network interface will receive/send no OSPF message.

To configure an interface as a passive interface, execute the following command in the OSPF3 configuration mode:

Command	Function
passive-interface {**default** | *interface-type interface-number* }	Configure a passive interface. default: with this parameter configured, all interfaces will be set as the passive interfaces. Interface: set the specified interface as the passive interface. Use the **passive-interface default** and **no passive-interface** *interface* command to set the specified interface as the non-passive interface, and other interfaces as the passive interfaces.

You can use the **no passive-interface** {*interface-id* | **default**} command to cancel the configuration of a passive interface.

5.2.12 Configuring the OSPFv3 Route Management Distance

The route management distance, representing the reliability of the route source, is used to compare the priorities for different routing protocols. The valid range for the management distance is 0-255. The smaller the management distance is, the higher the route priotity is, and the higher the route source reliability is.

By default, the OSPFv3 route management distance is 110. You can configure different management distances for different OSPFv3 routes in the intra-area, inter-area and external routes.

To modify the OSPFv3 route management distance, use the following command in the routing process configuration mode:

Command	Function
distance {*distance* | **ospf** { **intra-area** *distance* | **inter-area** *distance* | **external** *distance* }}	Modify the OSPFv3 route management distance.

Caution

The management distance must be used to compare the priorities of the different routes originated from the different OSPFv3 processes.

5.2.13 Configuring the OSPFv3 BFD

For the detailed OSPFv3 BFD configurations, refer to the chapter of *BFD Configuration*.

5.2.14 Debugging and Monitoring OSPFv3

The OSPFv3 process supports plenty of debug commands and monitoring commands.

5.2.14.1 OSPFv3 Debugging Command

To debug OSPFv3, execute the following commands in the privileged configuration mode:

Command	Function
debug ipv6 ospf events	Show the OSPFv3 event information.
debug ipv6 ospf ifsm	Show the state machine events and changes of the outbounding interface.
debug ipv6 ospf lsa	Show the related OSPFv3 LSA information.
debug ipv6 ospf nfsm	Show state machine events and changes of neighbor.
debug ipv6 ospf nsm	Show the OSPFv3 NSM module related information.
debug ipv6 ospf packet	Show the OSPFv3 packet information.
debug ipv6 ospf route	Show the OSPF routing calculation and addition information.

Use the above **undebug** commands to disable the above enabled **debug** commands.

Caution

The **debug** commands are provided for technicians.

Running a **debug** command will affect the performance of the system in a certain extent. Therefore, after running **debug** commands, be sure to use **undebug** commands to protect the performance of the system.

5.2.14.2 OSPFv3 Monitoring Command

To monitor OSPFv3, execute the following commands in the privileged configuration mode:

Command	Function
show ipv6 ospf	Show the information of the OSPFv3

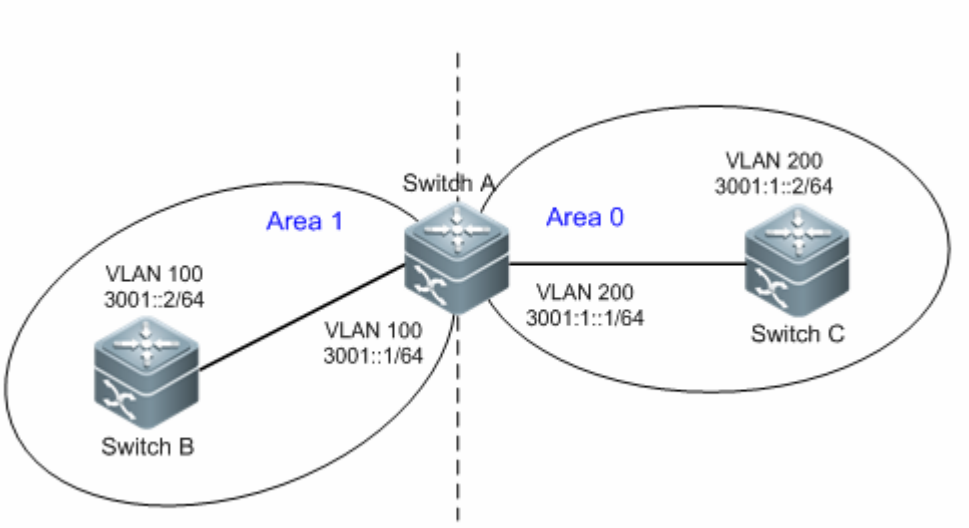
Command	Function
	process.
show ipv6 ospf [*process-id*] **database** [**isa-type** [**adv-router** *router-id*]]	Show the database information of the OSPF process.
show ipv6 ospf interface *[interface-type interface-number]*	Show the interface information of the OSPFv3 process.
show ipv6 ospf [*process-id*] **neighbor** [*interface-type interface-number* [**detail**]] *[neighbor-id*] [**detail**]	Show the neighbor information of the OSPFv3 process.
show ipv6 ospf [*process-id*] **route**	Show the OSPFv3 route information.
show ipv6 ospf [*process-id*] **topology** [**area** *area-id*]	Show each area topology of the OSPFv3.
show ipv6 ospf [*process-id*] **virtual-links**	Show the virtual link information of the OSPFv3 process.

5.3 OSPFv3 Configuration Example

5.3.1 OSPFv3 Basic Configuration Example

The following configuration example shows commands related to OSPF configuration.

Topological Diagram



OSPFv3 basic configuration

SwitchA and SwitchB belong to Area 0, while Switch A and Switch C belong to

Area 1. The intercommunication between three switches is realized via vlan interface.

Application Requirements

Enable OSPFv3 on all switches and specify two areas; IPv6 packets can be forwarded between two areas.

Configuration Tips

Configure Area0 and Area1, and enable OSPFv3 on the corresponding VLAN interface of switch (interface vlan 100 or vlan 200 of SwtichA/SwitchB/SwitchC)

The router-id must be specified, or else the adjacency cannot be created. Automatic acquisition of router-id is supported in 10.4 and subsequent releases.

Vlan must be created first, or else the VLAN interface cannot join OSPFv3.

Configuration Steps

- SwitchA

Step 1: Create VLAN and configure IPv6 address

```
SwitchA# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchA(config)# vlan 100
SwitchA(config-vlan)#exit
SwitchA(config-vlan)#interface vlan 100
SwitchA(config-if-VLAN 100)#ipv6 enable
SwitchA(config-if-VLAN 100)#ipv6 address 3001::1/64
SwitchA(config-if-VLAN 100)#exit
```

! Create and configure interface vlan200

```
SwitchA(config)#vlan 200
SwitchA(config-vlan)#interface vlan 200
SwitchA(config-if-VLAN 200)#ipv6 enable
SwitchA(config-if-VLAN 200)#ipv6 address 3001:1::1/64
SwitchA(config-if-VLAN 200)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchA(config)#ipv6 router ospf  10
SwitchA(config-router)#router-id 1.1.1.1
Change router-id and update OSPFv3 process!  [yes/no]:y
SwitchA(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0

```
SwitchA(config)#interface vlan 100
SwitchA(config-if-VLAN 100)#ipv6 ospf 10 area 0
SwitchA(config-if-VLAN 100)#exit
```

Step 4: Enable OSPFv3 on interface vlan 200, with area being Area1

```
SwitchA(config)#interface vlan 200
SwitchA(config-if-VLAN 200)#ipv6 ospf 10 area 1
SwitchA(config-if-VLAN 200)#end
```

- SwitchB

Step 1: Create VLAN and configure IPv6 address

```
SwitchB# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchB(config)# vlan 100
SwitchB(config-vlan)#interface vlan 100
SwitchB(config-if-VLAN 100)#ipv6 enable
SwitchB(config-if-VLAN 100)#ipv6 address 3001::2/64
SwitchB(config-if-VLAN 100)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchB(config)#ipv6 router ospf 10
SwitchB(config-router)#router-id 2.2.2.2
Change router-id and update OSPFv3 process!  [yes/no]:y
SwitchB(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0

```
SwitchB(config)#interface vlan 100
SwitchB(config-if-VLAN 100)#ipv6 ospf 10 area 0
SwitchB(config-if-VLAN 100)#end
```

- SwitchC

Step 1: Create VLAN and configure IPv6 address

```
SwitchC#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan200

```
SwitchC(config)#vlan 200
SwitchC(config-vlan)#interface vlan 200
SwitchC(config-if-VLAN 200)#ipv6 enable
SwitchC(config-if-VLAN 200)#ipv6 address 3001:1::2/64
SwitchC(config-if-VLAN 200)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchC(config)#ipv6 router ospf 10
SwitchC(config-router)#router-id 3.3.3.3
Change router-id and update OSPFv3 process!  [yes/no]:y
SwitchC(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 200, with area being Area1

```
SwitchC (config)#interface vlan 200
SwitchC (config-if-VLAN 200)#ipv6 ospf 10 area 1
SwitchC (config-if-VLAN 200)#end
```

Verify configurations

Step 1: Verify whether the configurations are correct. Key points: whether router-id is specified, whether OSPFv3 is enabled on the interface, and whether such parameters as OSPFv3 timer are identical in the same area.

- SwitchA

```
vlan 100
!
vlan 200
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::1/64
 ipv6 enable
ipv6 ospf 10 area 0
!
interface VLAN 200
 no ip proxy-arp
 ipv6 address 3001:1::1/64
 ipv6 enable
ipv6 ospf 10 area 1
!
ipv6 router ospf 10
router-id 1.1.1.1
```

- SwitchB

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::2/64
 ipv6 enable
```

```
 ipv6 ospf 10 area 0
!
ipv6 router ospf 10
 router-id 2.2.2.2
```

■ SwitchC

```
vlan 200
!
interface VLAN 200
 no ip proxy-arp
 ipv6 address 3001:1::2/64
 ipv6 enable
 ipv6 ospf 10 area 1
!
ipv6 router ospf 10
 router-id 3.3.3.3
```

Step 2: Display OSPFv3 neighbors Key point: whether the adjacencies have been created.

```
SwitchA#show ipv6 ospf neighbor
OSPFv3 Process (10), 2 Neighbors, 2 is Full:
Neighbor ID   Pri  State      Dead Time   Instance ID   Interface
2.2.2.2       1   Full/BDR    00:00:37    0           VLAN 100
3.3.3.3       1   Full/DR     00:00:34    0           VLAN 200
```

The information displayed on SwitchB and SwitchC is the same as the information displayed on SwitchA.

Step 3: Display OSPFv3 routes and ping IPv6 address in another area. Key point: whether all IPv6 routes and routes learned can be pinged.

```
SwitchC#show ipv6 route
IPv6 routing table name is Default(0) global scope - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF external type
1, OE2 - OSPF external type 2
       ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
       [*] - NOT in hardware forwarding table
L      ::1/128  via Loopback, local host
OI     3001::/64  [110/2] via FE80::21A:A9FF:FE15:4CB9, VLAN 200
C      3001:1::/64  via VLAN 200, directly connected
L      3001:1::2/128  via VLAN 200, local host
L      FE80::/10  via ::1, Null0
C      FE80::/64  via VLAN 200, directly connected
L      FE80::21A:A9FF:FE01:FB1F/128  via VLAN 200, local host
```

```
SwitchC#ping ipv6 3001::2
Sending 5, 100-byte ICMP Echoes to 3001::2, timeout is 2 seconds:
  < press Ctrl+C to break >
! ! ! ! !
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

The information displayed on SwitchA and SwitchB is the same as the information displayed on SwitchC.

5.3.2 OSPFv3 Redistribution Configuration Example

Configuration Requirements

For the connection of three devices, see the Figure-1.

- Enable the OSPFv3 protocol on RouterA; Enable BGP protocol and configure the static route on RouterC; For RouterB, redistribute the static route on the RouterC to the OSPFv3 domain. Set the specified community attribute for the static route redistributed to RouterC and redistribute the specified community attribute to the OSPFv3 domain on RouterB.
- Configure the external route aggregation on RouterB: aggregate the routes within the range of 2001:db8:77::/48 and notify the aggregation to the OSPFv3 domain.
- To speed up the convergence, set the SPF calculation delay time, holdtime and max-waittime for RouterA and RouterB as 5ms, 1000ms and 90000ms.

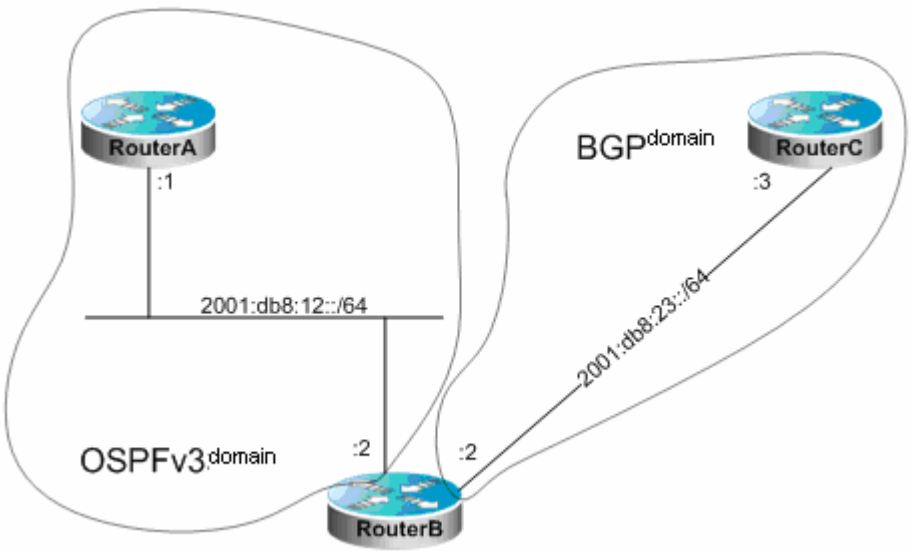


Figure-1 OSPFv3 Redistribution Configuration Example

Configuration Steps

Router A Configuration:

Configure the network interface

```
DES-7200(config)# interface gigabitEthernet 0/1

DES-7200(config-if)# ipv6 enable

DES-7200(config-if)# ipv6 address 2001:db8:12::1/64

DES-7200(config-if)# ipv6 ospf 12 area 0
```

Configure OSPFv3

```
DES-7200(config)# ipv6 router ospf 12

DES-7200(config-router)# router-id 1.1.1.1

DES-7200(config-router)# timers throttle spf 5 1000 90000
```

Router B Configuration:

Configure the network interface

```
DES-7200(config)# interface gigabitEthernet 0/1

DES-7200(config-if)# ipv6 enable

DES-7200(config-if)# ipv6 address 2001:db8:12::2/64

DES-7200(config-if)# ipv6 ospf 12 area 0

DES-7200(config)# interface gigabitEthernet 0/2

DES-7200(config-if)# ipv6 enable

DES-7200(config-if)# ipv6 address 2001:db8:23::2/64
```

Configure OSPFv3

```
DES-7200(config)# ipv6 router ospf 12

DES-7200(config-router)# router-id 2.2.2.2

DES-7200(config-router)# redistribute bgp route-map ospfrm

DES-7200(config-router)# timers throttle spf 5 1000 90000

DES-7200(config-router)# summary-prefix 2001:db8:77::/48
```

Configure BGP

```
DES-7200(config)# router bgp 2

DES-7200(config-router)# neighbor 2001:db8:23::3 remote-as 3

DES-7200(config-router)# address-family ipv6
```

```
DES-7200(config-router-af)# neighbor 2001:db8:23::3 activate
```

Configure route-map

```
DES-7200(config)# route-map ospfrm

DES-7200(config-route-map)# match community cl_110
```

Define community list

```
DES-7200(config)# ip community-list standard cl_110 permit 22:22
```

Router C Configuration:

Configure the network interface

```
DES-7200(config)# interface gigabitEthernet 0/1

DES-7200(config-if)# ipv6 enable

DES-7200(config-if)# ipv6 address 2001:db8:23::3/64
```

Configure BGP

```
DES-7200(config)# router bgp 3

DES-7200(config-router)# neighbor 2001:db8:23::2 remote-as 2

DES-7200(config-router)# address-family ipv6

DES-7200(config-router-af)# redistribute static route-map bgprm

DES-7200(config-router-af)# neighbor 2001:db8:23::2 activate

DES-7200(config-router-af)# neighbor 2001:db8:23::2 send-community
```

Configure static route

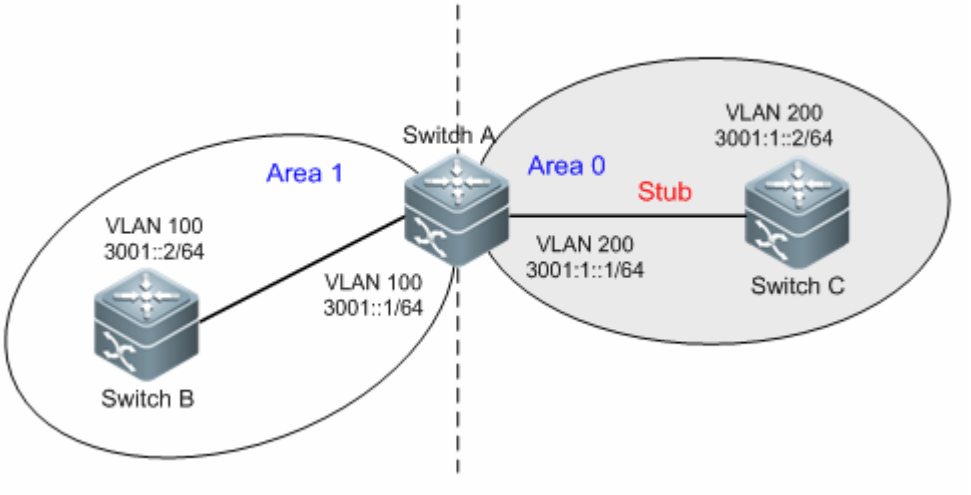
```
DES-7200(config)# ipv6 route 2001:db8:77:88::/64 null 0

DES-7200(config)# ipv6 route 2001:db8:77:99::/64 null 0
```

Configure route-map

```
DES-7200(config)# route-map bgprm

DES-7200(config-route-map)# set community 22:22
```

5.3.3 Example of stub area configuration

Topological Diagram



OSPFv3 stub area

Application Requirements

Configure Area 1 as a stub area in order to lessen the system overhead of switches in this area.

Configuration tips

Use the parameter of "stub no-summary" on the area border router (Switch A)

Use the parameter of "stub" on the non-area-border router（Switch C)

Configuration Steps

- **SwitchA**

Step 1: Configure OSPFv3 basic functions

Step 2: Configure stub no-summary

```
SwitchA# conf
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ipv6 router ospf 10
SwitchA(config-router)#area 1 stub no-summary
SwitchA(config-router)#exit
```

- **SwitchC**

Step 1: Configure OSPFv3 basic functions

Step 2: Configure stub

```
SwitchC# conf
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ipv6 router ospf 10
SwitchA(config-router)#area 1 stub
```

```
SwitchA(config-router)#exit
```

Verify configurations

Step 1: Verify whether the configurations are correct. While making sure the OSPFv3 basic functions have been correctly configured, pay attention to the difference in stub parameter between ABR and other router.

- **SwitchA**

```
vlan 100
!
vlan 200
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::1/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
interface VLAN 200
 no ip proxy-arp
 ipv6 address 3001:1::1/64
 ipv6 enable
 ipv6 ospf 10 area 1
!
ipv6 router ospf 10
 router-id 1.1.1.1
 area 1 stub no-summary
!
```

- **SwitchC**

```
vlan 200
!
interface VLAN 200
 no ip proxy-arp
 ipv6 address 3001:1::2/64
 ipv6 enable
 ipv6 ospf 10 area 1
!
ipv6 router ospf 10
 router-id 3.3.3.3
 area 1 stub
 !
```

Step 2: Display OSPFv3 neighbors. Key point: whether the adjacencies have been created.

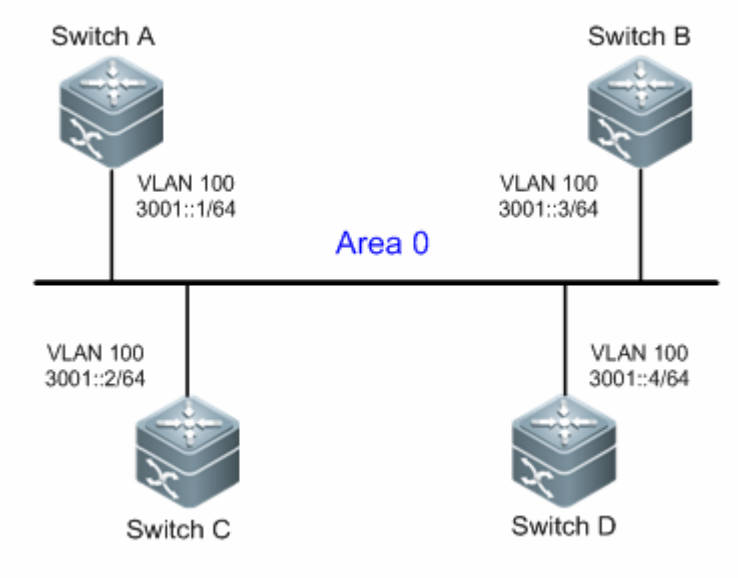
```
SwitchA#show ipv6 ospf neighbor
OSPFv3 Process (10), 2 Neighbors, 2 is Full:
Neighbor ID   Pri  State      Dead Time   Instance ID   Interface
2.2.2.2       1   Full/BDR    00:00:37    0           VLAN 100
3.3.3.3       1   Full/DR     00:00:34    0           VLAN 200

Similar information will be displayed on SwitchC.
```

Step 3: Display OSPFv3 routes. Key point: whether the default route is generated, and whether the inter-area route exists

```
SwitchC #show ipv6 route
IPv6 routing table name is Default(0) global scope - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
  I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
  O - OSPF intra area, OI - OSPF inter area,  OE1 - OSPF external type 1, OE2
- OSPF external type 2
ON1 - OSPF NSSA external type 1, ON2 - OSPF NSSA external type 2
      [*] - NOT in hardware forwarding table
OI    ::/0  [110/2] via FE80::21A:A9FF:FE15:4CB9, VLAN 200
L     ::1/128  via Loopback, local host
C     3001:1::/64  via VLAN 200, directly connected
L     3001:1::2/128  via VLAN 200, local host
L     FE80::/10  via ::1, Null0
C     FE80::/64  via VLAN 200, directly connected
L     FE80::21A:A9FF:FE01:FB1F/128  via VLAN 200, local host
```

5.3.4 Example of OSPFv3 DR election configuration

Topological Diagram



OSPFv3 DR election

SwitchA, SwitchB, SwitchC and SwitchD are in the same area (Area 0) and are interconnected via vlan 100. Switch A and Switch B are devices with the best configuration and the highest stability on the network.

Application Requirements

Corresponding requirements: By adjusting the priority, configure SwitchA as the DR and SwitchB as the BDR in order to avoid route oscillation.

Configuration Tips

Configure the priority of the interface of expected DR (Switch A) to he highest value (150 in this example) and the priority of the interface of BDR (Switch B) to the second highest value (50 in this example)

The default priority of interface is 1, and DR/BDR can be determined according to router-id. Generally, the router with the largest router-id will become DR, and the router with the second largest router-id will become BDR.

Configuration Steps

- **SwitchA**

Step 1: Create VLAN and configure IPv6 address

```
SwitchA# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchA(config)# vlan 100
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 100
SwitchA(config-if-VLAN 100)#ipv6 enable
```

```
SwitchA(config-if-VLAN 100)#ipv6 address 3001::1/64
SwitchA(config-if-VLAN 100)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchA(config)#ipv6 router ospf 10
SwitchA(config-router)#router-id 1.1.1.1
SwitchA(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0 and priority being 150

```
SwitchA(config)#interface vlan 100
SwitchA(config-if-VLAN 100)#ipv6 ospf 10 area 0
SwitchA(config-if-VLAN 100)# ipv6 ospf priority 150
SwitchA(config-if-VLAN 100)#end
```

- **SwitchB**

Step 1: Create VLAN and configure IPv6 address

```
SwitchB# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchB(config)# vlan 100
SwitchB(config-vlan)#exit
SwitchB(config)#interface vlan 100
SwitchB(config-if-VLAN 100)#ipv6 enable
SwitchB(config-if-VLAN 100)#ipv6 address 3001::2/64
SwitchB(config-if-VLAN 100)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchB(config)#ipv6 router ospf 10
SwitchB(config-router)#router-id 2.2.2.2
SwitchB(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0 and priority being 50

```
SwitchB(config)#interface vlan 100
SwitchB(config-if-VLAN 100)#ipv6 ospf 10 area 0
SwitchB(config-if-VLAN 100)# ipv6 ospf priority 50
SwitchB(config-if-VLAN 100)#end
```

- **SwitchC**

Step 1: Create VLAN and configure IPv6 address

```
SwitchC# conf
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchC(config)#vlan 100
SwitchC(config-vlan)#exit
SwitchC(config)##interface vlan 100
SwitchC(config-if-VLAN 100)#ipv6 enable
SwitchC(config-if-VLAN 100)#ipv6 address 3001::3/64
SwitchC(config-if-VLAN 100)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchC(config)#ipv6 router ospf 10
SwitchC(config-router)#router-id 3.3.3.3
SwitchC(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0 and priority using the default value.

```
SwitchC(config)#interface vlan 100
SwitchC(config-if-VLAN 100)#ipv6 ospf 10 area 0
SwitchC(config-if-VLAN 100)#end
```

- **SwitchD**

Step 1: Create VLAN and configure IPv6 address

```
SwitchD# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchD(config-vlan)#vlan 100
SwitchD(config-vlan)#exit
SwitchD(config)#interface vlan 100
SwitchD(config-if-VLAN 100)#ipv6 enable
SwitchD(config-if-VLAN 100)#ipv6 address 3001::4/64
SwitchD(config-if-VLAN 100)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchD(config)#ipv6 router ospf 10
SwitchD(config-router)#router-id 4.4.4.4
SwitchD(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0 and priority using the default value.

```
SwitchD(config)#interface vlan 100
SwitchD(config-if-VLAN 100)#ipv6 ospf 10 area 0
SwitchD(config-router)#end
```

Verify configurations

Step 1: Verify whether the configurations are correct. Key point: whether OSPF basic parameters and interface priority are correct

- **SwitchA**

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::1/64
 ipv6 enable
ipv6 ospf 10 area 0
ipv6 ospf priority 150
!
ipv6 router ospf 10
router-id 1.1.1.1
```

- **SwitchB**

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::2/64
 ipv6 enable
ipv6 ospf 10 area 0
ipv6 ospf priority 50
!
ipv6 router ospf 10
 router-id 2.2.2.2
```

- **SwitchC**

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::3/64
 ipv6 enable
ipv6 ospf 10 area 0
!
ipv6 router ospf 10
 router-id 3.3.3.3
```

■ **SwitchD**

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::4/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
ipv6 router ospf 10
 router-id 4.4.4.4
```

Step 2: Display OSPFv3 neighbors. Key point: whether the adjacencies have been created, and whether each switch assumes the correct role.

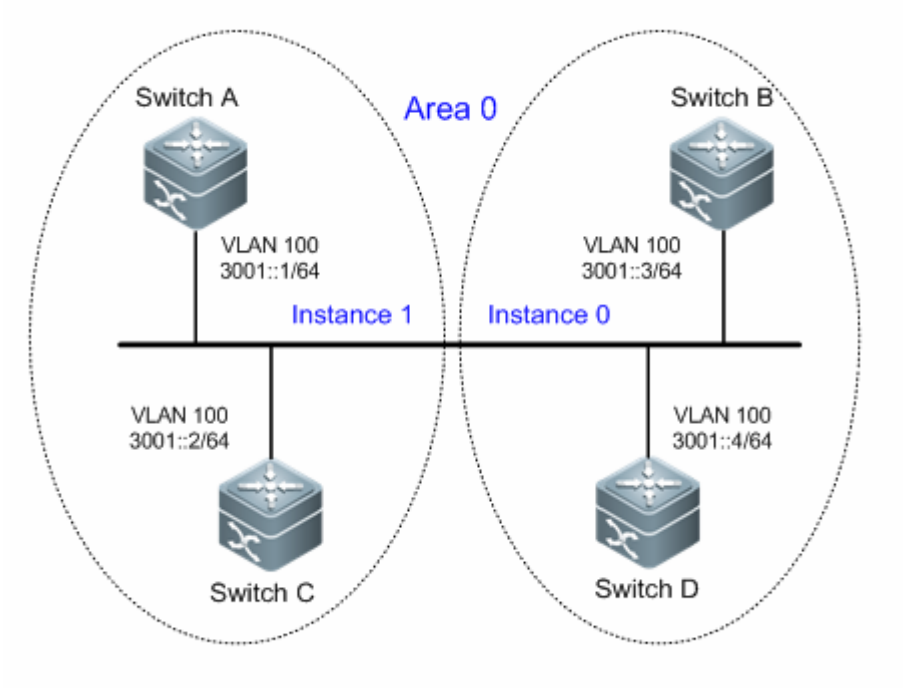
```
SwitchD#show ipv6 ospf neighbor
Neighbor ID  Pri   State    Dead Time   Interface ID    Interface
3.3.3.3      1   2WAY/DROTHER  00:00:33    4196         Vlan100
1.1.1.1      150   FULL/DR     00:00:35    4196          Vlan100
2.2.2.2      50   FULL/BDR     00:00:35    4196          Vlan100
```

Adjacencies before priority configuration are shown below. We can see that DR/BDR can be specified by adjusting the priority.

```
SwitchA#show ipv6 ospf neighbor
OSPFv3 Process (10), 3 Neighbors, 2 is Full:
Neighbor ID  Pri   Stat     Dead Time   Instance ID   Interface
2.2.2.2      1   Full/BDR       00:00:33    0           VLAN 100
3.3.3.3      1   2-Way/DROther   00:00:35   0           VLAN 100
4.4.4.4      1   Full/DR        00:00:33    0           VLAN 100
```

5.3.5 Example of OSPFv3 multiple instances per link configuration

Topological Diagram



Multiple instances per link

SwitchA, SwitchB, SwitchC and SwitchD are in the same area (Area 0) and are interconnected via vlan 100.

Application Requirements

On a broadcast link, especially within a same vlan, all switches will establish adjacencies with each other, and this may result in increased system overhead and network oscillation.

Application requirements: Switches in the same area are divided into several groups, and OSPFv3 adjacencies can only be established between switches belonging to the same group.

Configuration tips

By configuring multiple instances on the same link (the link on interface vlan100), adjacency establishment by group can be realized (in this example, SwitchA and SwitchB form a group, with instance ID being 1; SwitchC and SwitchD form a group, with instance ID being 0).

By default, the instance ID for interface is 0. In this example, you only need to configure the instance ID on Switch A and Switch B.

Configuration Steps

- **SwitchA**

Step 1: Create VLAN and configure IPv6 address

```
SwitchA# conf
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchA(config)# vlan 100
SwitchA(config-vlan)#interface vlan 100
SwitchA(config-if-VLAN 100)#ipv6 enable
SwitchA(config-if-VLAN 100)#ipv6 address 3001::1/64
SwitchA(config-if-VLAN 100)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchA(config)#ipv6 router ospf 10
SwitchA(config-router)#router-id 1.1.1.1
SwitchA(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0 and instance ID being 1

```
SwitchA(config)#interface vlan 100
SwitchA(config-if-VLAN 100)#ipv6 ospf 10 area 0 instance 1
SwitchA(config-if-VLAN 100)# end
```

- **SwitchB**

Step 1: Create VLAN and configure IPv6 address

```
SwitchB# conf
Enter configuration commands, one per line.  End with CNTL/Z.
```

! Create and configure interface vlan100

```
SwitchB(config)# vlan 100
SwitchB(config-vlan)#interface vlan 100
SwitchB(config-if-VLAN 100)#ipv6 enable
SwitchB(config-if-VLAN 100)#ipv6 address 3001::2/64
SwitchB(config-if-VLAN 100)#exit
```

Step 2: Create OSPFv3 process and specify the router-id

```
SwitchB(config)#ipv6 router ospf 10
SwitchB(config-router)#router-id 2.2.2.2
SwitchB(config-router)#exit
```

Step 3: Enable OSPFv3 on interface vlan 100, with area being Area0 and instance ID being 1

```
SwitchB(config)#interface vlan 100
SwitchB(config-if-VLAN 100)#ipv6 ospf 10 area 0 instance 1
SwitchB(config-if-VLAN 100)# end
```

Verify configurations

Step 1: Verify whether the configurations are correct. Key point: whether the instance ID for establishing adjacency between switches is correct.

- **SwitchA:**

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::1/64
 ipv6 enable
 ipv6 ospf 10 area 0 instance 1
!
ipv6 router ospf 10
 router-id 1.1.1.1
```

- **SwitchB:**

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::2/64
 ipv6 enable
ipv6 ospf 10 area 0 instance 1
!
ipv6 router ospf 10
 router-id 2.2.2.2
```

- **SwitchC:**

```
vlan 100
!
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::3/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
ipv6 router ospf 10
 router-id 3.3.3.3
```

- **SwitchD:**

```
vlan 100
!
```

```
interface VLAN 100
 no ip proxy-arp
 ipv6 address 3001::4/64
 ipv6 enable
 ipv6 ospf 10 area 0
!
ipv6 router ospf 10
 router-id 4.4.4.4
```

Step 2: Display the instance ID of interface link and reconfirm that the switch in the same group has the same instance ID

```
SwitchA#show ipv6 ospf interface vlan 100
VLAN 100 is up, line protocol is up
  Interface ID 4196
  IPv6 Prefixes
    fe80::21a:a9ff:fe15:4cb9/64 (Link-Local Address)
    3001::1/64
  OSPFv3 Process (10), Area 0.0.0.0, Instance ID 1
    Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State BDR, Priority 1
    Designated Router (ID) 2.2.2.2
      Interface Address fe80::2d0:f8ff:fe22:88b1
    Backup Designated Router (ID) 1.1.1.1
      Interface Address fe80::21a:a9ff:fe15:4cb9
    Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
      Hello due in 00:00:08
    Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 7 sent 8, DD received 3 sent 5
  LS-Req received 1 sent 1, LS-Upd received 5 sent 4
  LS-Ack received 3 sent 3, Discarded 0

SwitchB#show ipv6 ospf interface vlan 100
VLAN 100 is up, line protocol is up
  Interface ID 4196
  IPv6 Prefixes
    fe80::2d0:f8ff:fe22:88b1/64 (Link-Local Address)
    3001::2/64
  OSPFv3 Process (10), Area 0.0.0.0, Instance ID 1
    Router ID 2.2.2.2, Network Type BROADCAST, Cost: 1
    Transmit Delay is 1 sec, State DR, Priority 1
    Designated Router (ID) 2.2.2.2
      Interface Address fe80::2d0:f8ff:fe22:88b1
    Backup Designated Router (ID) 1.1.1.1
```

```
    Interface Address fe80::21a:a9ff:fe15:4cb9
   Timer interval configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:05
   Neighbor Count is 1, Adjacent neighbor count is 1
 Hello received 16 sent 21, DD received 10 sent 8
 LS-Req received 2 sent 2, LS-Upd received 10 sent 9
 LS-Ack received 6 sent 6, Discarded 0
```

Step 3: Display OSPFv3 neighbors. Key point: whether the adjacencies have been created, and the adjacency is established only between switches in the same group.

```
SwitchA#show ipv6 ospf neighbor
OSPFv3 Process (10), 1 Neighbors, 1 is Full:
Neighbor ID  Pri State     Dead Time   Instance ID   Interface
2.2.2.2      1   Full/DR   00:00:39    1             VLAN 100

SwitchB#show ipv6 ospf neighbor
OSPFv3 Process (10), 1 Neighbors, 1 is Full:
Neighbor ID  Pri  State       Dead Time   Instance ID   Interface

1.1.1.1      1   Full/BDR    00:00:34    1             VLAN 100
```

6 BGP Configuration

6.1 BGP Overview

The Border Gateway Protocol (BGP) is an Exterior Gateway Protocol (EGP) designed for routers in different autonomous systems to communicate one another. The goal is to exchange network reachability among different autonomous systems (AS) and eliminate loops by the natural features of the BGP protocol.

The BGP protocol uses the TCP protocol to transmit packets for its reliability.

The router which operates the BGP protocol is referred to as the BGP Speaker, and the BGP Speakers which set up a BGP session are referred to as the BGP Peers.

There are two modes of BGP session : IBGP (Internal BGP) and EBGP (External BGP). The IBGP refers to the BGP session set up in an AS, while the EBGP refers to the BGP session set up between different ASs. In a word, the EBGP exchanges the route information among different ASs; the IBGP transits the route information in an AS.

The BGP protocol features:

- Support BGP-4
- Support path attributes
- ORIGN Attribute
- AS_PATH Attribute
- NEXT_HOP Attribute
- MULTI_EXIT_DISC Attribute
- LOCAL-PREFERENCE Attribute
- ATOMIC_AGGREGATE Attribute
- AGGREGATOR Attribute
- COMMUNITY Attribute
- ORIGINATOR_ID Attribute
- CLUSTER_LIST Attribute

- Support BGP peer groups
- Support loopback interface
- Support MD5 authentication of TCP
- Support the synchronization of BGP and IGP
- Support the aggregation of BGP routes
- Support BGP route flap dampening
- Support BGP routing reflector
- Support AS confederation
- Support BGP soft reset
- Support BGP Graceful Restart (defined in RFC4724)

6.2 Enabling the BGP Protocol

To enable the BGP protocol, execute the following commands in the privileged mode:

Command	Function
DES-7200# configure terminal	Enter into the global configuration mode.
DES-7200(config)# **ip routing**	Enable the routing function (if the switch is disabled).
DES-7200(config)# **router bgp** *as-number*	Enable the BGP and configure the AS number. The range of *AS-number* is 1 to 65535.
DES-7200(config-router)# **bgp router-id** *router-id*	(Optional) Configure the ID used when this switch runs the BGP protocol.
DES-7200(config-router)# **end**	Return to the privileged EXEC mode.
DES-7200# **show run**	Show current configuration.
DES-7200# copy running-config startup-config	Save the configuration.

Use the **no router bgp** command to disable the BGP protocol**.**

6.3 Default BGP Configuration

The BGP protocol is not enabled by default.

After the BGP protocol is enabled, the default configuration of the BGP is shown as follows:

Router ID		To configure the loopback interface, select the maximum one from the loopback interface addresses. Otherwise, select the maximum interface address from the direct-connected interface.
Synchronization of BGP and IGP		Enabled
Generation of Default Route		Disabled
Multi hops of EBGP	Status	Off
	Number of hops	255
TCP MD5 Authentication		Disabled
Timer	Keepalive Time	60 seconds
	Holdtime	180 seconds
	ConnectRetry Time	120 seconds
	AdvInterval(IBGP)	15 seconds
	AdvInterval(EBGP)	30 seconds
Path Attribute	MED	0
	LOCAL_PREF	100
Route Aggregate		Off
Route Flap Dampening	Status	Off
	Suppress Limit	2000
	Half-life-time	15 minutes
	Reuse Limit	750
	Max-suppress-time	4*half-life-time
Route Reflector	Status	Off
	Cluster ID	Undefined
	Route among reflection clients	Enabled
AS Confederation		Off
Soft Reset		Off
Traceful Restart		Disabled
Management	External distanc	20

Distance	e	
	Internal-distance	200
	Local-distance	200

6.4 Injecting Route information into the BGP Protocol

The BGP protocol has no route information when it runs at the first time. There are two ways to inject the route information to the BGP:

- Manually inject the route information to the BGP by the **network** commands.
- Inject the route information to the BGP from the IGP protocol by the interaction with the IGP protocol.

The BGP will acvertise the injected route information to its neighbors. This section outline the manual injection of the route information. For the injection of the route information from the IGP protocol, refer to the *Configuration of BGP and IGP Interaction* in related section.

To manually inject the network information advertised by the BGP Speaker to other BGP Speaker, execute the following commands in the BGP configuration mode:

Command	Function
Router(config-router)# **network** network-number **mask** *network-mask*[**route-map** *map-tag*]	(Optional) Configure the network whose route information will be injected into the BGP routing table.

Use the **no network** *network-number* **mask** *network-mask* command to remove the configuration. If it is necessary to cancel the used route-map, configure it again by using the r*oute-map not added* option. If the configured network information is of standard class A, class B or class C network address, the mask option of this command may not be used.

In BGP4+, you can use this command in the IPv6 address family configuration mode to configure IPv6 routes.

Caution

1. The **network** command is used to inject the route of IGP into the routing table of BGP, and the advertised networks may be direct-connected route, static route and dynamic route.

2. For the external gateway protocol (EGP), the **network** command indicates the network to be advertised. This is different from the internal gateway protocol (IGP, such as OSPF and RIP). The latter uses the **network** commands to determine where the routing update message will be sent to.

Sometimes, you may need to use an IGP route rather than an EBGP route. This can be done through the **network backdoor** command. Execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)**# network** *network-number* **mask** *network-mask* **backdoor**	(Optional) Set the backdoor route.

Use the **no network** *network-number* **mask** *network-mask* **backdoor** command to remove the configuration.

Caution

By default, the management distance of the network information learned about from the BGP Speakers which establishes the EBGP connection is 20. Set the management distance of such network information by the **network backdoor** command as 200. Hence, the identical network information learned from the IGP presents higher priority. These networks learned from the IGP are considered as the backdoor network, and will not be advertised.

6.5 Controlling Route Advertisement

Control route advertisement

The BGP protocol can control the routes advertised to the core routing table by the **table-map** command. If a route is matched, the command modifies its attribute and advertises it. If a route is not matched or denied, the command advertises it without modifying its attribute.

By default, the **table-map** command advertises all routes without modifying their attributes.

To configure the **table-map** command, execute it in the BGP configuration mode or IPv4 address family confiugration mode:

Command	**Function**
Router(config-router)**# table-map** *route-map-name*	Configure the route map to be associated.

Use the **no table-map** command to remove the configuration.

To bring the configuration of the **table-map** command into effect immediately, run the **clear ip bgp** [vrf *vrf-name*] **table-map** command to update the core routing table. The **clear ip bgp** [vrf *vrf-name*] **table-map** command will not clear and then add the routes reflected in the core routing table. Instead, it directly applies the table-map to advertise route update messages without causing forwrding oscillation..

The **table-map** command supports the following rules-match, as-path/community/ip address/ip next-hop/metric/origin/route-type, set, metric/tag/next-hop.

Control the route redistribution from IBGP to IGP

The BGP protocol controls the redistribution of the routes learnded from the IBGP protocol to IGP protocol by the **bgp redistribute-internal** command. The routes learned from the EBGP protocol or confederation are allowed to be redistriubted to the IGP protocol.

To redistribute the route to the IGP protocol (inclding RIP/OSPF/ISIS), execute the followin command in the BGP configuraiton mode, IPv4/IPv6 address family configuration mode or IPv4 VRF address family configuraiton mode:

Command	Function
Router(config-router)# bgp-redistirbute-internal	Redistribute IBGP routes to the IGP protocol.

Use the **no bgp redistribute-internal** command to remove the configuration.

6.6 Configuring BGP Peer (Group) and Its Parameters

Since the BGP is an external gateway protocol (EGP), it is necessary for a BGP Speaker to know who is its peer (BGP Peer).

It is mentioned in the overview of the BGP protocol that two modes can be used to set up the connection relationship among BGP Speakers: IBGP (Internal BGP) and EBGP (External BGP). It will judge which connection mode will be established among BGP Speakers by the AS of BGP Peer and that of the BGP Speakers.

The BGP protocol supports IPv4 and IPv6. To check IPv6 function, verify whether the **address-family ipv6** command is executed in the BGP configuration mode. Otherwise, IPv6 is not supported. Note that you should activate neighbors in the corresponding address family.

In general, the BGP Speakers with EBGP connection should be physically connected. The BGP Speakers with IBGP connection, however, can be located in any place within an AS.

To configure the BGP peer, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **neighbor** {*address*|*peer-group-name*}	Configure the BGP peer. *address* indicates the IP addresses of

Command	Function
remote-as *as-number*	the BGP peer. *peer-group-name* indicates the name of the BGP peer group. The range of *as-number* is 1 to 65535.

Use the **no neighbor** {*address*|*peer-group-name*} to delete one peer or the peer group.

The BGP Speakers have some configuration in common (including the executed routing policy). To simplify configuration and improve efficiency, it is recommended to use the BGP peer group.

To configure the BGP peer group, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **neighbor** peer-group-name **peer-group**	(Optional) Create a BGP peer group.
DES-7200(config-router)# **neighbor** *address* **peer-group***peer-group-name*	(Optional) Set the BGP peer as the member of the BGP peer group.
DES-7200(config-router)# **neighbor** peer-group-name **remote-as** as-number	(Optional) Configure the BGP peer group. The range of *as-number* is 1 to 65535.

Use the **no neighbor** *address* **peer-group** to delete some member of the BGP peer group.

Use the **no neighbor** *peer-group-name* **peer-group** to delete the whole peer group.

Use the **no neighbor** *peer-group-name* **remote-as** to delete all members of the BGP peer group and the AS number of the peer group.

To configure the peer of the BGP Speakers or the optional parameter of the BGP peer group, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router-af)# **neighbor** {*address*|*peer-group-name*} **activate**	(Optional) Activate the address family of the neighbor so that the router can exchange routing information with the address family.
DES-7200(config-router)# **neighbor**	(Optional) Configure the network

Command	Function
{*address* | *peer-group-name*}**update-source** *interface*	interfaces to establish the BGP session with specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **ebgp-multihop** [*ttl*]	(Optional) Allow to establish the BGP session among non-direct-connected EBGP peer (group). The range of TTL is 1 to 255, the EBGP is 1 hop by default, and the IBGP is 255 hops by default.
DES-7200(config-router)# **neighbor**{*address* | *peer-group-name*} **password** *string*	(Optional) Enable the TCP MD5 authentication when the connection is established among specified BGP peer (group), and configure the password.
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **times** *keepalive holdtime*	(Optional) Configure the Keepalive and Holdtime value to establish the connection with the specified BGP peer (group). The range of the *keepalive* is 0 to 65535 seconds, 60 seconds by default. The range of the *holdtime* is 0 to 65535 seconds, 180 seconds by default.
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **advertisemet-interval** *seconds*	(Optional) Configure the minimal time interval to send the routing update message to the specified BGP peer (group). The range of advertisement-interval is 1 to 600 seconds, the IBGP peer is 15 seconds by default, and the EBGP peer is 30 seconds by default.
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **default-originate** [**route-map** *map-tag*]	(Optional) Configure to send the default route to the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **next-hop-self**	(Optional) Configure to set the next route information as this BGP speaker when the route is distributed to the specified BGP peer (group).

Command	Function
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **remove-private-as**	(Optional) Configure to delete the private AS number in the AS path attribute when distributing the route information to the EBGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*}**send-community**	(Optional) Configure to send the community attribute to the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **maximum-prefix** *maximum* [**warning-only**]	(Optional) Limit the number of the route information received from the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **distribute-list** *access-list-name* {**in** | **out**}	(Optional) Configure to implement the routing police according to the access control list when the route information is received from and sent to the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **prefix-list** *prefix-list-name* {**in** | **out**}	(Optional) Configure to implement the routing policy according to the prefix list when the route information is received from and sent to specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **route-map** *map-tag* {**in** | **out**}	(Optional) Configure to implement the routing policy according to the route-map when the route information is received from and sent to the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **filter-list** *path-list-name* {**in** | **out**}	(Optional) Configure to implement the routing policy according to the AS path list when the route information is received from and sent to the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **unsuppress-map** *map-tag*	(Optional) Configure to selectively advertise the route information suppressed by the **aggregate-address** command previously when it is distributed to the specified BGP peer.
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*}	(Optional) Restart the BGP session and reserve the unchanged route

Command	Function
soft-reconfiguration inbound	information sent by the BGP peer (group).
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **route-reflector-client**	(Optional) Configure this switch as the route reflector and specify its client.
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **shutdown**	(Optional) Disable the BGP peer (group).

Use the **no** mode of above commands to disable the configurations.

If one peer is not configured with the **remote-as**, each of its members can use the **neighbor remote-as** command to configure it independently.

By default, each member of the BGP peer group will inherit all its configurations. However, each member is allowed to configure the optional configurations which have no effect on the output update independently to replace the unified configuration of the BGP peer group.

Caution

Each member of the BGP peer group is allowed to configure the optional configurations which have no effect on the output update independently to replace the unified configuration of the BGP peer group. That is to say, each member of the BGP peer group will inherit the following configurations: **remote-as**、**update-source**、**local-as**、**reconnect-interval**、**times**、**advertisemet-interval**、**default-originate**、**next-hop-self**、**password remove-private-as**、**send-community**、**distribute-list out**、**filter-list out**、**prefix-list out**、**route-map out**、**unspress-map**、**route-reflector-client.**

The **neighbor update-source** command can be used to select any valid interface to establish the TCP connection. The key function of this command is to provide available Loopback interface, which makes the connection to the IBGP Speaker more stable.

By default, it is required to directly connect with BGP peers physically to establish the EBGP connection. To establish the EBGP peers among non-direct-connected external BGP Speakers, the **neighbor ebgp-multihop** command can be used.

Caution

To avoid route loop and oscillation, the EBGP peers who need multiple hops to establish BGP connection must have non-default routes to each other.

For the sake of the security, you can set the authentication for the BGP peers (group) which will establish the connection, the authentication uses the MD5 algorithm. The authentication password set for the BGP peer should be identical.

The process to enable the MD5 authentication on the BGP peer is shown as follows:

Command	Function
DES-7200(config-router)# **neighbor** {address | peer-group-name} **password** string	When the BGP connection with the BGP peer is established, use this command to enable the TCP MD5 authentication and set the password.

Use the **no neighbor** {*ip-address* | *peer-group-name*} **password** command to disable the MD5 authentication set for the BGP peer (group).

Use the **neighbor shutdown** command to disable the valid connection established with the BGP peer (group), and delete all route information related to the BGP peer (group).

Caution

To tear down the connection established with the specified BGP peer (group) and reserve the configuration information set for this specified BGP peer (group), use the **neighbor shutdown** command. If such configuration information is not required again, use the **no neighbor** [**peer-group**] command.

6.7 Configuring the Management Policy

Whenever the routing policy (including the **distribute-list**, **neighbor route-map**, **neighbor prefix-list and neighbor filter-list)** changes, you need to take effective measure to implement new routing policy. The traditional way is to tear down and then reestablish the BGP session.

This product supports implementing new routing policy without the close of the BGP session connection by the configuration of the soft reset for BGP effectively.

To facilitate the description of the BGP soft reset, the following will refer to the routing policy which has an effect on the input route information as the input routing policy (such as the **In-route-map** and **In-dist-list**), and that has an effect on the output route information as the output routing policy (such as the **Out-route-map** and **Out-dist-list**).

If the output routing policy changes, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **clear ip bgp** {* | neighbor *address* | peer-group *peer-group-name* | **external} soft out**	Do soft reset of the BGP session and execute the routing policy without resetting up the BGP session.

If the input routing policy changes, its operation will be more complicated than

that of the output routing policy, because the implementation of the output routing policy is based on the routing table of this BGP Speaker. The implement of the input routing policy is based on the route information received from the BGP peer. To reduce the memory consumption, the local BGP Speaker will not remain the original route information received from BGP peers.

If it is necessary to modify the input routing policy, the common method is to save the original route information for each specified BGP peer in this BGP Speaker by the **neighbor soft-reconfiguration inbound** command, so as to provide the original foundation of the route information to modify the input routing policy in future.

At present, there is a standard implementation method referred to as the Route Refresh Performance, which can support modifying the routing policy without the storage of the original route information. This product supports the route refreshing performance.

If the input routing policy changes, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **neighbor** {address | peer-group-name} soft-reconfiguration inbound	(Optional) Restart the BGP session and reserve the unchanged route information sent by the BGP peer (group). Execution of this command will consume more memory. If both parties support the route refreshing performance, it is not necessary to execute this command.
DES-7200(config-router)# **clear ip bgp** {***** | *neighbor-address* | **peer-group** *peer-group-name* | **external**} **soft in**	Do soft reset of the BGP session and execute the routing policy without resetting up the BGP session.

You can judge whether the BGP peer supports the route refreshing performance by the **show ip bgp neighbors** command. If so, you need to execute the **neighbor soft-reconfiguration inbound** command when the input routing policy changes.

6.8 Configuring Synchronization between BGP and IGP

The routing information can be transmitted to another AS through the local AS only when ,it will pass through this AS and reach anther AS, the route information will be advertised to ll the routers in the local AS have learned the routing

information. Otherwise, if some routers running the IGP protocol within this AS have not learn about this route information, the data packets may be discarded for these routers don't know this route when these packets traverses through this AS, namely, it will cause the route black hole.

The BGP-IGP synchronization is designed to ensure all routers within this AS can learn the outbounding route information. A simple way is that the BGP Speakers redistribute all of the routes learned by the BGP protocol to the IGP protocol, guaranteeing that the routers within the AS learn such route information.

The BGP-IGP synchronization mechanism can be cancelled under two conditions:

1. There is no the route information which pass through the local AS (In general, this AS is an end AS).
2. All routers within this AS operate the BGP protocol and the full connection relationship is established among all BGP Speakers (The adjacent relationship is established between any two BGP Speakers).

Caution

By default, the synchronization is disabled. Enable synchronization when not all the routers are running BGP when traversing an AS.

To enable synchronization of BGP speakers, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **synchronization**	(Optional) Enable synchronization of BGP and IGP.

Execute the **no synchronization** command to disable the synchronization mechanism.

6.9 Configuring Interaction between BGP and IGP

To inject the route information generated by the IGP protocol into the BGP protocol, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **redistribute** [**connected** | **rip** | **static**] [**route-map** *map-tag*] [**metric** *metric-value*]	(Optional) Redistribute static route, direct route and the route information generated by RIP.
DES-7200(config-router)# redistribute ospf *process-id* [route-map *map-tag*]	(Optional) Redistribute the route information generated by OSPF.

Command	Function
[metric *metric-value*] [match internal external [1 | 2] nssa-external [1 |2]]	
DES-7200(config-router)# **redistribute is is** [*isis-tag*] [**route-map** *map-tag*] [**metric** *metric-value*] [level-1| level-1-2| level-2]	(Optional) Redistribute the route information generated by ISIS.

By default, distribution of default route is disabled. To enable this function, execute the following commands:

Command	Function
DES-7200(config-router)# default-information originate	(Optional) Redistribute default route.

6.10 Configuring BGP Timer

The BGP uses the Kepalive timer to maintain the effective connection with the peers, and takes the Hldtime timer to judge whether the peers are effective. By default, the value of the Kepalive timer is 60s, and the value of the Holdtime timer is 180s. When the BGP session is established between BGP Speakers, both parties will negotiate with the Holdtime timer and that with smaller value will be selected. While, the selection of the Keepalive timer is based on the smaller one between 1/3 of the negotiated Holdtime timer and the configured Keepalive timer.

To adjust the value of the BGP timer based on all peers, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **timers bgp** keepalive holdtime	(Optional) Adjust the keepalive and holdtime value of BGP based on all peers. The range of the *keepalive* is 0 to 65535 seconds, and 60 seconds by default. The range of the *holdtime* is 0 to 65535 seconds, 180 seconds by default.

Certainly, you can adjust the value of the BGP timer based on the specified peers, and execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **neighbor** {address | peer-group-name} **times** keepalive holdtime	(Optional) Configure the Keepalive and Holdtime value to establish a session with the specified BGP peer (group). The range of the keepalive is 0 to 65535 seconds, 60 seconds by default. The range of the holdtime is 0 to 65535 seconds, 180 seconds by default.

Use the **no** option of corresponding commands to clear the value of configured timer.

6.11 Configuring BGP Path Attributes

6.11.1 AS_PATH Attribute

The BGP protocol controls the distribution of the route information in three ways:

- IP address by using the neighbor distribute-list and neighbor prefix-list commands
- AS_PATH Attribute(refer to the description in this section)
- COMMUNITY Attribute(refer to the COMMUNITY Attribute configuration)

You can use the AS path-based access control list to control the distribution of the route information, where the AS path-based ACL will use Regular Expression to resolute the AS path.

To configure the AS path-based distribution of the route information, execute the following operations in the privileged mode:

Command	Function
DES-7200# configure terminal	Enter into the global configuration mode.
DES-7200(config)# **ip as-path** access-list *path-list-name* {permit | **deny**} as-regular-expression	(Optional) Define an AS path list.
DES-7200(config)# **ip routing**	Enable the routing function (if disabled)
DES-7200(config)# **router bgp**	Enable the BGP and configure this

Command	Function
as-number	AS number to enter into the BGP configuration mode.
DES-7200(config-router)# **neighbor** {address | peer-group-name} **filter-list** *path-list-name* {**in** | **out**}	(Optional) Implement the routing policy according to the AS path list when the route information is received from and sent to the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {address | peer-group-name} route-map *map-tag* {in | out}	(Optional) Implement the routing policy according to the route-map when the route information is received from and sent to the specified BGP peer (group). In the route-map configuration mode, you can use the **match as-path** to operate the AS path attribute by the AS path list, or take the **set as-path** to operate the AS attribute value directly.

The BGP protocol will not take the length of the AS path into account when it selects the optimal path as specified in RFC1771. In general, the shorter the length of the AS path, the higher the path priority is. Hence, we take the length of the AS path when we select the optimal path. You can determine whether it is necessary to take the length of the AS path into account when you select the optimal path according to the actual condition.

If you don't want take the length of the AS path into account when you select the optimal path, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp bestpath** as-path ignore	(Optional) Compare with the length of the AS path when selecting the optimal path.

Caution

Within the AS, whether all BGP Speakers take the length of the AS path into account will be consistent when selecting the optimal path. Otherwise, the optimal path information selected by various BGP Speakers will be different.

6.11.2 NEXT_HOP Attribute

To set the next hop as the local BGP Speaker for sending the route information to the specified BGP peer, you can use the **neighbor next-hop-self** command, which is mainly used in the non-mesh networks (such as frame relay and X.25). Execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **neighbor** {address | peer-group-name} next-hop-self	(Optional) Set the next hop as the local BGP speaker for distributing the route information to the specified BGP peer (group).

You can also modify the next hop of the specified path by the **set next-hop** command of Route-map.

Caution

This command is not recommended to use under the full mesh network environment (such as Ethernet) for it will cause additional hops and incur unnecessary overhead.

6.11.3 MULTI_EXIT_DISC Attribute Configuration

The BGP takes the MED value as the foundation of priority comparision of the paths learned from the EBGP Peers. The smaller the MED value, the higher the priority of the path is.

By default, it will only compare with the MED value for the path of the peers from the same AS when the optimal path is selected. If you hope to compare with the MED value for the path of the peers from different ASs, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp** always-compare-med	(Optional) Compare with the MED value for the path of different ASs.

By default, it will not compare with the MED value for the path of the peers for other ASs within the AS association when the optimal path is selected. If you hope to compare with the MED value for the path of the peers from different AS confederations, execute the following operations in the BGP :configuration mode

Command	Function
DES-7200(config-router)# **bgp bestpath** med confed	(Optional) Compare with the MED value for the path of the peers from other ASs within the confederation.

By default, if the path whose MED attribute is not set is received, the MED value of this path will be taken as 0. For the smaller the MED value, the higher the priority of the path is, the MED value of this path reaches the highest priority. If you hope the MED attribute for the path whose MED attribute is not set presents the lowest priority, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp bestpath** med missing-as-worst	(Optional) Set the priority of the path whose MED attribute is not set as the lowest.

By default, they will be compared with each other according to the sequence the paths are received when the optimal path is selected. If you hope to compare with the path of the peers from the same AS firstly, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp** deterministic-med	(Optional) Compare with the path of the peers from the same AS firstly. By default, they will be compared with by the received sequence, the later received path will be compared with firstly.

6.11.4 LOCAL_PREF Attribute Configuration

The BGP takes the LOCAL_PREF as the foundation of priority comparision of the path learned from the IBGP peers. The larger the LOCAL_PREF value, the higher the priority of the path is.

The BGP Speakers will add the local preference when they send the received external routes to the IBGP peers. To modify the local preference, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp default** local-preference *value*	(Optional) Change the default local preference. The range of the value is 0 to 4294967295, 100 by default.

You can also modify the local preference of the specified path by the **set local-preference** command of Route-map.

6.11.5 COMMUNITY Attribute Configuration

COMMUNITY Attribute is another method to control the distribution of the route information.

The community is a set of destinations. The purpose is to implement the community-based routing policy so as to simplify the configuration to control the distribution of the route information in the BGP Speakers.

Each destination may be of more than one community, and the manager of the AS can define which community the destination is of.

By default, all destinations are of the Internet community carried in the community attribute of the path.

At present, total for four common community attribute values are predefined:

- **Internet**: Indicate the Internet community, and all paths are of this community.
- **no-export**: Indicate this path will not be exported to the BGP peers.
- **no-export**: Indicate this path will not be advertised to the BGP peers.
- **local-as**: Indicate this path will be advertised only in the local AS or the AS confederation if it is configured.

You can control the receiving, priority and distribution of the route information by the community attribute.

The BGP supports up to 32 COMMUNITY attributes for every route. When configuring the **route-map** command, you can set up to 32 COMMUNITY attributes for the parameters **match** and **set COMMUNITY.**

The BGP Speakers can set, add or modify the community attribute value when they learn about, issue or redistribute the route. The aggregated path includes the community attribute of all aggregated paths when the route aggregate is carried out.

To configure the community attribute-based distribution of the route information, execute the following operations in the privileged mode:

Command	Function
DES-7200# configure terminal	Enter into the global configuration mode.
DES-7200(config)# **ip community-list standard** *community-list-name* {**permit** | **deny**} *community-number*	(Optional) Create the community list. The *community-list-name* is the name of the community list. The community-number is the

Command	Function
	concrete value of the community list in the range 1 to 4,294,967,200, or the well-known community attribute such as **Internet**, **local-AS**, **no-advertise** and **no-export**.
DES-7200(config)# **ip routing**	Enable the routing function (if disabled).
DES-7200(config)# **router bgp** *as-number*	Enable the BGP and configure this AS number to enter into the BGP configuration mode.
DES-7200(config-router)# **neighbor** {address | peer-group-name} send-community	(Optional) Configure to send the community attribute to the specified BGP peer (group).
DES-7200(config-router)# **neighbor** {address | peer-group-name} route-map *map-tag* {in | out}	(Optional) Configure to implement the routing policy according to the route-map when the route information is received from and sent to the specified BGP peer (group). In the route-map configuration mode, you can use the **match community-list [exact]** and **set community-list delete** to operate the community attribute by the community list, or take the **set community** command to operate the community attribute value directly.

6.11.6 Other Related Configuration

By default, if two paths with full identical path attributes are received from different EBGP peers during the selection of the optimal path, we will select the optimal path according to the path received sequence. You can select the path with smaller router ID as the optimal path by configuring the following commands.

Command	Function
DES-7200(config-router)# **bgp bestpath** compare-routerid	(Optional) Allow the BGP to compare with the router ID when the optimal path is selected.

6.12 Selecting the Optimal Path for BGP

The selection of the optimal route is an important part of the BGP protocol. The following will describe the selection process of the BGP route protocol in details:

1. Discard the unreachable Next-hop route.
2. Select the route with the maximal weight.
3. Select the route with the high LOCAL_PREF attribute value.
4. Select the route generated by the local BGP speaker.
5. The route generated by the local BGP speaker includes the one generated by the **neighbor default-originate, network, redistribute, aggregate** command.
6. Select the route with the shortest AS length.
7. Select the route with the lowest ORIGIN attribute value.
8. Select the route with the smallest MED value.
9. The priority of the EBGP path is higher than that of the route of the IBGP path and the AS
10. confederation, and the priority of the IBGP path and the AS confederation is identical.
11. Select the route with the smallest IGP metric to reach the next hop.
12. Select the route received comparativelly earlier from the EBGP routes.
13. Select the route which advertises that the router ID of the BGP speaker is small.
14. Select the route with the great cluster length.
15. Select the route: the value of neighbor address for which is high.

Caution

Above is the process of select the optimum route under the default configuration. You can change the selection process of the route by the CLI command. For instance, you can use the **bgp bestpath as-path ignore** command to make the step 5 in the process of selecting the optimum route invalid.

6.13 Configuring BGP Route Aggregation

Since the BGP-4 supports CIDR, aggregated entries are allowed to create to reduce the size of the BGP routing table. Certainly, only when there is valid path within the aggregation scope can the BGP aggregated entries be added to the

BGP routing table.

To configure the BGP route aggregation, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **aggregate-address** address mask	(Optional) Configure the aggregated address.
DES-7200(config-router)# **aggregate-address** address mask **as-set**	(Optional) Configure the aggregated address, and remain the AS path information of the path within the scope of the aggregated address.
DES-7200(config-router)# **aggregate-address** address mask **summary-only**	(Optional) Configure the aggregated address and only advertise the aggregated path.
DES-7200(config-router)# **aggregate-address** *address mask* as-set summary-only	(Optional) Configure the aggregated address, and remain the AS path information of the path within the scope of the aggregated address. At the same time, only the aggregated path is advertised.

Use the **no** mode of above commands to disable the configured content.

Caution

By default, the BGP will advertise all route information both before and after aggregation. If you want to advertise only the aggregated path information, use the **aggregate-address summary-only** command.

6.14 Configuring Route Reflector for BGP

To speed up the convergence of the route information, all BGP Speakers within one AS will usually establish the full connection relationship (The adjacent relationship is established between any two BGP Speakers). Too many BGP Speakers within the AS will increase the resource overhead of the BGP Speakers, raise the configuration workload and complexity of network administrators and reduce the network scalability.

For this reason, two measures such as the route reflector and AS confederation are proposed to reduce the connections of the IBGP peers within an AS.

The route reflector is a measure to reduce the connections of the IBGP peer within the AS. One BGP Speaker is set as the route reflector, which divides the

IBGP peer within this AS into two types, such as client and non-client.

The rule to implement the route reflector within the AS is shown as follows:

- Configure the route reflector and specify its client, so the route reflector and other clients form a cluster. The route reflector establishes the connection relationship with clients.
- The clients of the route reflector within one cluster should not establish the connection relationship with other BGP Speakers of other clusters.
- Within an AS, the full connection relationship is established among the IBGP peer of non-clients. Where, the IBGP peer of non-clients includes the following conditions: among several route reflectors within one cluster, among the route reflector within the cluster and the BGP Speakers which don't participate in the route reflector function out of the cluster (In general, the BGP Speakers don't support the route reflector function), among the route reflector within the cluster and the route reflector of other cluster.

The processing rule when the route reflector receives one route is shown as follows:

- The route update received from the EBGP Speaker will be sent to all clients and non-clients.
- The route update received from the clients will be sent to other clients and all non-clients.
- The route update received from the IBGP non-clients will be sent to all its clients.

To configure the BGP route reflector, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **neighbor** {*address* | *peer-group-name*} **route-reflector-client**	(Optional) Configure this product as the route reflector and specify its clients.

In general, one group is only configured with one route reflector. In this case, the Router ID of the route reflector can be used to identify this cluster. To increase the redundancy, you can set more than one route reflector within this cluster. In this case, you must configure the cluster ID, so that one route reflector can identify the route update from other route reflectors of this cluster.

Caution

To set several route reflectors for one cluster, it is necessary for you to configure a cluster ID for this cluster.

To configure the cluster ID of the BGP, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp cluster-id** cluster-id	(Optional) Configure the cluster ID of the route reflector.

In general, it is not necessary to establish the connection relationship between the clients of the route reflector within the cluster, and the route reflector will reflect the routes among clients. However, if the full connection relationship is established among all clients, this function can be disabled.

To disable the function of reflecting the routes of the client, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **no bgp** client-to-client reflection	(Optional) Disable route reflection on clients.

6.15 Configuring Route Flap Dampening for BGP

Route flap means a route changes between the valid status and the invalid status. The route flap usually causes instable routes to be transmitted on the Internet, and thus a instable network. The BGP route flap dampening is a measure to reduce route flap by monitoring the route information of EBGP peers.

The route flap dampening of BGP uses the following glossaries:

- Route Flap: A route changes between the valid status and the invalid status.
- Penalty: The route flap dampening-enabled BGP Speakers will add a penalty for the route every time when a route flaps. The penalty will be accumulated to exceed the suppress limit.
- Suppress Limit: When the penalty of a route exceeds this value, the route will be suppressed.
- Half-life-time: The time elapsed when the penalty is reduced to half of its value.
- Reuse Limit: When the penalty of the route is lower than this value, the route suppression is released.
- Max-suppress-time: The maximal time the route can be suppressed.

Brief description of route flap dampening: The BGP Speakers will add a penalty for the route every time when a route flaps. The penalty is accumulated. Once the

penalty value reaches the suppress limit, the route will be suppressed. When the half-life-time reaches, the penalty value is reduced to half of its value. Once the penalty value is reduced to the reuse limit, the route will be activated again. A route can be suppressed for the maximal suppress time.

To configure the route flap dampening of the BGP, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp dampening**	Enable the route flap dampening of the BGP protocol.
DES-7200(config-router)# **bgp dampening** half-life-time reuse suppress max-suppress-time	(Optional) Configure the parameters of the route flap dampening. half-life-time: in the range 1 to 45minutes, 15minutes by default. reuse: in the range 1 to 20000, 750 by default. suppress: in the range 1 to 20000, 2000 by default. max-suppress-time: in the range 1 to 255 minutes, 4*half-life-time by default.

If it is necessary to monitor the route flap dampening information, execute the following operations in the privileged mode:

Command	Function
DES-7200# show ip bgp dampening **flap-statistics**	Show the flap statistics information of all router.
DES-7200# show ip bgp dampening dampened-paths	Show the dampened statistics information.

To clear the route flap dampening information or clear the dampened routes, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200# clear ip bgp flap-statistics	Clear the flap statistics information of all un-dampened route.
DES-7200# clear ip bgp flap-statistics address mask	Clear the flap statistics information of the specified route (excluding the dampened routes).
DES-7200# clear ip bgp dampening	Clear the flap statistics information

Command	Function
[address mask]	of all routes, and release the suppressed routes.

6.16 Configuring AS Confederation for BGP

The confederation is a measure to reduce the connections of the IBGP peer within the AS.

One AS is divided into multiple sub ASs that can form a confederation by setting a unified confederation ID (namely, confederation AS number). An external confederation is still considered to be an AS and only the AS number of the confederation is visible. Within the confederation, the full IBGP peer connection is still established among the BGP Speakers and the EBGP connection is established among the BGP Speakers within the sub AS. Although the EBGP connection is established among BGP Speakers within the sub ASs, the path attribute information of NEXT_HOP, MED and LOCAL_PREF retains intact when the information is exchanged.

To implement the AS confederation, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **bgp** confederation identifier *as-number*	Configure the AS confederation number. The range of *as-number* is 1 to 65535.
DES-7200(config-router)# **bgp** confederation peers *as-numbe* [as-number..]	Configure other sub AS numbers within the AS confederation. The range of *as-number* is 1 to 65535.

Use the **no** mode of above commands to disable the configured content.

6.17 Configuring BGP Management Distance

The management distance indicates the reliability of the route information resource, whose range is 1 to 255. The larger the value of the management distance, the lower the reliability is.

The BGP sets different management distances for various information sources learned, such as External-distance, Internal-distance and Local-distance.

- **External-distance:** The management distance of the route learned from the EBGP peers.

- **Internal-distance:** The management distance of the route learned from the IBGP peers.
- **Local-distance:** The management distance of the route learned from the peers. However, it is considered that the optimal one can be learned from the IGP. In general, these routes are indicated by the **Network Backdoor** command.

To modify the management distance of the BGP protocol, execute the following operations in the BGP configuration mode:

Command	Function
DES-7200(config-router)# **distance bgp** *external-distance internal-distance* local-distance	(Optional) Configure the management distance. The range of the distance is 1 to 255. For the default configuration: *external-distance 20* *internal-distance 200* local-distance 200

Use the **no** command to restore the default management distance of the BGP protocol.

Caution

It is not recommended to change the management distance of the BGP route. If it is necessary to change, please keep it in mind that:

1. The External-distance should be lower than the management distance of other IGP route protocol (OSPF and RIP).
2. The Internal-distance and Local-distance should be higher than the management distance of other IGP route protocol.

6.18 Configuring BGP Route Update Mechanism

The BGP route update mechanism includes two parts: timing scanning update and event trigger update. The former means that the timer is used in the BGP to start the scanning mechanism periodically to update the routing table. The latter means that when BGP configuration or the next hop of BGP route changes, the BGP protocol starts the scanning mechanism to update the routing table..

To configure the BGP route update mechanism, execute the following operations in the BGP configuration mode:

Command	Function

Command	Function
DES-7200(config-router)# **bgp scan-rib disable**	Enable the event trigger mechanism. By default, the timing scanning update mechanism is used.
DES-7200(config-router)# **bgp scan-time** *scan-time*	(Optional) Set the scanning interval. *scan-time*: In the range 5 to 60 seconds, 60 seconds by default

You can also configure this command in IPv4/IPv6/VPNv4/VPNv6 address family mode.

Use the **no** command to remove the configuration.

Caution

When you run the **bgp scan-rib disable** command to enable the event trigger mechanism, the synchronization should be disabled and the BGP next hop trigger mechanism should be enabled. Meanwhile, when the synchronization is enabled or the BGP next hop trigger mechanism is disabled, the BGP updates the routing table in timing scanning way.

6.19 Configuring BGP Nexthop Trigger Update Mechanism

The BGP next hop trigger update mechansim improves the converge of BGP routes. It monitors the monitroing of the next hop of BGP routes to speed up converge in stable network topology.

By default, the BGP next hop trigger update mechansim is enabled. After establishing connections with neighbors, the BGP will automatically monitor the next hop of the routes learned from neighbors. When the next hop changes, the BGP will receive a notification to update the routing tble. This can reduce the time to check the change of next hop for better converge of BGP routes.

To configure the BGP next hop trigger update mechanism, execute the following operations in the BGP configuration mode:

Command	**Function**
DES-7200(config-router)# no bgp nexthop trigger enable	Disabled the BGP next hop trigger update.
DES-7200(config-router)# **bgp nexthop trigger delay** *delay-time*	(Optional) Set the delay of the BGP next hop trigger update. *delay-time*: In the range 0 to 100 seconds, 5 seconds by default

You can also configure this command in IPv4/IPv6/VPNv4/VPNv6 address family

mode.

Use the **bgp nexthop trigger enable** command to restore the setting to the default value.

The **bgp nexthop trigger enable** command and the **bgp scan-time** command control the same timer. When the timing scanning mechanism is enabled, the time of larger than 60 seconds set by the the **bgp nexthop trigger enable** command does not take effect because the timing scanning mechanism is always activated before the delay time.

Caution

In an unstable network (the next hop changes frequently), especially there are a lot number of routes, this function carries out unnecessary route calculation and thus aggravates consumption of CPU resource. In this case, it is recommended to disable the BGP next hop trigger update mechanism.

6.20 Configuring BGP GR

GR (Graceful Restart) can ensure continous data forwarding duing the reset of the BGP protocol.

6.20.1 Working Mechanism of GR

1 Standard

RFC4724: Graceful Restart Mechanism for BGP, which is represented by BGP GR later.

2 Working mechanism

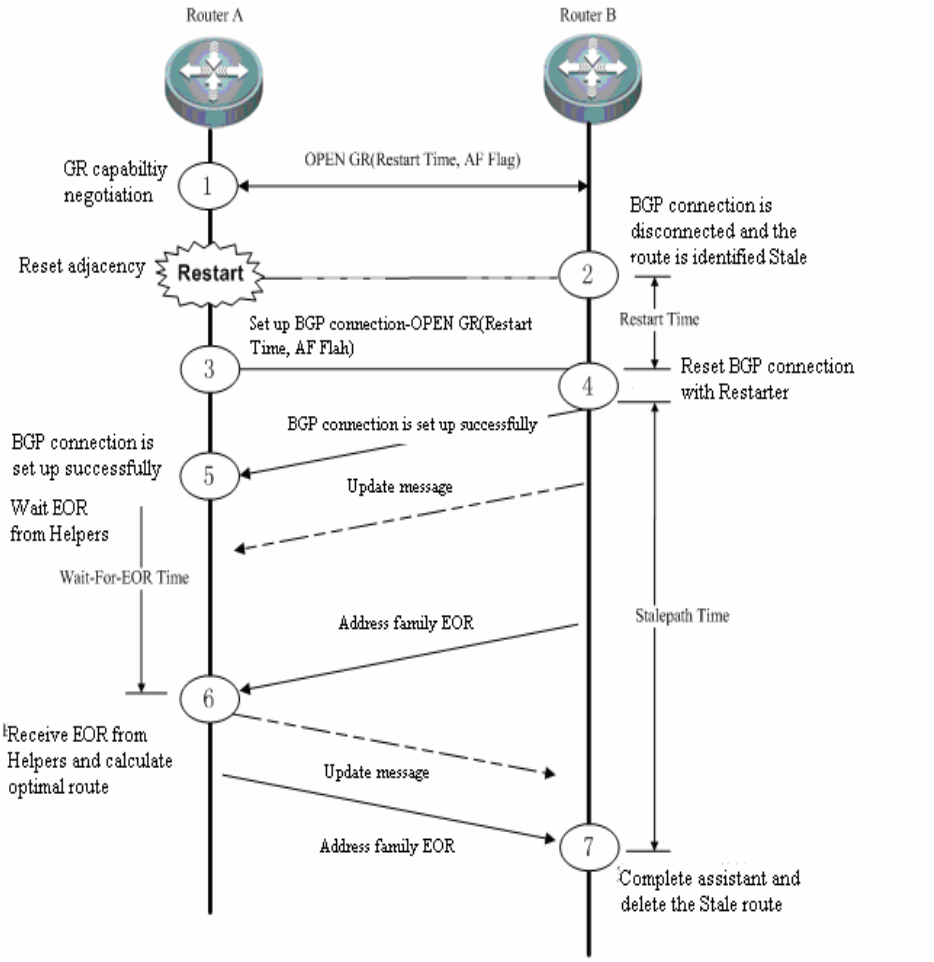
RFC4724 is a standard GR protocol that IETF especially defines for the BGP protocol. This document outlines the principles of BGP GR, including:

Graceful Restart Capability is added to the OPEN message of the BGP protocol, indicating that the BGP supports GR. The GR capability is negotiated by neighbors during the initiation of BGP connection.

GR Restarter and GR Helper. GR Restarter refers to the router restarting the BGP protocol, which can ensure continuous route forwarding when the route control panel fails. GR Helper is the BGP neighbor of the GR Restarter that assists the GR Restarter to do BGP GR for continous forwarding in the overall network.

In the update message, EOR (End-of-RIB) is added to indicate that the route message update is completed.

The following ffigure illustrates the process of BGR GR.



Initially, the BGP protocol establishes the neighbor relationship and negotiates respective GR capability with the GR Capability field of the OPEN message. At a point, the device reboots and the BGP session is disconnected. The neighbor detects disconnection. With GR supported, the BGP neighbor keeps the route of the GR Restarter valid but identifies it Stale. The GR Restarter reboots and reestablish connection with the GR Helper and waits the route update message and EOR label from the GR Helper. After receiving the EOR label from all neighbors, the BGP Restarter calculates routes and update the routing table, and begins to send update routes to the GR Restarter. Upon the receipt of these routes, the GR Helper removes the Stale tag from these routes. Then it deletes the routes tagged with Stale after receiving the EOR label from the BGP Restarter, calculates routes and updates the routing table.

Some key timers are defined to assist the implemetation of BGP GR:

Restart-Timer: The GR Restarter notifies the GR Helper of restart time that the GR Helper needs to wait before reestablishing the BGP connection. You can modify this value by the **bgp graceful-restart restart-time** command.

Wait-For-EOR Timer: Time the GR Restarter needs to wait for the EOR label of all GR Helpers. After receiving the EOR label of all GR Helpers or the timer times out, the GR Restarter calculates optimal routes and updates the routing table.

You can modify this value by the **bgp update-delay** command.

StalePath Timer: Time the GR Helper needs to wait before receiving the EOR label from the GR Restarter after reestablishing the connection with the GR Restarter. During this period, the GT Helper keeps the route of the GR Restarter valid. It will delete the rotue tagged with Stale after receiving the EOR lable or the StalePath timer is expired. You can modify this value by the **bgp graceful-restart stalepath-time** command.

6.20.2 Implementation of BGP GR

Implementation of BGP GR is not an independent process. All BGP peers are necessary to enable BGP GR capability for normal operation. Failed GR may cause temporary route black hole or loop and affect the network operation. Consequently, it is recommended to ensure the GR capability is negotiatied successfully by the **show ip bgp neighbors** command.

To enable BGP GR, exeucte the **bgp graceful-restart** command in the BGP route configuration mode.

6.20.3 Configuring BGP GR Capability

BGP GR capability is an extended capability of the BGP protocol, which is disabled by default. When enabling GR, the BGP reestablishes the connection with its neighbor and negotiates GR capability. The GR is enabled only when both sides support GR capability.

To enable the GR capability, execute the following commands:

Command	Function
DES-7200 # configure terminal	Enter the global configuration mode.
DES-7200(config)# **router bgp** *500*	Enter the BGP configuration mode.
DES-7200(config-router)# **bgp graceful-restart**	Enable GR.
DES-7200(config-router)# **end**	Exit to the privileged mode.
DES-7200 # show running-config	Show the configuration.
DES-7200 # **write**	(Optional) Save the configuration.

All the products supporting BGP support this command.

Caution

The **bgp graceful-restart** command does not take effect for established BGP connection. Namely, the BGP connect will not negotiate GR capability immediately when it is in Established status. In this case, you need to forcibly restart the peer to negotiate the GR capability again, for instance, **clear ip bgp 192.168.195.64**. This avoids network oscillation caused by reestablishing neighbor relationship.

Caution

Supporting BGP GR capability does not mean a device can serve as the GR Restarter for graceful restart, which also depends on the hardware of the device. The GR Restarter device needs to support dual-engine redundant hot backup.

6.20.4 Configuring BGP GR Timer

After enabling the GR capability, the BGP automatically configures relevant timers with default values. By default, the Restart Timer is 120s, the Wait-For-EOR Timer is 120s and the StalePath Timer is 360s.

To cofnigure these timers, execute the following commands:

Command	Function
DES-7200 # configure terminal	Enter the global configuration mode.
DES-7200(config)# **router bgp** *500*	Enter the BGP configuration mode.
DES-7200(config-router)# **bgp graceful-restart**	Enable GR capability.
DES-7200(config-router)# bgp graceful-restart restart-time *150*	Set the Restart Timer to 150s.
DES-7200(config-router)# **bgp update-delay** *150*	Set the Wait-For-EOR Timer to 150s.
DES-7200(config-router)# bgp graceful-restart stalepath-time *400*	Set the StalePath Timer to 400s.
DES-7200(config-router)# **end**	Exit to the privileged mode.
DES-7200 # show running-config	Show the configuration.
DES-7200 # **write**	(Optional) Save the configuration.

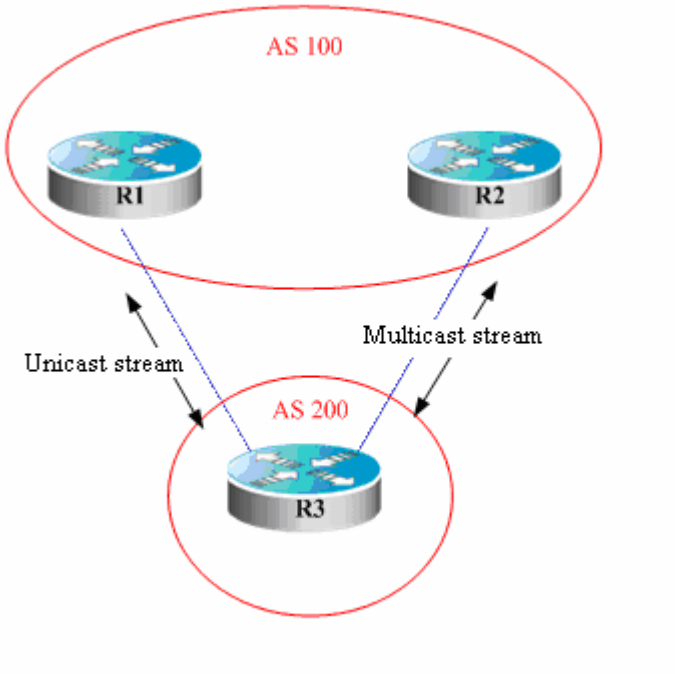
All the products supporting BGP support this command.

Caution

The restart time configured by the **bgp graceful-restart restart-time** command should be no more than the Hold time of the BGP peer, or otherwise the Hold Time will be used as the restart time and be notified to the peer for GR capability negotiation.

6.21 Configuring BGP Multicast

The BGP multicast route is used for multicast RFC check. In general, the multicast forwarding topology can be similar to the unicast forwarding topology. You can design different multicast topology by using BGP multicast, which is used for multicast topology between ASs, as shown in the following figure.



There are two routers in AS100. In design, unicast streams are sent to R1 and multicast streams are sent to R2. In this case, MPBGP is necessary between R2 and R3.

Step 1: Enable BGP on R1, R2 and R3 and establish neighbor relationships among them.

Take R3 as an example. Configure R1 and R2 as its BGP neighbors.

Command	Function
DES-7200 # configure terminal	Enter the global configuration mode.
DES-7200(config)# **router bgp** *200*	Enter the BGP configuration mode with the AS number of 200.

Command	Function
DES-7200(config-router)# **neighbor** *R2* **remote-as** *100*	Configure R2 as the BGP neighbor with the AS number of 100.
DES-7200(config-router)# **neighbor** *R1* **remote-as** *100*	Configure R1 as the BGP neighbor with the AS number of 100.

Step 2: Since R3 does not need to transmit multicst route with R1, disable the multicast address of R1.

Command	Function
DES-7200(config-router)# address-family ipv4 multicast	Enter the IPv4 multicast address family configuration mode.
DES-7200(config-router)# **no neighbor** *R1* **active**	Disable the multicast address of R1.

Step 3: Since R2 needs to transmit multicast rotue with R1, enable the multicast address of R2.

Command	Function
DES-7200(config-router)# address-family ipv4 multicast	Enter the IPv4 multicast address family configuration mode.
DES-7200(config-router)# **neighbor** *R2* **active**	Enable the multicast address of R2.

Step 4: Import the routes that R3 needs to advertise to R2 in the multicast address family mode.

Command	Function
DES-7200(config-router)# address-family ipv4 multicast	Enter the IPv4 multicast address family configuration mode.
DES-7200(config-router-af)# **redistribute ospf** 1	Redistribute OSPF routes.

Caution

During redistribution, the routes imported are unicast routes. For instance, the **redistribute ospf 1** command imports OSPF unicast routes. This is because that multicast routes actually depend on the egress of unicast routes for the establishment of multicast spanning tree.

6.22 Configuring BGP Local AS

This function configures a local AS different from the real AS (rotuer BGP AS) for

one peer, which equals to virtualizing an AS . when the real AS changes, you still can establish BGP connection without modifying the BGP cofniguration of the peer. Local AS applies to AS migration and converge of large networks without influencing the configurations of the devices in other interconenected ASs.

When establishing the BGP connection, the local device will advertise local AS number to the peer in the OPEN message. The peer checks whether the AS number matches the locally configured one and refuses the BGP connection if there is a difference. By default, the local AS of the BGP connection is the real BGP AS. With this function, the local device replaces the real AS with the configured one to establish the BGP connection.

To configure local AS for one peer, execute the following commands:

Command	Function
DES-7200 # configure terminal	Enter the global configuration mode.
DES-7200(config)# **router bgp** *500*	Enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *192.168.195.64* **remote-as** *100*	Configure the peer.
DES-7200(config-router)# **neighbor** *192.168.195.64* **local-as** *300*	Configure AS 300 as the local AS for the peer

The local AS function applies to only EBGP peers, not IBGP peers, confederation EBGP peers. Meanwhile, there are some limits as below:

- The local AS cannot be configured as the remote as of the peer.
- Local AS cannot be configured for one member of the peer group.
- The local AS cannot be configured as the real BGP AS.
- The local AS cannot be configured as the AS number of the confederation if the device is the member of one confederation.

For details of the **neighbor** *peer-address* **local-as** *as-num* command, refer to *Command Reference*.

6.23 BGP 4-Octet AS Configuration

The traditional AS number consists of two octets within the range of 1-65535. The AS number defined by RFC4893 consists of 4 octets falling within the range of 1-4294967295, so as to address the problem of limited AS number resource. According RFC5396, 4-octet AS number supports two representation formats: asplain and asdot+. The asplain (decimal) representation is the same as the former representation format, namely the 4-octet AS number will be represented using decimal value. The asdot+ representation is featured by ([high order 2 octets.] low order 2 octets). The high order 2 octets won't be displayed if the value

is 0, namely the AS number of 65536 in asplain format will be represented as 1.0 in asdot+ format. Also, the AS number of 65534 in asplain format will be represented as 65534 in asdot+ format (without displaying the 0 value).

6.23.1 Working principle

With the introduction of 4-octet AS number, there comes the problem of establishing BGP connection between an old bgp speaker supporting only 2-octet AS number and a new bgp speaker supporting 4-octet AS number. If the autonomous system to which the new bgp speaker belongs uses 4-octet AS number, then the old bgp speaker shall use the reserved AS number of 23456 to replace the 4-octet AS number of new bgp speaker while creating the neighbor. In the packets sent from new bgp speaker to old bgp speaker, 23456 will also be used to replace the 4-octet AS number in the domain of "My Autonomous System". Meanwhile, in the UPDAT packets sent to old bgp speaker, 23456 will also be used to replace the 4-octet AS number existing in AS-PATH and AGGREGATOR attributes; such packets will also carry the true 4-octet AS number preserved in the optional transitive attributes of AS4-PATH and AS4-AGGREGATOR, so that the true AS-PATH attribute and AGGREGATOR attribute can be restored when this route arrives at the next new bgp speaker.

In other cases, the true AS number of peer side is directly used to create neighbor.

6.23.2 Protocol specification

RFC 4893

RFC 5396

6.23.3 Configuring BGP instance with 4-octet AS number

By default, BGP protocol is not enabled. After enabling BGP protocol, the decimal value is by default used to represent 4-octet AS number.

Command	Function
DES-7200 # **configure terminal**	Enter global configuration mode
DES-7200(config)# **router bgp 65538**	Enable BGP protocol and configure device AS number as 65538
DES-7200(config)# **router bgp 1.2**	You can also use asdot+ format 1.2 to represent four-octet AS number of 65538
DES-7200(config-router)# **end**	Return to privileged mode.
DES-7200 # **write**	(Optional) Save configurations.

6.23.4 Configuring the display format of 4-octet AS number

By default, the asplain format is used to display 4-octet AS number. You can also configure the display format to asdot+ format. Meanwhile, after changing the display format of 4-octet AS number, the 4-octet AS number in regular expression will also be matched using asdot+ format.

Command	Function
DES-7200 # **configure terminal**	Enter global configuration mode
DES-7200(config)# **router bgp 65538**	Enable BGP protocol and configure device AS number as 65538
DES-7200(config-router)# **bgp asnotation dot**	Use asdot+ format to display 4-octet AS number, namely 1.2
DES-7200(config-router)# **end**	Return to privileged mode.
DES-7200 # **clear ip bgp ***	Reset BGP protocol so that the regular expression can rematch.
DES-7200 # **write**	(Optional) Save configurations.

After executing "**bgp asnotation dot**" command, you must execute "**clear ip bgp ***" command to reset BGP protocol, so that the regular expression can rematch.

6.23.5 Displaying configurations

Execute "show" command to view the configuration of 4-octet AS number. This command is similar to the "show" command used in BGP.

Command	Function
DES-7200 # **show ip bgp summary**	Display the connection state of all BGP neighbors.

6.24 BGP MDT address family Configuration

When using PIM-SSM to create Default-MDT during multicast VPN network configuration, you will need to configure BGP MDT address family. Through the routing of MDT address family, PE can discover other PE addresses and initiate the grating of SPT to other PEs. (the configuration steps are detailed in "MD-SCG.doc")

6.24.1 Configuring MDT address family

6.24.1.1 Configuring VRF instance and route-related attributes

Before configuring MDT address family, VRF instance and route-related attributes must be configured first:

Command	Function
DES-7200 # **configure terminal**	Enter global configuration mode
DES-7200(config)# **ip vrf** *VRF*	Create a VRF named VRF1 and enter VRF mode.
DES-7200(config-vrf)# **rd** *rd-value*	Configure VRF RD value, which is identified using XX:XX format, such as RD 1:100. 1 refers to the AS ID of backbone network, while 100 is a numerical value specified by the user.
DES-7200(config-vrf)# **route-target** {**both | export | import**} *rt-value*	Configure route export and import RT attribute of VRF.
DES-7200(config-vrf)# {**export | import**} **map** *map*	Configure the route map for import and export routes, allowing policy-based filtering of import and export routes.
DES-7200(config-vrf)# **mdt default** *group-address*	Configure MDT group address of VRF.
DES-7200(config-vrf)# **exit**	Exit VRF mode and enter global configuration mode
DES-7200(config)# **interface** *IFNAME*	Enter interface configuration mode
DES-7200(config-if)# **ip vrf forwarding** *VRF*	Associate interface with VRF instance
DES-7200(config-if)# **ip address** *ip-address mask*	Configure IP address for the interface
DES-7200(config-if)# **end**	Return to privileged mode
DES-7200 # **show running-config**	Verify the configurations.
DES-7200 # **write**	(Optional) Save configurations.

6.24.1.2 Configuring MDT address family

Steps of MDT address family configuration are shown below:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **router bgp** *asn-num*	Create BGP and enter BGP configuration mode.
DES-7200(config-router)# **neighbor** *ip-address* **remote-as** *asn-number*	Configure BGP session.
Ruiije(config-router)# **neighbor** *ip-address* **update-source** *interface-name*	Configure to use interface address as the source address when MP-IBGP session is established; usually, the Loopback interface address is used as the source address.
Ruiije(config-router)# **address-family ipv4 mdt**	Enter MDT address family.
DES-7200(config-router-af)# **neighbor** *ip-address* **activate**	Activate the route to exchange MDT address family on BGP session.
DES-7200(config-router-af)# **neighbor** *ip-address* **next-hop-self**	Change the next-hop route to self; this command can be executed on ASBR in OptionB.

6.24.2 Displaying configurations

BGP MDT address family can be viewed by executing "show bgp ipv4 mdt" commands, including:

Command	Function
DES-7200 # **show bgp ipv4 mdt all [***ip-address* **| neighbor [***ip-address***] | summary]**	Display all routes under all RDs, a specific route, neighbor information and summary information of MDT address family.
DES-7200 # **show bgp ipv4 mdt rd** *rd* **[***ip-address***]**	Display all routes or a specific route under a specific RD of MDT address family.

6.25 BGP MCE Configuration

6.25.1 MCE Overview

MCE refers to Multi-CE. MCE enabled network device can function as the CEs of multiple VPN instances in a BGP/MPLS VPN network, thus reducing the

investment on network equipment.

6.25.2 Working principle of BGP MCE

With BGP/MPLS VPN, data of private networks can be transmitted in the public network securely through tunnels. However, in a typical BGP/MPLS VPN network, each VPN is connected to the PE through a CE, as shown in Figure 15:

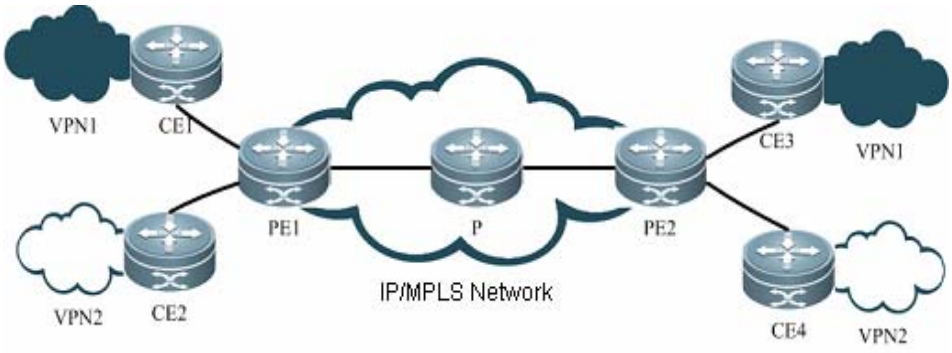


Fig 15 BGP/MPLS VPN network

With the users' increasing demand for service segmentation and security, a private network may be divided into multiple VPNs, and the users of different VPNs are usually isolated from each other. In such a circumstance, equipment investment and maintenance cost may increase by assigning a CE for each of the VPNs, while data security cannot be guaranteed by sharing one CE and using the same routing entry among multiple VPNs. MCE can well address the contradiction between data security and network cost. By binding the VLAN interfaces of CE device to the VPNs in a network, you can create and maintain a routing table for each of the VPNs (Multi-VRF). In this way, packets of different VPNs in the private network can be isolated. Moreover, with the cooperation of the PE, the routes of each VPN can be advertised to the corresponding remote PE properly, so that packets of each VPN can be transmitted securely through the public network.

The following example shows how MCE maintains routing entries of multiple VPNs and how the MCE exchanges VPN routes with PEs.

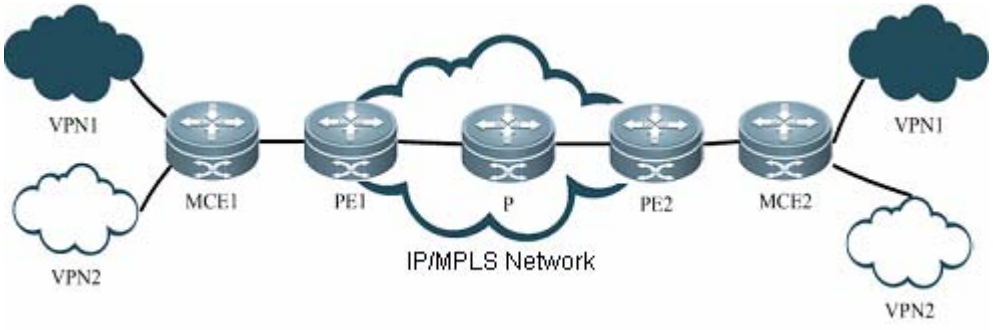


Fig 4 MCE functional diagram

As shown in Figure 16, two VPN sites on the left side (VPN1 and VPN2) are connected to the MPLS backbone network through an MCE device. Users of VPN1 and VPN2 need to establish VPN tunnels with remote users of VPN1 and VPN2. With MCE enabled, routing tables can be created for VPN1 and VPN2 individually on MCE device; VLAN-interface 2 can be bound to VPN1, and VLAN-interface 3 can be bound to VPN 2. When receiving a piece of routing information, MCE determines the source of the routing information according to the number of the interface receiving the information and then maintains the corresponding VPN routing table accordingly. Meanwhile, you also need to bind the MCE-connecting interfaces on PE1 to the VPNs in the same way as those on the MCE device. The MCE device is connected to PE1 through a trunk, which permits packets of VLAN2 and VLAN3 with VLAN tags carried. In this way, PE1 can determine the VPN to which a received packet belongs according to the VLAN tag of the packet and passes the packet to the corresponding tunnel.

How does MCE device accurately transmit the private routing information of multiple VPN instances to PEs? This involves two steps: routing information exchange between MCE and VPN site, and routing information exchange between MCE and PE. There are multiple ways to exchange routing information, such as static route, RIP, OSPF, ISIS and BGP. If BGP routing protocol is utilized to exchange routing information, BGP MCE is then used, namely BGP MCE allows BGP protocol to support VRF and enable BGP routing information exchange under VRF. We need to configure BGP peer for each VRF instance on MCE and introduce IGP routing information of corresponding VPN. Since each VPN is generally in different AS, EBGP is therefore used to advertise routes.

6.25.3 Default configurations

The following table describes the default configurations of BGP MCE.

Function	Default setting
VRF instance	No VRF instance is created by default.
BGP-VRF binding	No BGP-VRF binding by default

6.25.4 Configuring VRF instance and route-related attributes

Before configuring BGP MCE, VRF instance and route-related attributes must be configured first:

Command	Function
DES-7200 # **configure terminal**	Enter global configuration mode
DES-7200(config)# **ip vrf** *VRF1*	Create a VRF named VRF1 and enter VRF mode.

DES-7200(config-vrf)# **rd** *rd-value*	Configure VRF RD value, which is identified using XX:XX format, such as RD 1:100. 1 refers to the AS ID of backbone network, while 100 is a numerical value specified by the user.
DES-7200(config-vrf)# **route-target** {**both | export | import**} *rt-value*	Configure route export and import RT attribute of VRF.
DES-7200(config-vrf)# {**export | import**} **map** *map*	Configure the route map for import and export routes, allowing policy-based filtering of import and export routes.
DES-7200(config-vrf)# **exit**	Exit VRF mode and enter global configuration mode
DES-7200(config)# **interface vlan** *2*	Enter VLAN 2 interface configuration mode.
DES-7200(config-if)# **ip vrf forwarding** *VRF1*	Associate interface with VRF instance of VRF2
DES-7200(config-if)# **ip address** *172.16.25.18 255.255.255.0*	Configure IP address for VLAN 2
DES-7200(config-if)# **end**	Return to privileged mode
DES-7200 # **show running-config**	Verify the configurations
DES-7200 # **write**	(Optional) Save configurations.

6.25.5 Configuring BGP route exchange between MCE and VPN site

To use BGP protocol to exchange routing information between MCE and VPN site, you need to bind BGP to the corresponding VRF instance on MCE, and configure site device as EBGP neighbor, as shown below:

Command	Function
DES-7200 # **configure terminal**	Enter global configuration mode
DES-7200(config)# **router bgp** *23*	Enable BGP protocol and enter BGP routing process mode
DES-7200(config-router)# **address-family ipv4 vrf** *VRF1*	Enter IPv4 address family configuration mode of VRF1
DES-7200(config-router-af)# **neighbor** *172.16.25.57* **remote-as** *65531*	Configure EBGP neighbor and study the routing information advertised by VPN site through BGP.

DES-7200(config-router-af)# **redistribute** *ospf 1*	Introduce the routing information of remote VPN as advertised by PE. Here we assume that MCE and PE exchange routing information through OSPF protocol.
DES-7200(config- router-af))# **end**	Return to privileged mode.
DES-7200 # **show running-config**	Verify the configurations.
DES-7200 # **write**	(Optional) Save configurations.

BGP protocol shall also be configured on the CE device of VPN site, allowing VPN site to exchange routing information with MCE device through BGP protocol.

6.25.6 Configuring BGP route exchange between MCE and PE

To use BGP protocol to exchange routing information between MCE and PE, you need to bind BGP to the corresponding VRF instance on MCE, and configure PE device as EBGP neighbor, as shown below:

Command	Function
DES-7200 # **configure terminal**	Enter global configuration mode
DES-7200(config)# **router bgp** *23*	Enable BGP protocol and enter BGP routing mode
DES-7200(config-router)# **address-family ipv4 vrf** *VRF1*	Enter IPv4 address family configuration mode of VRF1
DES-7200(config-router-af)# **neighbor** *172.16.25.157* **remote-as** *65532*	Configure EBGP neighbor and study the routing information advertised by PE through BGP.
DES-7200(config-router-af)# **redistribute** *ospf 1*	Introduce the routing information of local VPN. Here we assume that MCE and local VPN site exchange routing information through OSPF protocol.
DES-7200(config- router-af))# **end**	Return to privileged mode.
DES-7200 # **show running-config**	Verify the configurations.
DES-7200 # **write**	(Optional) Save configurations.

BGP protocol shall also be configured on the PE device, and MCE shall be configured as EBGP neighbor, allowing PE to exchange routing information with

MCE device through BGP protocol.

6.25.7 Displaying configurations

The "show" commands used in BGP MCE are similar to the "show" commands used in ordinary BGP. The displayed information includes neighbor state, routing information, neighbor summary and etc.

Command	Function
DES-7200 # **show ip vrf**	Display all VRF summary information configured on the device.
DES-7200 # **show ip vrf detail** [*VRF1*]	Display the detailed configurations about all VRFs or a specific VRF.
DES-7200 # **show ip vrf interfaces** [*VRF1*]	Display the interface binding information and state of all VRFs or a specific VRF.
DES-7200# **show ip bgp vrf** *VRF1* [**summary| neighbors|** *A.B.C.D*]	Display the summary information, detailed information, specific routing information, and all routing information of BGP neighbor under VRF1. Similar to those "show" commands used in ordinary BGP, other subcommands won't be explained herein.
DES-7200# **show bgp vpnv4 unicast** [**all | rd** *rd* **| vrf** *vrf-name*] [**neighbors | summary |** *A.B.C.D*]	This command is similar to the above command, but the routes displayed are different: "all" will display all vpn routes, "rd" will display vpn routes with a specific RD value, and "vrf" will display vpn routes under a specific VRF.

6.26 BGP/MPLS VPN Configuration

Please refer to the section of "BGP/MPLS L3VPN Configuration" in "MPLS Configuration Guideline" for details.

6.27 Protocol Independent Configuration

6.27.1 route-map Configuration

The BGP protocol applies the Route-map policy on a large scale. For the configuration of the Route-map policy, refer to the Protocol Independent Configuration Part in this manual.

6.27.2 Regular Expression Configuration

The regular expression is the formula to match the string according to a certain template. The regular expression is used to evaluate the text data and return a true or false value. That is to say, whether the expression can describe this data correctly.

6.27.2.1 Description of Control Characters for Regular Expression

The BGP path attribute uses the regular expression. Here will briefly describe the use of the special characters for the regular expression:

Characters	Signs	Special Functions
Period	.	Match with any single character.
Asterisk	*	Match with none or any sequence of the string.
Plus	+	Match with one or any sequence of the string.
Interrogation Mark	?	Match with none or one sign of the string.
Plus Sign	^	Match with the starting of the string.
Dollar	$	Match with the end of the string.
Underlining	_	Match with the comma, bracket, the starting and end of the string and blank.
Square Brackets	[ ]	Match with the single character within the specified scope.

6.27.2.2 Application Example of Regular Expression

Run the **show ip bgp** command on the device:

```
DES-7200# show ip bgp

Status codes: s suppressed, d damped, h history, * valid, > best, i - internal

 Origin codes: i - IGP, e - EGP, ? - incomplete
 Status Network          Next Hop     Metric  LocPrf  Path
 ------ ----------------- --------------  --------  --------
 -------------------
 *>  211.21.21.0/24   110.110.110.10  0     1000   200 300
 *>  211.21.23.0/24   110.110.110.10  0     1000   200 300
 *>  211.21.25.0/24   110.110.110.10  0     1000   300
```

```
*>  211.21.26.0/24    110.110.110.10  0     1000   300
*> 1.1.1.0/24       192.168.88.250  444         0   606
*> 179.98.0.0       192.168.88.250  444         0   606
*> 192.92.86.0      192.168.88.250  8883        0   606
*> 192.168.88.0     192.168.88.250  444         0   606
*> 200.200.200.0    192.168.88.250  777         0   606
```

Use the regular expression in the **show** command:

```
DES-7200# show ip bgp regexp _300_
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
Status Network        Next Hop          Metric  LocPrf  Path
------ -----------------  ---------------   --------  --------
-------------------
*>  211.21.21.0/24  110.110.110.10  0     1000   200 300
*>  211.21.23.0/24  110.110.110.10  0     1000   200 300
*>  211.21.25.0/24  110.110.110.10  0     1000   300
*>  211.21.26.0/24  110.110.110.10  0     1000   300
```

6.28 BGP Load Protection Configuration

Too many BGP routes will always lead to the switch overload, especially for the switch with low memory size. Configuring the BGP load protection can prevent the occurance of the unforeseen switch operation problem due to the overall switch resource usage.

This section includes:

- Limiting the BGP route number
- Configuring Overflow Memory-lack

6.28.1 Limiting BGP Routes

To limit BGP routes, configure the maximum route number in the BGP address-family mode.

Use the following commands to configure the maximum route number learned from the BGP neighbor:

Command	Function
DES-7200(config)# r**outer bgp** *as-num*	Enter the BGP configuration mode.
DES-7200(config-router)#**neighbor** {*peer-address* | *peer-group-name*} **remote-as** *as-num*	Configure the BGP neighbor.
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **maximum-prefix** *maximum* [**threshold**]	Configure the maximum route number learned from the BGP neighbor.

Command	Function
[**warning-only**]	

Use the following commands to configure the maximum route number in the specified BGP address-family mode:

Command	Function
DES-7200(config)# **router bgp** *as-num*	Enter the BGP configuration mode.
DES-7200(config-router)#address-family ipv4 unicast	Enter the BGP ipv4 unicast address-family mode.
Or : DES-7200(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the BGP ipv4 VRF address-family mode.
Or : DES-7200(config-router)#address-family vpnv4 unicast	Enter the BGP VPNV4 address-family mode.
DES-7200(config-router)# **maximum-prefix** *maximum*	Configure the maximum route number in the specified BGP address-family mode.

6.28.2 Configuring Overflow Memory-lack

BGP is allowed to be in the overflow state when the memory lacks. In general, the routes BGP learned in the overflow state are dropped, and the system memory maintains in a steady state.

Use the following commands to enable BGP to be in the overflow state:

Command	Function
DES-7200(config)# **router bgp** *as-num*	Enter the BGP configuration mode.
DES-7200(config-router)# **overflow memory-lack**	Enable BGP to be in the overflow state.

Note

By default, when the memory lacks, BGP is in OVERFLOW state automatically. Use the no overflow memory-lack command to disable the BGP to be in OVERFLOW state.

Caution

In OVERFLOW state, BGP supports the **clear bgp** { *addressfamily* | **all** } * command, or you can disable and reenable BGP to exit the OVERFLOS state. When the memory restores to be enough, BGP exits the OVERFLOW state automatically.

6.29 Monitoring BGP

You can use the **Show** commands to view the route table, buffer and database of the BGP. Execute the following operations in the privileged mode:

Command	Function
DES-7200# **show ip bgp**	Show the information on all BGP routes.
DES-7200# **show ip bgp** {*network* | *network-mask* } [**longer-prefixes**]	Show the BGP route information of the specified destination.
DES-7200# **show ip bgp prefix-list** *prefix-list-name*	Show the BGP route information of the specified matching against the prefix list.
DES-7200# **show ip bgp community** [**exact**] *community-number*	Show the BGP route information including the specified community.
DES-7200# **show ip bgp community-list** *community-lister-number* [**exact**]	Show the BGP route information which matches against the specified community list.
DES-7200# **show ip bgp filter-list** *path-list-number*	Show the BGP route information which matches against the specified AS path list.
DES-7200# **show ip bgp regexp** *as-regular-expression*	Show the BGP route information of the specified regular expression which matches against the AS path attribute.
DES-7200# **show ip bgp dampening dampened-paths**	Show the suppressed flap statistics information.
DES-7200# **show ip bgp dampening flap-statistics**	Show the flap statistics information of all routes with the flap record.
DES-7200# **show ip bgp neighbors** [*address*] [**received-routes** | **routes** | **advertised-routes** | **flap-statistics** | **dampened-routes**]	Show the information of the BGP peer.
DES-7200# **show ip bgp summary**	Briefly show the configuration of the BGP router itself and the information of

Command	Function
	the peer.
DES-7200# **show ip bgp peer-group** [*peer-group-name*]	Show the configuration information of the BGP peer group.

6.30 BGP Configuration Examples

The following lists the BGP configuration.

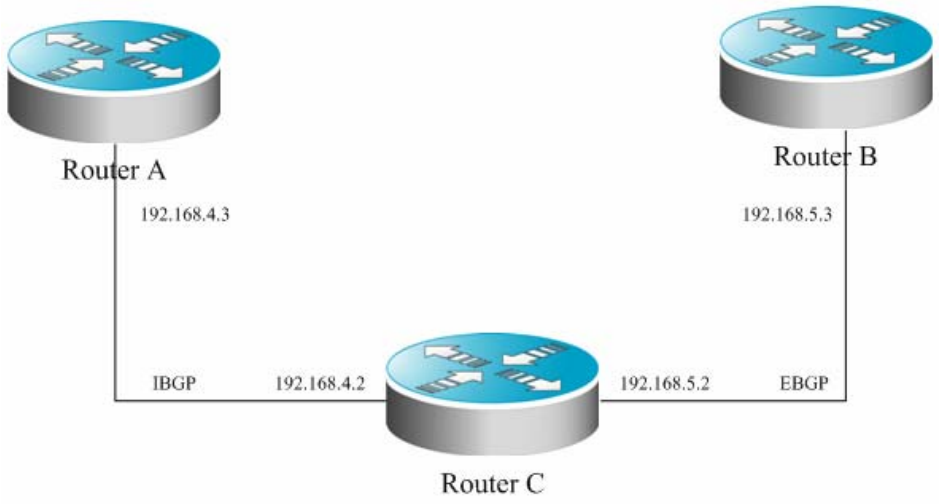
6.30.1 Configuring BGP Neighbor

The following will show how to configure the BGP neighbor. Use the **neighbor remote-as** command to configure the BGP neighbor. The concrete configuration is shown as follows:

```
router bgp 109
neighbor 131.108.200.1 remote-as 167
neighbor 131.108.234.2 remote-as 109
neighbor 150.136.64.19 remote-as 99
```

Configure one IBGP peer 131.108.234.2 and two EBGP peers 131.108.200.1 and 150.136.64.19.

The following is an example to configure the BGP neighbor. For the relationship among routers and the assignment of the IP addresses, refer to the schematics.



In this example, the BGP configuration of various routers is shown as follows:

Router A Configuration:

```
!
router bgp 100
 neighbor 192.168.4.2 remote-as 100
```

Router B Configuration:

```
!
router bgp 100
 neighbor 192.168.4.3 remote-as 100
 neighbor 192.168.5.3 remote-as 200
```

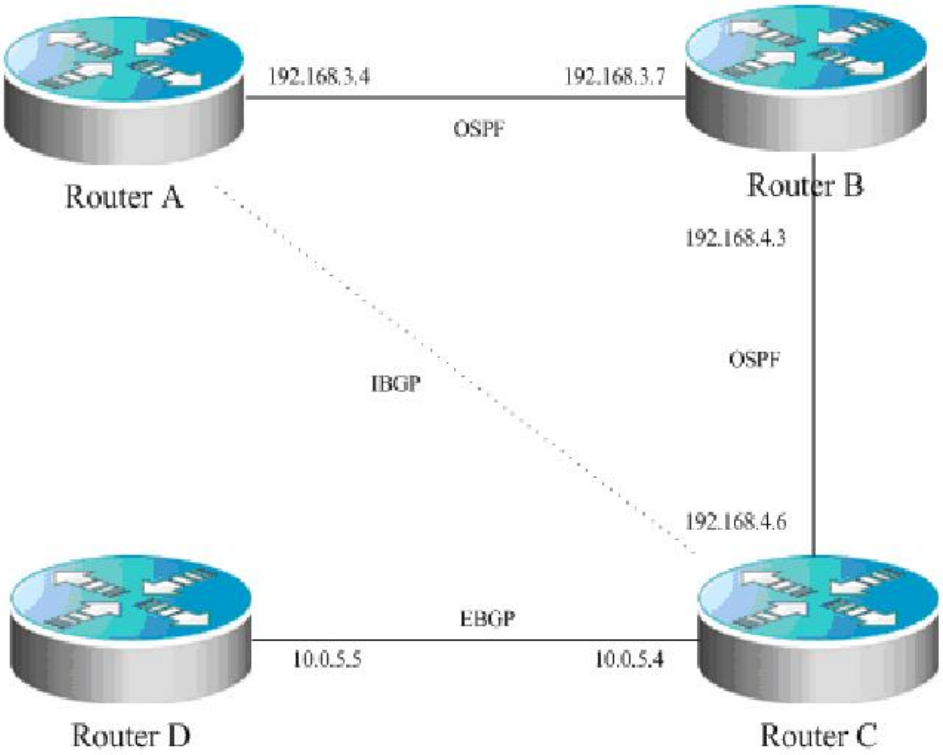
Router C Configuration:

```
!
router bgp 200
 neighbor 192.168.5.2 remote-as 100
```

6.30.2 Configuring BGP Synchronization

Use the **synchronization** command to configure synchronization in the BGP routing configuration mode, and use the **no synchronization** command to cancel the configured synchronization.

The following example shows the function of synchronization. The relationship among equipments and the assignment of the IP addresses are shown as the schematics:



In the schematics, there is a route p in the router A, which is sent to router C by the IBGP neighbor relationship. If the router C is configured with the BGP synchronization, it is necessary for the router C to wait for the IGP (this example uses the OSPF protocol) to receive the same route information p, so as to send

the route p to the EBGP neighbor router D. If the router C is configured asynchronously, it is not necessary for the BGP to wait for the IGP to receive the route p, so as to send the route p to the EBGP neighbor router D.

6.30.3 Configuring Neighbors to Use aspath Filter

Configure the **as-path access-list** command for filtering in the configuration mode firstly. Enter into the route configuration mode of the BGP after configuration, and use the **neighbor filter-list** command to apply the configured as-path access list among the BGP neighbors to filter AS paths.

The detailed configurations are as below:

```
router bgp 200
neighbor 193.1.12.10 remote-as 100
neighbor 193.1.12.10 filter-list 2 out
neighbor 193.1.12.10 filter-list 3 in
ip as-path access-list 2 permit _200$
ip as-path access-list 2 permit ^100$
ip as-path access-list 3 deny _690$
ip as-path access-list 3 permit .*
```

This configuration indicates that only the routes permitted by the **as-path access-list** *2* can be advertised to the neighbor 193.1.12.10, and the advertised routes from the neighbor 193.1.12.10 can be received only they are permitted by the **as-path access-list** *3*.

The following diagram is a configuration eaxmple showing the relationship and IP addresses of devices:

Do AS path-based filter on Router A.

The following presents the configuraiton of various devices:

Router A configuration:

```
!
ip as-path access-list 4 deny ^300_
ip as-path access-list 4 permit .*
ip as-path access-list 5 deny ^450_65_
ip as-path access-list 5 permit .*
!
router bgp 100
```

```
 bgp log-neighbor-changes
 neighbor 192.168.5.8 remote-as 200
 neighbor 192.168.5.8 filter-list 5 in
 neighbor 192.168.5.8 filter-list 4 out
```

Router B configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.5.6 remote-as 100
```

6.30.4 Configuring Route Aggregation

Use the **aggregate-address** command to configure an aggregated route in the route configuration mode. Once any route is within the configured range, this aggregated route will take into effect.

The concrete configuration is shown as follows:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0
```

Configure one aggregate route:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0 as-set
```

The **as-path** segment of the aggregated route is an collection of **ASs**:

```
router bgp 100
aggregate-address 193.0.0.0 255.0.0.0 summary-only
```

The aggregated route will not be advertised

6.30.5 Configuring Confederation

When configuring a confederatin, you need to use the **bgp confederation identifier** command to configure the AS number for external connection, and use the **bgp confederation peers** command to configure confederation members.

The concrete configuration is shown as follows:

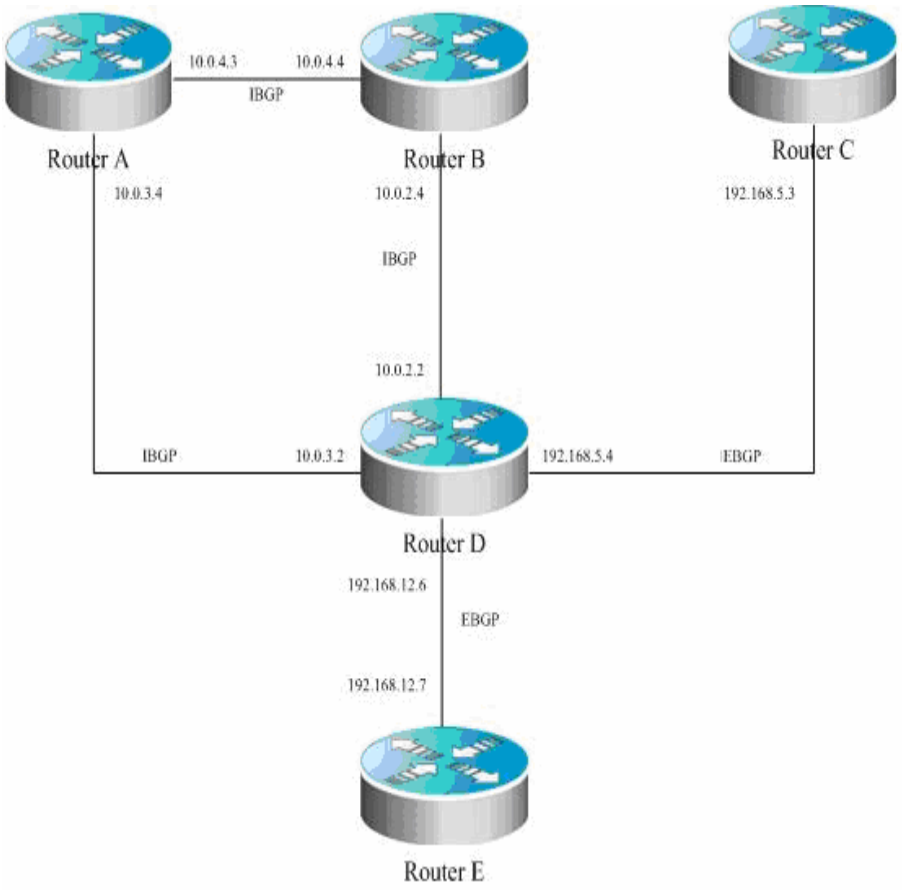
```
router bgp 6003
bgp confederation identifier 666
bgp confederation peers 6001 6002
neighbor 171.69.232.57 remote-as 6001
neighbor 171.69.232.55 remote-as 6002
neighbor 200.200.200.200 remote-as 701
```

The configuration of peer 200.200.200.200 out of the confederation is shown as follows:

```
router bgp 701
neighbor 171.69.232.56 remote-as 666
neighbor 200,200,200,205 remote-as 701
```

For the configuration, the first device is of the confederation, while the second device is not of the confederation, so they are of the EBGP neighbor relationship.

The following is an example showing the relationship and IP addresses of devices:



The following presents the configuration of various devices:

Router A configuration:

```
!
router bgp 65530
 bgp confederation identifier 100
 bgp confederation peers 65531
 bgp log-neighbor-changes
 neighbor 10.0.3.2 remote-as 65530
 neighbor 10.0.4.4 remote-as 65530
```

Router B configuration:

```
!
router bgp 65530
 bgp confederation identifier 100
 bgp log-neighbor-changes
 neighbor 192.168.5.4 remote-as 65530
```

Router C configuration

```
!
router bgp 65531
 bgp confederation identifier 100
 bgp confederation peers 65530
 bgp log-neighbor-changes
 neighbor 10.0.3.2 remote-as 65530
 neighbor 10.0.4.4 remote-as 65530
```

Router D configuration:

```
!
router bgp 65530
 bgp confederation identifier 100
 bgp confederation peers 65531
 bgp log-neighbor-changes
 neighbor 10.0.2.4 remote-as 65530
 neighbor 10.0.3.4 remote-as 65530
 neighbor 192.168.5.3 remote-as 65531
 neighbor 192.168.12.7 remote-as 200
```

Router E configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.12.6 remote-as 100
```

6.30.6 Configuring Route Reflector

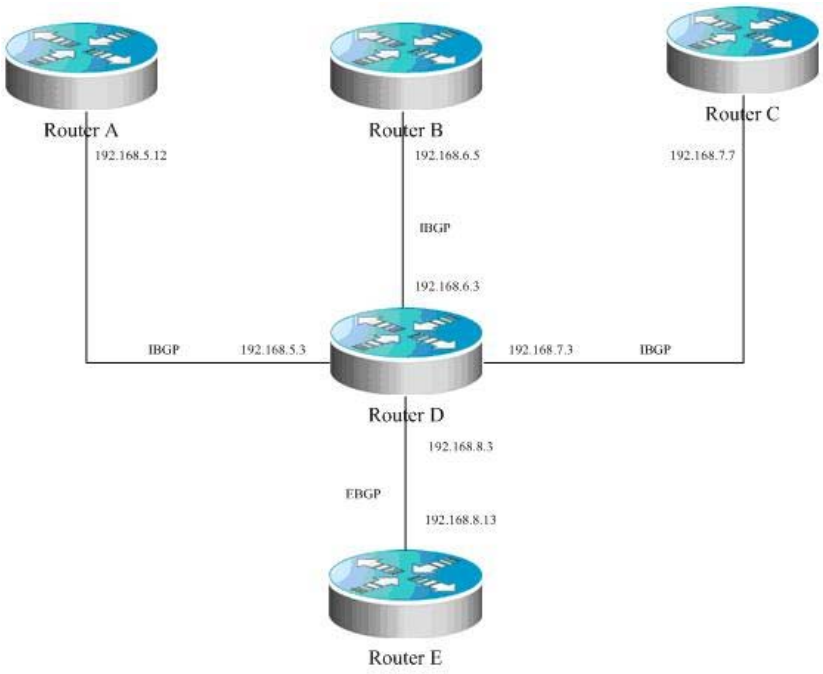
When the route reflector is configured, it is necessary to use the **bgp client-to-client reflection** command to enable the route reflection function on the device. If there are more than one route reflector within one cluster, use the **bgp** *cluster-id* command to configure the cluster ID of the reflector, and use the **neighbor** *A.B.C.D* **route-reflector-client** command to add the peer to the client of the route reflection.

The concrete configuration is shown as follows:

```
router bgp 601
```

```
bgp cluster-id 200.200.200.200
neighbor 171.69.232.56 remote-as 601
neighbor 200,200,200,205 remote-as 701
neighbor 171.69.232.56 route-reflector-client
```

The following is an example showing the relastionship and IP addresses of devices:



In this configuration example, Router D is a route reflector. The following presents the configuration of various devices:

Router A configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.5.3 remote-as 100
 neighbor 192.168.5.3 description route-reflector server
```

Router B configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.6.3 remote-as 100
 neighbor 192.168.6.3 description route-reflector server
```

Router C configuration:

```
!
router bgp 100
```

```
 bgp log-neighbor-changes
 neighbor 192.168.7.3 remote-as 100
 neighbor 192.168.7.3 description not the route-reflector server
```

Router D Configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor 192.168.5.12 remote-as 100
 neighbor 192.168.5.12 description route-reflector client
 neighbor 192.168.5.12 route-reflector-client
 neighbor 192.168.6.5 remote-as 100
 neighbor 192.168.6.5 description route-reflector client
 neighbor 192.168.6.5 route-reflector-client
 neighbor 192.168.7.7 remote-as 100
 neighbor 192.168.7.7 description not the route-reflector client
 neighbor 192.168.8.13 remote-as 200
```

Router E configuration:

```
!
router bgp 500
 bgp log-neighbor-changes
 neighbor 192.168.8.3 remote-as 100
```

6.30.7 Configuring peergroup

Here will take the configuration of **peergroup** for IBGP and EBGP as an example.

6.30.7.1 Configuring IBGP peergroup

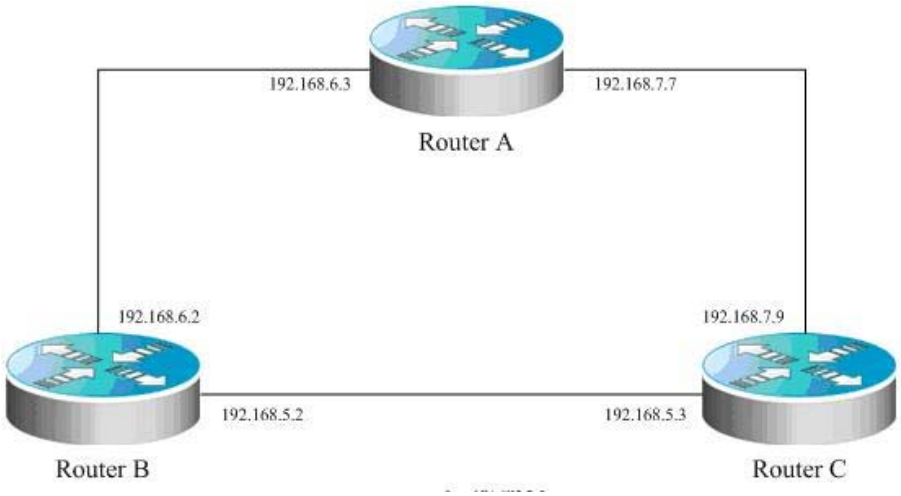
Use the **neighbor** *internal* **peer-group** command to create a peer group named *internal* firstly, and then configure a remote AS and other options for the peer group. Use the **neighbor** *A.B.C.D* **peer-group internal** command to add the peers A.B.C.D into the peer group.

The configuration commands are as below:

```
router bgp 100
neighbor internal peer-group
neighbor internal remote-as 100
neighbor internal update-source loopback 0
neighbor internal route-map set-med out
neighbor internal filter-list 1 out
neighbor internal filter-list 2 in
neighbor 171.69.232.53 peer-group internal
neighbor 171.69.232.54 peer-group internal
```

```
neighbor 171.69.232.55 peer-group internal
neighbor 171.69.232.55 filter-list 3 in
```

The following is an example showing the relastionship and IP addresses of devices:



Router A configuration

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ibgp-group peer-group
 neighbor ibgp-group description peer in the same as
 neighbor 192.168.6.2 remote-as 100
 neighbor 192.168.6.2 peer-group ibgp-group
 neighbor 192.168.6.2 description one peer in the ibgp-group
 neighbor 192.168.7.9 remote-as 100
 neighbor 192.168.7.9 peer-group ibgp-group
```

Router B configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ibgp-peer peer-group
 neighbor ibgp-peer remote-as 100
 neighbor ibgp-peer route-map ibgp-rmap out
 neighbor 192.168.5.3 peer-group ibgp-peer
 neighbor 192.168.5.3 route-map set-localpref in
 neighbor 192.168.6.3 peer-group ibgp-peer
```

Router C configuration:

```
!
router bgp 100
```

```
bgp log-neighbor-changes
neighbor ibgp-group peer-group
neighbor 192.168.5.2 remote-as 100
neighbor 192.168.5.2 peer-group ibgp-group
neighbor 192.168.7.7 remote-as 100
neighbor 192.168.7.7 peer-group ibgp-group
```

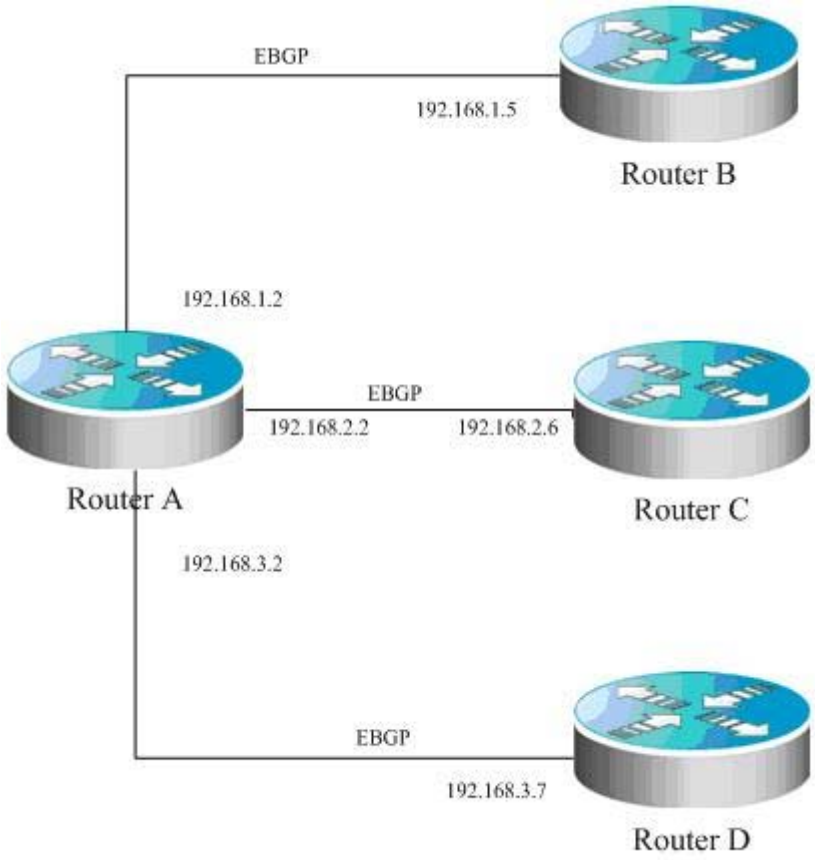
6.30.7.2 Configuring EBGP peergroup

Use the **neighbor** *A.B.C.D* **remote-as** *num* command to configure an EBGP peer . Use the **neighbor external peer-group** command to create a peer group named **external**, and then apply the **neighbor** *A.B.C.D* **peer-group** *external* command to add the peers A.B.C.D into the peer group *external*.

Following is an example of the specific configuration:

```
router bgp 100
neighbor external-peers peer-group
neighbor external-peers route-map set-metric out
neighbor external-peers filter-list 99 out
neighbor external-peers filter-list 101 in
neighbor 171.69.232.90 remote-as 200
neighbor 171.69.232.90 peer-group external-peers
neighbor 171.69.232.100 remote-as 300
neighbor 171.69.232.100 peer-group external-peers
neighbor 171.69.232.110 remote-as 400
neighbor 171.69.232.110 peer-group external-peers
neighbor 171.69.232.110 filter-list 400 in
```

Following is a diagram to show the configuration of peer-group:



The relationship between devices and the assigning of IP address are shown in the figure.

Router A configuration:

```
!
router bgp 100
 bgp log-neighbor-changes
 neighbor ebgp-group peer-group
 neighbor ebgp-group distribute-list 2 in
 neighbor ebgp-group route-map set-med out
 neighbor 192.168.1.5 remote-as 200
 neighbor 192.168.1.5 peer-group ebgp-group
 neighbor 192.168.2.6 remote-as 300
 neighbor 192.168.2.6 peer-group ebgp-group
 neighbor 192.168.2.6 distribute-list 3 in
 neighbor 192.168.3.7 remote-as 400
 neighbor 192.168.3.7 peer-group ebgp-group
!
```

Router B configuration:

```
!
router bgp 200
```

```
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 100
!
```

Router C configuration:

```
!
router bgp 300
 bgp log-neighbor-changes
 neighbor 192.168.2.2 remote-as 100
!
```

Router D configuration:

```
!
router bgp 400
 bgp log-neighbor-changes
 neighbor 192.168.3.2 remote-as 100
!
```

6.30.8 Configuring TCP MD5

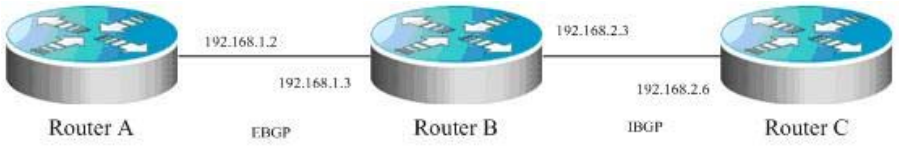
Use the CLI command **neighbor password** to configure the TCP MD5 for the BGP connection in the BGP configuration mode.

The configuration format is shown as follows:

```
router bgp 100
neighbor 171.69.232.54 remote-as 110
neighbor 171.69.232.54 password peerpassword
```

Here configures the *password* of peer 171.69.232.54 as *peerpassword.*

The following diagram shows the configuration of MD5 and IP address on various devices:



The AS of router A is 100, and the AS of router B and router C is 200. Router A establishes EBGP neighbor relationship with router B and uses EBGP as the MD5 password. Router B establishes IBGP neighbor relationship with router C and uses IBGP as the MD5 password.

router A configuration:

```
!
router bgp 100
```

```
 bgp log-neighbor-changes
 neighbor 192.168.1.3 remote-as 200
 eighbor 192.168.1.3 password ebgp
!
```

Router B configuration:

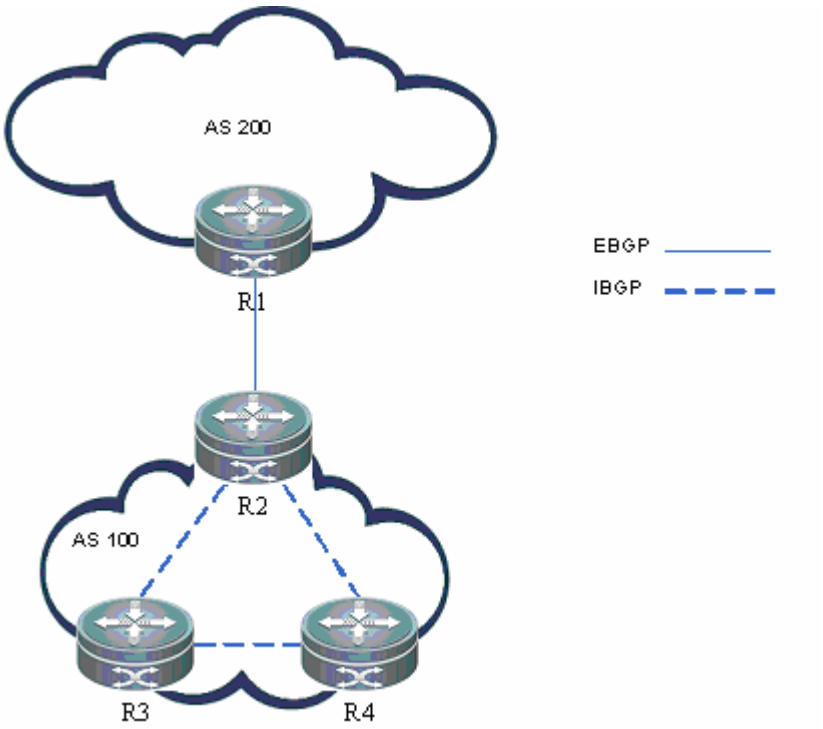
```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.1.2 remote-as 100
 neighbor 192.168.1.2 password ebgp
 neighbor 192.168.2.6 remote-as 200
 neighbor 192.168.2.6 password ibgp
!
```

Router C configuration:

```
!
router bgp 200
 bgp log-neighbor-changes
 neighbor 192.168.2.3 remote-as 200
 neighbor 192.168.2.3 password ibgp
!
```

6.30.9 Configuring BGP GR

As shown in the following figure, R2 is the border device of AS100 and AS200. R1 is the access device of AS200. In AS100, R2, R3 run OSPF to offer IBGP connection for the BGP protocol. At the same time, mutual IBGP conneciton is established among them. R2 establishes an EBGP conneciton with R1. R2 as the border device connecting AS100 and AS200 requires higher reliability. Here R2 is configured to support dual-system redundant bakcup for continuous forwrding and graceful restart of routing protocols (OSPF and BGP in this example). The graceful restart of routing protocols needs the assistant of adjacent devices. Hence, R1, 3 and R4 need to support the BGP GR capability, and R3 and R4 need to support the GR Helper of OSPF to support the OSPF GR capabiltiy. In this way, when one engine of R2 fails, the transmission of data is not interrupted for higher reliability.



Confiugration precaution:

Before configuration, make sure that R2 can serve as the GR Restarter for graceful restart and the software on all devices support OSPF GR and BRP GR capability. If the software does not support OSPF GR and BGP GR, continuous data forwarding is not available when the backup engine takes over the works of the master engine in case of failure. Meanwhile, the enablement of BGP protocol depends on the BGP connection from OSPF. Hence, the BGP protocol and the OSPF protocol should enable GR simultaneously. This is why R2 is required to support OSPF GR.

- Whether R2 enables dual-eningle redundnat hot backup
- The software of all devices support OSPF GR and BGP GR capability
- Enable OSPF GR on R2
- Enable BGP GR on R2
- Enable BGP GR on neighbors to support the GR Helper of BGP
- Restart all BGP connections on R2 to neotitate GR capabitliy

Configuration steps

1，Make sure whether R2 enables dual-eningle redundnat hot backup

2，Make sure the software of all devices support OSPF GR and BGP GR capability

Check wheter these devices support the configuration commands of BGP GR and OSPF GR. For details, refer to Step 3.

3，Enable OSPF GR on R2

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# graceful-restart
```

4，Enable BGP GR on R2

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# graceful-restart
```

5，Enable BGP GR on neighbors to support the GR Helper of BGP

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# bgp graceful-restart
```

For negotiation of BGP GR, both sides of the BGP connection need to enable BGP GR. Hence, R2 needs to negotiate with its neighbors which serve as the GR Helper to assist BGP GR.

6，Restart all BGP connections on R2 to neotitate GR capabitliy

```
DES-7200# clear ip bgp *
```

Check configuration

In order for R2 to enable continuous data forwarding during engine handover, check the negotiation of BGP GR and OSPF GR configration.

Ensure that BGP GR negitation with all neighbors succeed.

```
DES-7200# show ip bgp neighbors
BGP neighbor is 192.168.195.183, remote AS 200, local AS 100, external link
Using BFD to detect fast fallover - BFD session state up
  BGP version 4, remote router ID 10.0.0.1
  BGP state = Established, up for 00:06:37
  Last read 00:06:37, hold time is 180, keepalive interval is 60 seconds
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
Address family IPv4 Unicast: advertised and received
Graceful restart: advertised and received
  Remote Restart timer is 120 seconds
  Address families preserved by peer:
    None
```

Here “Graceful restart: advertised and received” means BGP GR negotiation of the BGP connection succeeds. Here you need to make sure that BGP GR negotiation of all BGP connections succeeds.

Enuser that OSPF GR is configured on R2 successfully

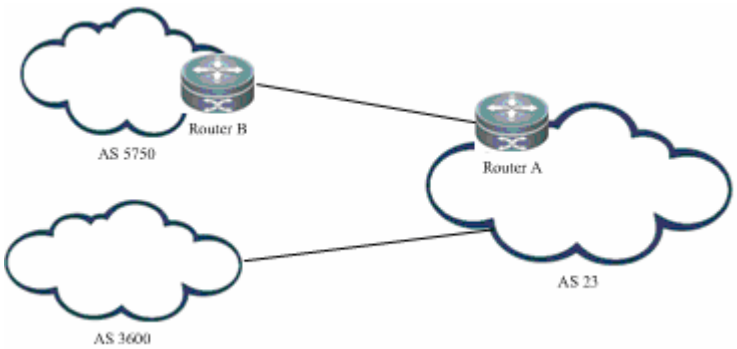
```
DES-7200# show ip ospf
Routing Process "ospf 1" with ID 10.0.0.2
Process uptime is 4 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583Compatibility flag isenabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
This router is an ASBR (injecting external routing information)
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
LsaGroupPacing: 240 secs
Number of incomming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 4. Checksum 0x0278E0
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 4
External LSA database is unlimited.
Number of LSA originated 6
Number of LSA received 2
Log Neighbor Adjency Changes : Enabled
Graceful-restart enabled
Graceful-restart helper support enabled
Number of areas attached to this router: 1
Area 0 (BACKBONE)
```

Here “Graceful restart enabled “means OSPF GR is configured successfully.

6.30.10 Configuring BGP Local AS

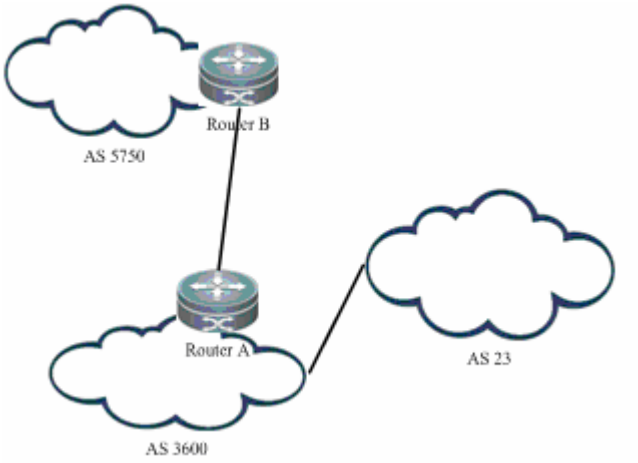
Network requirements

As shown in the following figure, Router A and the network it belogs to is located in AS 23, which connects AS 3600 through EBGP. The route information of AS 5750 is transmitted to AS 3600 via AS 23.



Locial topology before AS migration

Now there is a need to migrate Router A and the network it belogs to AS 3600.

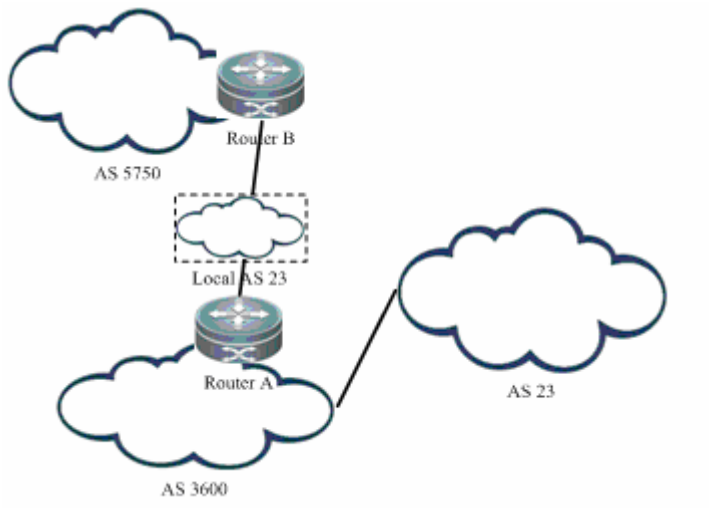


Logical topology after AS migration

AS 23 and AS 3600 belong to one management domain. The configurations of these two ASs are modified after negotiation. At this point, Router A configures AS 3600 as the AS of the BGP protocol. In this case, you need to maintain the BGP connection between Router A and Router B, and modify the corresponding peer configuration on Router B of AS 5750. For some reasons, Router B will not modify the configuration immediately. As a result, Router B cannot establish the BGP connection with Router A. Here on Router A, you can configure local AS for Router B so as to establish the BGP connection between them wihtout affecting the transmisison and calculation of routes.

Networking topology

The following figure illustrates how to configure local AS for Router B.



After configuration, there is a virtual AS 23 between Router A and Router B. Router B considers that it directly connects to AS 23 and transmits routes to it.

Consequently, Router B does not need to modify its configuration. Later when AS 3600 reaches an agreement with AS 5750 in terms of management, Router B can modify the remote AS of Router A to be AS 3600 and Router A deletes the corresponding local AS for migration of part network in different ASs.

Configuration steps

1, Enter the BGP configuration mode

```
DES-7200-A(config)# router bgp 3600
```

2, Configure local AS for the peer

```
DES-7200-A(config-router)# neighbor 57.50.1.1 local-as 23 no-prepend
replace-as dual-as
```

3, Delete local AS after Router B modifies its configuration

```
DES-7200-A(config-router)#no neighbor 57.50.1.1 local-as
```

Check configuration

The neighbor uses local AS to establish the BGP conneciton.

```
DES-7200-A#show ip bgp neighbors 57.50.1.1
BGP neighbor is 57.50.1.1,  remote AS 5750, local AS 23(using Peer's Local AS,
no-prepend, replace-as, dual-as), external link
  BGP version 4, remote router ID 0.0.0.0
  BGP state = Idle
  Last read       , hold time is 180, keepalive interval is 60 seconds
  Received 0 messages, 0 notifications, 0 in queue
    open message:0 update message:0 keepalive message:0
    refresh message:0 dynamic cap:0 notifications:0
  Sent 0 messages, 0 notifications, 0 in queue
```

Detailed configuration:

Router A configuration

```
router bgp 3600
neighbor 57.50.1.1 remote-as 5750
neighbor 57.50.1.1 local-as 23 no-prepend replace-as dual-as
neighbor 57.50.1.1 update-source loopback 0
neighbor 57.50.1.1 ebgp-multihop 255
```

Router B configuration

```
router bgp 5750
neighbor 36.0.1.1 remote-as 23
neighbor 36.0.1.1 update-source loopback 0
neighbor 36.0.1.1 ebgp-multihop 255
```

6.30.11 Configuring Typical BGP 4-Octet AS

Networking requirements

- BGP connection is established between the router supporting 2-octet AS number and the router supporting 4-octet AS number (using 2-octet AS number);
- BGP connection is established between the router supporting 2-octet AS number and the router supporting 4-octet AS number (using 4-octet AS number);
- BGP connection is established between routers supporting 4-octet AS number, with one router using 2-octet AS number and the other router using 4-octet AS number.

Network topology

As shown below, Router A, Router B and Router C are edge routers of three autonomous systems, and BGP connections have been established between them. Router A only supports 2-octet AS number; Router B and Router C support 4-octet AS number. The autonomous system to which Router A belongs uses a 2-octet AS number of 64496; the autonomous system to which Router B belongs uses a 2-octet AS number of 64497; the autonomous system to which Router C belongs uses a 4-octet number of 1.2.

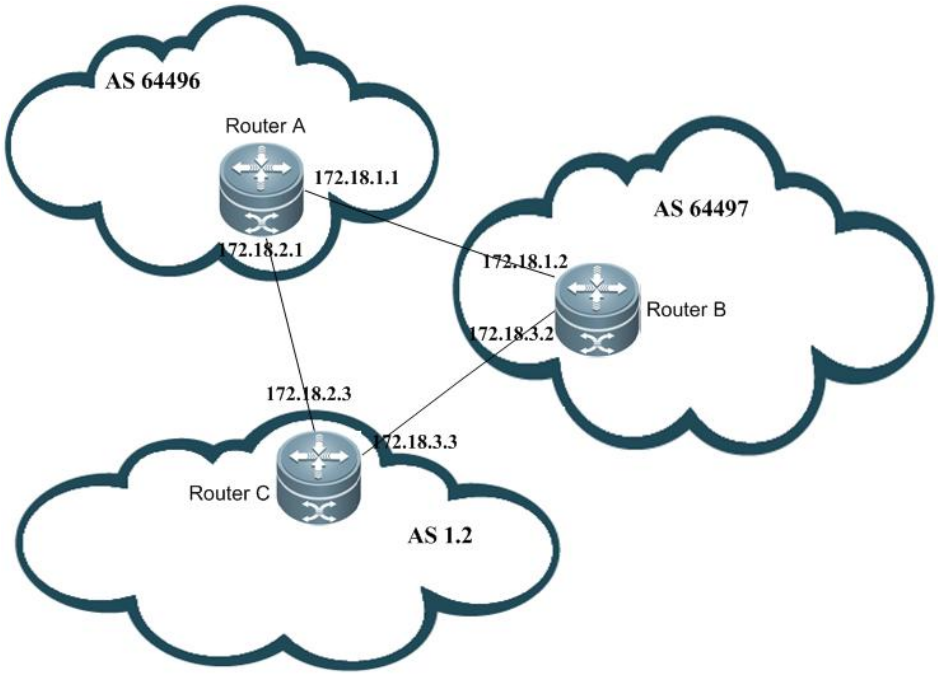


Fig 18 BGP 4-Octet AS configuration

Configuration tips

- Router A cannot recognize the 4-octet AS number of 1.2 used by the

autonomous system to which Router C belongs; when creating the neighbor, the reserved AS number of 23456 shall be used to replace 1.2 when configuring remote-as.

- Although Router B supports 4-octet AS number, it still uses the 2-octet AS number. Therefore, the AS number of peer side can be used as remote-as while neighbor interconnection is being created between Router A and Router B.
- Router B can recognize the 4-octet AS number used by the autonomous system to which Router C belongs. The AS number of peer side can be used as remote-as while creating the neighbor.

Configuration Steps

Router A

```
DES-7200# conf t
DES-7200(config)# router bgp 64496
DES-7200(config-router)# neighbor 172.18.1.2 remote-as 64497
DES-7200(config-router)# neighbor 172.18.2.3 remote-as 23456
```

Router B

```
DES-7200# conf t
DES-7200(config)# router bgp 64497
DES-7200(config-router)# neighbor 172.18.1.1 remote-as 64496
DES-7200(config-router)# neighbor 172.18.3.3 remote-as 1.2
# Use "bgp asnotation dot" command to change the display format of 4-octet AS
number
DES-7200(config-router)# bgp asnotation dot
DES-7200(config-router)# end
DES-7200# clear ip bgp *
```

Router C

```
DES-7200# conf t
DES-7200(config)# router bgp 1.2
DES-7200(config-router)# neighbor 172.18.2.1 remote-as 64496
DES-7200(config-router)# neighbor 172.18.3.2 remote-as 64497
```

Verification

Display the neighbor connection state on Router A:

```
DES-7200# show ip bgp summary

BGP router identifier 172.18.1.1, local AS number 64496
BGP table version is 1, main routing table version 1
```

```
Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
172.18.1.2      4      64497       7       7        1    0    0 00:03:04     0
172.18.2.3      4      23456       4       4        1    0    0 00:00:15     0
```

Display the neighbor connection state on Router B:

```
DES-7200# show ip bgp summary

BGP router identifier 172.18.3.2, local AS number 64497
BGP table version is 1, main routing table version 1

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
172.18.1.1      4      64496       7       7        1    0    0 00:03:04     0
172.18.3.2      4      65538       4       4        1    0    0 00:01:18     0
After executing "bgp notation dot" command, the following information will be
displayed:
DES-7200# show ip bgp summary

BGP router identifier 172.18.3.2, local AS number 64497
BGP table version is 1, main routing table version 1

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
172.18.1.1      4      64496       7       7        1    0    0 00:00:04     0
172.18.3.2      4        1.2       4       4        1    0    0 00:00:16     0
```

Display the neighbor connection state on Router C:

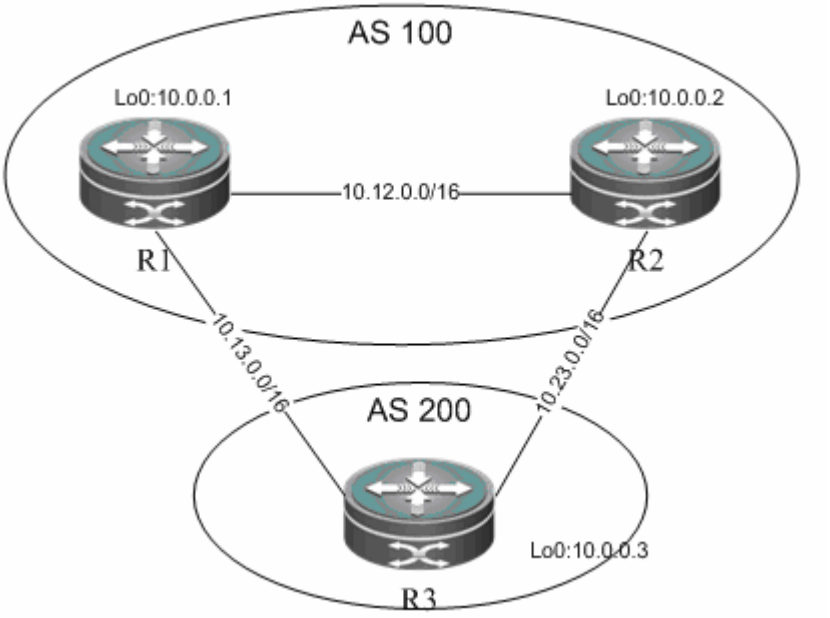
```
DES-7200# show ip bgp summary

BGP router identifier 172.18.3.3, local AS number 65538
BGP table version is 1, main routing table version 1

Neighbor        V         AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  Statd
172.18.2.1      4      64496       7       7        1    0    0 00:00:15     0
172.18.3.2      4      65597       4       4        1    0    0 00:01:19     0
```

6.30.12 Configuring BGP MDT address family

Networking requirements

Device R1 and R2 belong to the same AS. Device R3 belongs to another AS. Multicast VPN needs to be established between them, and BGP is used to transmit information about MDT address family.

Network topology



Here, R1 and R2 belong to AS100; IBGP connection is established between R1 and R2 to transmit routes of MDT address family. R3 belongs to AS200 and establishes EBGP connections with R1 and R2 to transmit MDT address family.

Configuration tips

- Configure VRF instances and associate with interfaces to allow network isolation;
- Configure BGP routing protocol to advertise routes of MDT address family

Configuration Steps

1, Configure VRF instances and associate with interfaces;

R1

Create a VRF instance named "VRF1"

```
DES-7200# config terminal
DES-7200(config)# ip vrf VRF1
DES-7200(config-vrf)# rd 100:1
```

```
DES-7200(config-vrf)# route-target both 123:123
DES-7200(config-vrf)# mdt default 232.1.1.1
DES-7200(config-vrf)# exit
```

Associate Gi0/1 with VRF1

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-GigabitEthernet 0/1)# ip vrf forwarding VRF1
DES-7200(config-GigabitEthernet 0/1)# ip address 10.1.1.1 255.255.255.0
DES-7200(config-GigabitEthernet 0/1)# exit
```

The configurations of R2 and R3 are the same as that of R1.

2, Configure BGP routing protocol to advertise routes of MDT address family

R1

Configure MDT address family

```
DES-7200# configure terminal
DES-7200(config)# router bgp 100
```

Configure R2 and R3 as BGP neighbors

```
DES-7200(config-router)# neighbor 10.0.0.2 remote-as 100
DES-7200(config-router)# neighbor 10.0.0.2 update-source loopback 0
DES-7200(config-router)# neighbor 10.13.0.3 remote-as 200
```

Activate R2 and R3 under MDT address family

```
DES-7200(config-router)# address-family ipv4 mdt
DES-7200(config-router-af)# neighobr 10.0.0.2 activate
DES-7200(config-router-af)# neighobr 10.13.0.3 activate
```

Activate R2 and R3 under VPNv4 address family

```
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighobr 10.0.0.2 activate
DES-7200(config-router-af)# neighobr 10.13.0.3 activate
```

Bind VRF to BGP

```
DES-7200(config-router)# address-family ipv4 vrf VRFi
DES-7200(config-router)# exit
```

The configurations of R2 and R3 are the same as that of R1.

Verification

Execute the following steps to verify configurations:

1, Verify the state of interfaces bound to VRF. Execute "show ip vrf interface" to

verify interface binding information and interface state.

```
DES-7200#show ip vrf interfaces
Interface           IP-Address     VRF                Protocol
GigabitEthernet 0/1  10.1.1.1       VRF1               up
```

2, Make sure MDT routes exist in BGP protocol, as shown below:

```
DES-7200#show bgp ipv4 mdt all
BGP table version is 1, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network         Next Hop          Metric  LocPrf     Weight Path
Route Distinguisher: 100:1
*> 10.0.0.1/32    0.0.0.0             0        32768      ?
*>i10.0.0.2/32    10.0.0.2            0        100        ?
*> 10.0.0.3/32    10.13.0.3           0                  200 ?

Total number of prefixes 3
```

7 Policy-based Routing Configuration

7.1 Overview

7.1.1 Introduction to Policy-based Routing

Policy-based Routing offers a more flexible packet routing forwarding mechanism than destination address-based routing forwarding, which enables you to route IPv4/v6 packets by elements like source address, destination address, port number and packet length.

In general, user networks apply different bandwidths from different ISPs. To ensure resources for important users, the system needs to selectively forward packets rather than fording packets by the general routing table. In this case, policy-based routing comes into being to take full advantages of ISP resources and satisfy the flexible and diversified applications.

7.1.2 Basic Concepts and Features

7.1.2.1 Application Process

Creating the routing map is necessary for application of policy-based routing. A routing map consists of many policies with corresponding sequence. Smaller sequence means higher priority.

Each policy consists of one or more **match** statements and corresponding one or more **set** statements. The **match** statement defines the matching rule of IPv4/v6 packets, and the **set** statement defines the processing rules of matched IPv4/v6 packets. In the course of policy-based routing, packets are matched by priorities in descending order. Once a policy is matched, the system performs corresponding actions and quits policy-based routing.

Policy-based routing for IPv4 packets uses standard or extended ACL as matching rule. Policy-based routing for IPv6 packets, however, uses extended ACL as matching rule. For IPv6 packets, only one *match ipv6 address* can be configured a policy at most.

7.1.2.2 Routing Map Policy Matching Mode

When you configure the routing map, you can specify the match mode of a policy as permit or deny, which is described as below:

Permit: Apply the corresponding **set** rule to the IPv4/v6 packets meeting the match rules of the policy. If no match rule is met, the system applies the next policy to packets.

Deny: If IPv4/v6 packets meet all **match** statements, the system performs common routing rather than policy-based routing.

IPv4/IPv6 packets are matched by the priority of every policy of the routing map in descending order. If the packets do not match any policy of the routing map, the system performs common routing.

7.1.2.3 Next Hop Rules

Policy-based routing offers two forwarding rules-**set {ip | ipv6} next-hop** and **set {ip | ipv6} default next-hop**, which set the next hop and the egress, respectively.

set {ip | ipv6} next-hop: Configure the policy-based routing's next hop IPv4/IPv6 address, which takes precedence over common routes. The IPv4/v6 packets meeting the match rule received on the interface are first forwarded to the next hop specified by the **set {ip | ipv6} next-hop** command, no matter whether the real routing of the packets in the routing table and the next hop specified by the policy-based route is valid or not.

set {ip | ipv6} default next-hop: The policy-based routing specified by this command is of the priority lower than common route but higher than default route. For the packets meeting the match rule received on the interface, if routing in the routing table is failed or the default route is used, these packets will be forwarded to the next hop specified by this command.

The next hops specified by these two rules must be direct or otherwise the configuration does not take effect.

The priority is subject to the order of set {ip | ipv6} next-hop > network route/host route > set {ip | ipv6} default next-hop >default route. These two commands can be configured simultaneously, but only the one of higher priority takes effect.

7.1.2.4 Load Balancing Mode for Policy-based Routing Next Hop

More than one next hop can be configured in the sequence of a route map, and one of the following load balancing modes can be configured among them.

Redundant backup: Only one next hop takes effect at a time if there are many next hops. Once the active next hop failed, another next hop will take over its

works immediately.

When R1 of the active next hop fails, the system automatically hands over to R2 of the next next hop. When R1 recovers, the system will automatically hand over back to R1.

When there are many next hops in the order, for instance, R1/R2/R3, R2 takes effect after you deleting and then adding R1 in the order of R2/R3/R1.

Load balancing: Load balancing is enabled among next hops by traffic. This function is not available for the next hop in egress type.

Caution

1 Only one route map can be configured on a port. Configuring route maps repeatedly on a port will overlap the previous configurations, namely that latest configuration takes effect.

2 Only one IPv6 ACL can be configured in the sub route map.

3 If the sub route map is configured with next hop but not ACL, all packets are matched; if the sub route map is configured with ACL but not next hop, the matched packets are forwarding by common routes; if the sub route map is not configured with ACL and next hop, all packets are forwarded by common routes.

4 If the policy-based routing is configured with an inexistent ACL, all packets are matched; if the policy-based routing is configured with an ACL without any ACE, the system will not match the packets starting from the ACL of the next sub route map. If the policy-based routing is configured with an inexistent ACL, all packets are matched; if the policy-based routing is configured with an ACL without any ACE, the system skips this sequence and matches packets starting from the ACL of next sub route map. It is not recommended to configure ACL without ACE.

5 The deny rule of ACE forwards packets by common routes. To meet the match rule of policy-based routing, the **deny any any** command matches packets starting from the next IPv6 ACL.

6 Enabling PBR will apply to incoming packets at the same time. If you do not need to apply PBR to a specific incoming IPv4/v6 packet, add "*deny the specific IPv4/v6 address*" in the ACL by hand.

7 In redundant backup mode, the IP packets matching the policy of the sub route map are forwarded to the next hop firstly resolved in the sequence. If all next hops are not resolved, the IP packets matching the policy are dropped. If the first next hop is resolved later, the IP packets matching the policy are forwarded to the first next hop.

8 Routers do not support enabling PBR on the DAILER interface. PBR does not take effect if it is enabled.

Note

For details on the next hop of PBR set actions, refer to *Rns&track Configuration Guide* and *Rns&track Command Reference* (for switches) or *Link Detection Configuration Guide* and *DLDP Command Reference* (for routers). IPv6 PBR is not supported at present.

For linkup of PBR and BFD, refer to *BFD Configuration Guide* and *BFD Command Reference*.

7.1.3 Enable Track Function

Track function can increate the insight of policy-based routing in the change of networks. When the device perceives that the next hop for forwarding failed, policy-based routing will rapidly hand the traffic over to the next valid next hop (in redundant backup mode) or all other valid next hops (in load balancing mode).

For track configuration, refer to Rns&track *Configuration Guide*. IPv6 PBR does not support linkup with track.

7.1.4 Enable BFD Function

Linkup of policy-based routing and BFD avoids setting the policy-based routing as forwarding path when it is not reachable. If the backup forwarding path is available, the system rapidly hands over to this path.

7.1.5 VRF Selection using Policy-based Routing

The PBR implementation of the VRF selection feature allows you to filter the packets received on the ports that PBR is applied based on match criteria. Match criteria is defined in an IP access list or based on packet length. Users can balance traffic on different VRF instances as required.

In general, the packets received on an interface of a VRF are routed and forwarded through this VRF. The packets received on an interface of the global routing table are routed and forward through the global routing table. VRF selection using policy based routing can remove this limit. This feature supports VRF successor route, the route across VRFs and the route from VRF to the global routing table. In VRF successor route, the packets received on an interface of a VRF are routed and forwarded by the routing table of this VRF. In the route across VRFs mode, the packets received on an interface of a VRF are routed and forwarded by the routing table of another VRF. In the route from VRF to the global routing table mode, the packets received on an interface of a VRF are routed and forwarded by the global routing table.

7.1.6 Operation Principles

For policy-based routing, first of all, you need to define a route map used to

specify the policy on packet forwarding. The route map consists of a set of statements with permit or deny action.

Secondly, define a set of **set** statements in the route map to forward and control packets in order.

Finally, apply the policy-based routing at the inbounding direction. If the policy-based routing is applied at the outbounding direction, packets are forwarded by common routes.

For routers, outgoing packets can be processed by the specific policy-based routing, not the common routing table.

7.2 Default Configurations

Below describes the default configurations of policy-based routing.

Function	Default value
Load balance of many next hops	Redundancy (redundant backup)
Next hop WCMP weight	1

7.3 Configure IPv4 Policy-based Routing

You need to set a route map for the policy-based routing and create the route map before applying the policy-based routing. A route map consists of many policies with corresponding sequences. The smaller the sequence, the higher the policy is. Each policy consists of one or more **match** statements and corresponding one or more **set** statements. The **match** statement defines the matching rule of IPv4/v6 packets, and the **set** statement defines the processing rules of matched IPv4/v6 packets. In the course of policy-based routing, packets are matched by priorities in descending order. Once a policy is matched, the system performs corresponding actions and quits policy-based routing.

There is one kind of match statement. **match ip address** matches packets by ACL. For a policy, you can configure many **match ip address** statements.

Similarly, there are two types of set statements. Type 1 modifies the QoS field of IP packet, for instance, **set ip tos**, **set ip precedence** and **set ip dscp**. Type 2 controls IP packet, for instance, **set vrf**, **set ip nexthop** and **set ip default nexthop**. Once all match rules are met, Type 1 set statements must be executed and Type 2 set statements are executed by priority in the following order:

set vrf: Set policy-based routing as the VRF instance for IP packet routing with the priority higher than common route. The command is mutually exclusive with **set ip [default] nexthop**. The IPv4 packets received on the interface that meet match rules will be routed by the routing table of the VRF instance specified by

this command, no matter whether the VRF is the same as the one the interface belongs to.

set ip nexthop: Set next hop of policy-based routing with the priority higher than common route. This command takes precedence over the following command. The IPv4 packets received on the interface that meet match rules will be firstly forwarded to the next hop specified by the **set ip nexthop** command, no matter whether the real routing of IPv4 packets in the routing table is the same as the one specified by the policy-based routing.

set ip default nexthop: Set the policy-based routing with the priority higher than default route but lower than common route. The IPv4 packets received on the interface that meet match rules will be forwarded to the default next hop in case of routing failure or default route.

When you configure the routing map, you can specify the match mode of a policy as permit or deny, which is described as below:

Permit: Apply the corresponding **set** rule to the IPv4/v6 packets meeting the match rules of the policy. If no match rule is met, the system applies the next policy to packets.

Deny: If IPv4/v6 packets meet all **match** statements, the system performs common routing rather than policy-based routing.

IPv4/IPv6 packets are matched by the priority of every policy of the routing map in descending order. If the packets do not match any policy of the routing map, the system performs common routing.

The next hop specified by the **set ip nexthop** command is used for forwarding only when its tracking object is active.

To configure a policy-based routing, do the following steps:

7.3.1 Configuring route map

Step 1 Define an ACL.

Command	Function
DES-7200(config)# **ip access-list** {**extended** | **standard**} {*id* | *name*}	Define an ACL as the matching rule of IP packets.

Step 2 Define a route map, which consists of many policies in sequence order. When a policy is matched, the system quits the execution of the route map.

Command	Function

DES-7200(config)# **route-map** *route-map-name* [**permit** | **deny**] *sequence*	Define a route map.

Step 3 Define the match rule of every policy of the route map.

Command	Function
DES-7200(config-route-map)# **match ip address** {*access-list-number* | *access-list-name*}	Match the address in the ACL.

Step 4 Define the action after meeting match rule.

Command	Function
DES-7200(config-route-map)# **set vrf** *name*	Route the packets matching PBR by the routing table of the specific VRF instance.
DES-7200(config-route-map)# **set ip next-hop** *ip-address* [*weight*][*ip-address*[*weight*]]	Set the next hop IP address of packets.
DES-7200(config-route-map)# **set ip default next-hop** *ip-address*[*weight*] [*ip-address*[*weight*]]	Set the default next hop IP address for the packets without route.
DES-7200(config-route-map)# **set ip precedence**	Modify the priority of IP packet.
DES-7200(config-route-map)# **set ip tos**	Modify the ToS value of IP packet.
DES-7200(config-route-map)# **set ip dscp**	Modify the DSCP value of IP packet.

1 The **set vrf** and **set ip [default] nexthop** commands cannot be configured simultaneously for a policy. But the **set vrf** command can be configured with other set statements. The VRF must exist when you configure the VRF of policy-based routing or otherwise the system prompts configuration failure.

2 The **set ip dscp**, **set ip tos** and **set ip precedence** commands cannot be configured simultaneously for a policy or otherwise the corresponding domains of IP packet may be different than the expectation.

Caution

3 The **set vrf** and **set ip nexthop** commands take precedence over common route. IP packets matching policy-based routing are forwarded by policy-based routing, but the IP packets not matching the policy-based routing are forwarded by common routes.

4 The **set default ip nexthop** commands are lower than common route in terms of priority. IP packets are forwarding by policy-based routing only after common route failed.

7.3.2 Apply the route map

To apply the policy-based routing on the interface, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)**# ip policy route-map** *name*	Apply policy-based routing on the interface.

To apply the policy-based routing on local device, run the following command in the global configuration mode.

Command	Function
DES-7200(config)**# ip local policy route-map** [*name*]	Apply the policy-based routing to the packets from local device.

For example:

Configure policy-based routing on Fastethernet 0/0 so that all incoming packets are forwarded to the device whose next hop is 192.168.5.5.

```
DES-7200(config)# access-list 1 permit any
DES-7200(config)# route-map name
DES-7200(config-route-map)# match ip address 1
DES-7200(config-route-map)# set ip next-hop 192.168.5.5
DES-7200(config-route-map)# int fastethernet 0/0
DES-7200(config-if)# ip policy route-map name
```

7.3.3 Configuring load balancing mode

In redundant backup mode, the policy-based routing will automatically hand over the next valid next hop when the active next hop fails. In load balancing mode, on contrary, the traffic will be balanced on other valid next hop when the active next hop fails.

To configure load balance or redundant backup, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **ip policy** {**load-balance** | **redundance**}	Configure load balance or redundant backup for policy-based routing forwarding.
DES-7200(config)# **no ip policy**	Remove the configuration.

Caution

In load balancing mode, WCMP (Weighted Cost Multiple Path) supports up to 4 next hops and ECMP (Equal Cost Multiple Path) supports up to 32 next hops.

For default policy-based routing, WCMP (Weighted Cost Multiple Path) supports up to 4 next hops and ECMP (Equal Cost Multiple Path) supports up to 32 next hops.

In redundant backup mode, the first resolved next hop takes effect. If all next hops are not resolved, the packets matching policy-based routing are dropped. If the originally unresolved next hop of higher priority than active next hop is resolved, the system hands over to this next hop.

7.4 Configure IPv6 Policy-based Routing

Command	Function
DES-7200**#configure terminal**	Enter the global configuration mode.
DES-7200(config)**#ipv6 access-list** *access-list-name*	Create an IPv6 ACL.
DES-7200(config)**#route-map** *route-map-name* [**permit** | **deny**] *sequence*	Create a route map.
DES-7200 (config-route-map)**#match ipv6 address** *access-list-name*	Match the IPv6 address in ACL.

DES-7200 (config-route-map)**#set ipv6 next-hop** *global-ipv6-address* [*weight*][*global-ipv6-address* [*weight*]] [*global-ipv6-address...*]	Set the next hop IPv6 address of packets.
Or: DES-7200 (config-route-map)**#set ipv6 default next-hop** *global-ipv6-address* [*weight*][*global-ipv6-address* [*weight*]] [*global-ipv6-address...*]	Specify the next hop IPv6 address for the packets without obvious routes in the routing table.
DES-7200 (config)**#interface** *interface-type interface-number*	Enter the interface configuration mode.
DES-7200 (config-if- *interface-type interface-number*)**#ipv6 policy route-map** *route-map-name*	Apply policy-based routing on the interface.
Or: DES-7200 (config-if- *interface-type interface-number*)**#no pv6 policy route-map**	Remove the policy-based routing applied on the interface.
DES-7200(config)**#Ipv6 policy** [**load-balance** | **redundance**]	Configure load balance mode.
DES-7200**#show ipv6 policy**	Show the configuration of policy-based routing.
Or: DES-7200**#show route-map**	Show the configuration of route map.
Or: DES-7200**#show access-lists**	Show the configuration of ACL.

7.5 Configuration Example

7.5.1 Example 1: Source address based PBR

Network requirement

There are two egresses of a LAN connecting to the Internet. In general, load balance and backup should be enabled for these two egresses. All streams from subnet 1 to the Internet are transmitted through GigabitEthernet 0/1 and all streams from subnet 2 to the Internet are transmitted through GigabitEthernet 0/2. If GigabitEthernet 0/1 is disconnected, the data streams on this interface should be transferred to GigabitEthernet 0/2, and vice versa.

Network topology

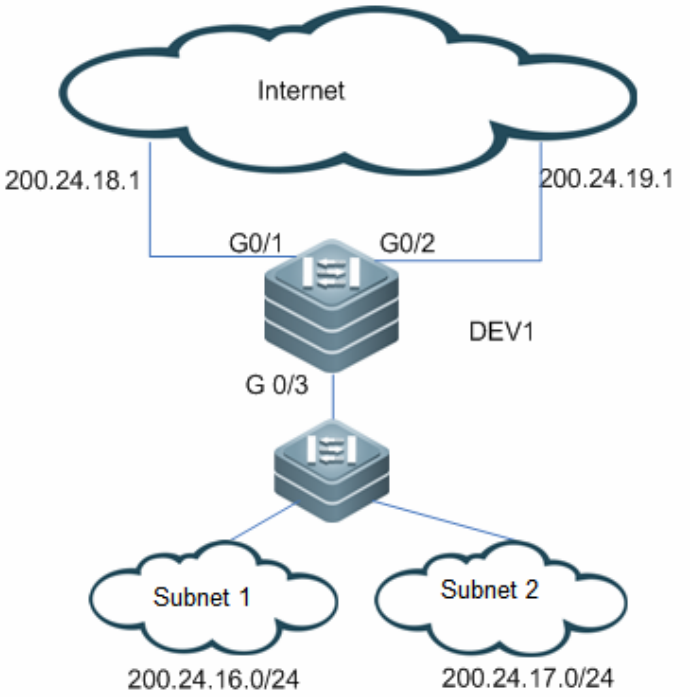


Figure 5 Network topology

As shown in the Figure-1, DEV1 connects to subnets 1 and 2 through G0/3, and connects to the Internet through G0/1 and G0/2 with the next hop of 200.24.18.1 and 200.24.19.1, respectively. Subnet 1's segment is 200.24.16/20 and subnet 2's segment is 200.25.19.1.

Configuration steps

Create an ACL for subnet 1 and subnet 2, respectively.

```
DES-7200(config)#access-list 1 permit 200.24.16.0 0.0.0.255
DES-7200(config)#access-list 2 permit 200.24.17.0 0.0.0.255
```

Configure a route map used to control data streams of subnet 1. Set the next hop of G0/1 prefer.

```
DES-7200(config)#route-map RM_FOR_PBR 10
DES-7200(config-route-map)#match ip address 1
DES-7200(config-route-map)#set ip nexthop 200.24.18.1
DES-7200(config-route-map)#set ip nexthop 200.24.19.1
```

Configure a route map used to control data streams of subnet 2. Set the next hop of G0/2 prefer.

```
DES-7200(config)#route-map RM_FOR_PBR 20
DES-7200(config-route-map)#match ip address 2
DES-7200(config-route-map)#set ip nexthop 200.24.19.1
DES-7200(config-route-map)#set ip nexthop 200.24.18.1
```

Configure redundant backup.

```
DES-7200(config)#ip policy redundance
```

Apply policy-based routing on GigabitEthernet 0/3.

```
DES-7200(config)#interface GigabitEthernet 0/3
DES-7200(config-if)#ip policy route-map RM_FOR_PBR
```

7.5.2 Example 2: Enable Track function.

Network requirement

There are two egresses of a LAN connecting to the Internet. In general, load balance and backup should be enabled for these two egresses. All streams from subnet 1 to the Internet are transmitted through GigabitEthernet 0/1 and all streams from subnet 2 to the Internet are transmitted through GigabitEthernet 0/2. If the next hop 200.24.18.1 fails, the data streams on this interface should be transferred to GigabitEthernet 0/2, and vice versa.

Network topology

As shown in Figure 1.

Configuration steps

Track GigabitEthernet 0/1's next hop 200.24.18.1.

```
DES-7200(config)#ip rns 1
DES-7200(config-ip-rns)#icmp-echo destination-hostname 200.24.18.1
DES-7200(config)#track 1 rns 1
```

Track GigabitEthernet 0/2's next hop 200.24.19.1.

```
DES-7200(config)#ip rns 2
DES-7200(config-ip-rns)#icmp-echo destination-hostname 200.24.19.1
DES-7200(config)#track 2 rns 2
```

Enable track function.

```
DES-7200(config)#route-map RM_FOR_PBR 10
DES-7200(config-route-map)#match ip address 1
DES-7200(config-route-map)#set ip nexthop verify-availability 200.24.18.1
track 1
DES-7200(config-route-map)#set ip nexthop verify-availability 200.24.19.1
track 2
```

Configure a route map used to control data streams of subnet 2. Set the next hop of G0/2 prefer.

```
DES-7200(config)#route-map RM_FOR_PBR 20
```

```
DES-7200(config-route-map)#match ip address 1
DES-7200(config-route-map)#set ip nexthop verify-availability 200.24.19.1
track 2
DES-7200(config-route-map)#set ip nexthop verify-availability 200.24.18.1
track 1
```

Configure redundant backup.

```
DES-7200(config)#ip policy redundance
```

Apply policy-based routing on GigabitEthernet 0/3.

```
DES-7200(config)#interface GigabitEthernet 0/3
DES-7200(config-if)#ip policy route-map RM_FOR_PBR
```

7.5.3 Example 3: Configure VRF selection using PBR

Network requirement

A provider edge needs to apply policy-based routing for the packets received from **FastEthernet** *0/1*. It routes the IP packets from subnet 1 by VRF1, the IP packets from subnet 2 by VRF2, and the IP packets from subnet 3 by VRF3. Other packets are routed in the public network.

Configuration steps

Create VRF instances.

```
DES-7200(config)#ip vrf VRF1
DES-7200(config)#ip vrf VRF2
DES-7200(config)#ip vrf VRF3
```

Create ACLs.

```
DES-7200(config)#access-list 1 permit 192.168.195.0 0.0.0.255
DES-7200(config)#access-list 2 permit 192.168.196.0 0.0.0.255
DES-7200(config)#access-list 3 permit 192.168.197.0 0.0.0.255
```

Create route maps.

```
DES-7200(config)#route-map PBR-VRF-Selection permit 10
DES-7200(config-route-map)#match ip address 1
DES-7200(config-route-map)#set vrf VRF1

DES-7200(config)#route-map PBR-VRF-Selection permit 20
DES-7200(config-route-map)#match ip address 2
DES-7200(config-route-map)#set vrf VRF2

DES-7200(config)#route-map PBR-VRF-Selection permit 30
DES-7200(config-route-map)#match ip address 3
```

```
DES-7200(config-route-map)#set vrf VRF3
```

Import IP address of the interface to VRFs 1 to 3.

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#ip address 192.168.195.1 255.255.255.0
DES-7200(config-if)#ip vrf receive VRF1
DES-7200(config-if)#ip vrf receive VRF2
DES-7200(config-if)#ip vrf receive VRF3
```

Apply the policy-based routing on the interface.

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#ip policy route-map PBR-VRF-Selection
```

7.5.4 Example 4: Apply IPv6 policy-based routing on the interface

Network requirement

There are two egresses of a LAN connecting to the Internet. In general, load balance and backup should be enabled for these two egresses. All streams from subnet 1 to the Internet are transmitted through GigabitEthernet 0/1 and all streams from subnet 2 to the Internet are transmitted through GigabitEthernet 0/2. If GigabitEthernet 0/1 is disconnected, the data streams on this interface should be transferred to GigabitEthernet 0/2, and vice versa.

Network topology

As shown in Figure 2, Device1 connects to subnets 1 and 2 through G0/3 (routed port), and connects to the Internet through G0/1 and G0/2 with the next hop of 2001::1/64 and 2002::1/64, respectively. Subnet 1's segment is 2003::/64 and subnet 2's segment is 2004::/64.

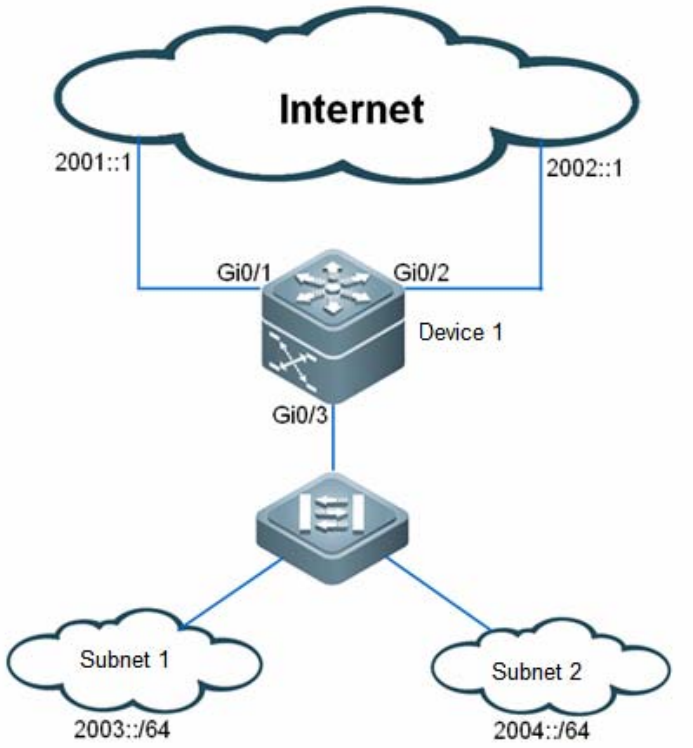


Figure 2 IPV6 PBR topology

Configuration steps

Create an ACL for subnet 1 and subnet 2, respectively.

```
DES-7200(config)#ipv6 access-list net1
DES-7200(config-ipv6-acl)#permit ipv6 2003::/64 any
DES-7200(config)#ipv6 access-list net2
DES-7200(config-ipv6-acl)#permit ipv6 2004::/64 any
```

Configure a route map used to control data streams of subnet 1. Set the next hop of G0/1 prefer.

```
DES-7200(config)#route-map RM_FOR_PBR 10
DES-7200(config-route-map)#match ipv6 address net1
DES-7200(config-route-map)#set ipv6 next-hop 2001::1
DES-7200(config-route-map)#set ipv6 next-hop 2002::1
```

Configure a route map used to control data streams of subnet 2. Set the next hop of G0/2 prefer.

```
DES-7200(config)#route-map RM_FOR_PBR 20
DES-7200(config-route-map)#match ipv6 address net2
DES-7200(config-route-map)#set ipv6 next-hop 2002::1
DES-7200(config-route-map)#set ipv6 next-hop 2001::1
```

Configure redundant backup.

```
DES-7200(config)#ipv6 policy redundance
```

Apply the policy-based routing on the interface GigabitEthernet 0/3.

```
DES-7200(config)#interface GigabitEthernet 0/3
DES-7200(config-if-GigabitEthernet 0/3)#ipv6 policy route-map RM_FOR_PBR
```

Verify configuration

Show the configuration of route map.

```
DES-7200#show route-map
route-map RM_FOR_PBR, permit, sequence 10
  Match clauses:
    ipv6 address net1
  Set clauses:
    ipv6 next-hop 2001::1 2002::1
route-map RM_FOR_PBR, permit, sequence 20
  Match clauses:
    ipv6 address net2
  Set clauses:
ipv6 next-hop 2002::1 2001::1
```

Show the configuration of IPv6 policy-based routing.

```
DES-7200#show ipv6 policy
Interface                          Route map
GigabitEthernet 0/3                RM_FOR_PBR

# Show the configuration of ACL.
DES-7200#show access-lists
ipv6 access-list net1
 10 permit ipv6 2003::/64 any
 (0 packets matched)
ipv6 access-list net2
 10 permit ipv6 2004::/64 any
 (0 packets matched)
```

7.5.5 Example 5: Configure IPv4/IPv6 PBRs simultaneously

Network requirement

There are two egresses of a LAN connecting to the Internet, one of which is the egress of education network. In general, load balance and backup should be enabled for these two egresses.

IPv4/IPv6 dual stacks are used in the networks. IPv4 and IPv6 PBRs should be enabled on an interface at the same time.

All streams from the IPv4 education network of subnet 1 to the Internet are transmitted through the egress of education network.

All streams from the IPv4 education network of subnet 2 to the Internet are transmitted through the egress of the Internet.

All streams from the IPv6 education network of subnet 1 to the Internet are transmitted through GigabitEthernet 0/1.

All streams from the IPv6 education network of subnet 2 to the Internet are transmitted through GigabitEthernet 0/2.

Internal interactive data, for example, the data from subnet 1 to subnet 2, is transmitted internal dynamic route rather than policy-based routing.

By default, data streams are transmitted through the egress of the Internet by default route.

If GigabitEthernet 0/1 fails, the data streams on the interface are switched over to GigabitEthernet 0/2, and vice versa.

Network topology

As shown in Figure 3, Device 1 connects to subnets 1 and 2 through G0/3 (routed port), and connects to the Internet through G0/1 and G0/2 with the next hop of 2001::1/64(210.82.12.1) and 2002::1/64(59.78.184.1), respectively. Subnet 1's segment is 2003::/64 (202.112.144.0/25) and subnet 2's segment is 2004::/64(218.62.95.0/24).

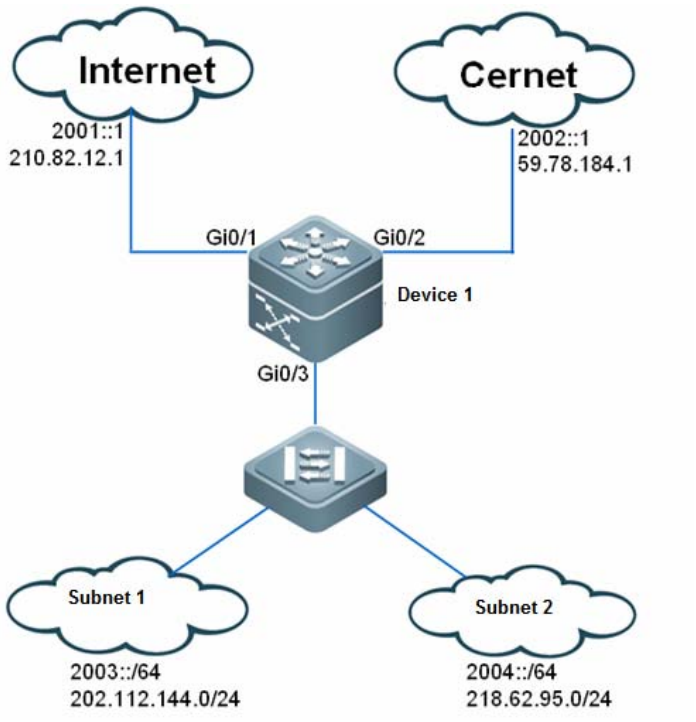


Figure 3 IPv4/IPv6 PBR topology

Configuration steps

Create an IPv4 ACL for subnet 1 and subnet 2, respectively.

```
DES-7200(config)#ip access-list extended 101
DES-7200(config-ip-acl)#permit ip 202.112.144.0 0.0.0.255 any
DES-7200(config)#ip access-list extended 102
DES-7200(config-ip-acl)#permit ip 218.62.95.0 0.0.0.255 any
```

Create an IPv6 ACL for subnet 1 and subnet 2, respectively.

```
DES-7200(config)#ipv6 access-list net1
DES-7200(config-ipv6-acl)#permit ipv6 2003::/64 any
DES-7200(config)#ipv6 access-list net2
DES-7200(config-ipv6-acl)#permit ipv6 2004::/64 any
```

Configure a route map used to control data streams of subnet 1. Set the next hop of G0/1 prefer.

```
DES-7200(config)#route-map RM_FOR_PBR 10
DES-7200(config-route-map)#match ip address 101
DES-7200(config-route-map)#set ip default next-hop 59.78.184.1
DES-7200(config-route-map)#set ip default next-hop 210.82.12.1

DES-7200(config-route-map)#match ipv6 address net1
DES-7200(config-route-map)#set ipv6 next-hop 2001::1
DES-7200(config-route-map)#set ipv6 next-hop 2002::1
```

Configure a route map used to control data streams of subnet 2. Set the next hop of G0/2 prefer.

```
DES-7200(config)#route-map RM_FOR_PBR 20
DES-7200(config-route-map)#match ip address 102
DES-7200(config-route-map)#set ip default next-hop 210.82.12.1
DES-7200(config-route-map)#set ip default next-hop 59.78.184.1

DES-7200(config)#route-map RM_FOR_PBR 20
DES-7200(config-route-map)#match ipv6 address net2
DES-7200(config-route-map)#set ipv6 next-hop 2002::1
DES-7200(config-route-map)#set ipv6 next-hop 2001::1
```

Configure redundant backup.

```
DES-7200(config)#ipv6 policy redundance
```

Apply the policy-based routing on the interface GigabitEthernet 0/3.

```
DES-7200(config)#interface GigabitEthernet 0/3
DES-7200(config-if-GigabitEthernet 0/3)#ip policy route-map RM_FOR_PBR
DES-7200(config-if-GigabitEthernet 0/3)#ipv6 policy route-map RM_FOR_PBR
```

Verify configuration

Show the configuration of route map.

```
DES-7200#show route-map
route-map RM_FOR_PBR, permit, sequence 10
  Match clauses:
    ip address 101
    ipv6 address net1
  Set clauses:
    ipv6 next-hop 2001::1 2002::1
    ip default next-hop 59.78.184.1 210.82.12.1
route-map RM_FOR_PBR, permit, sequence 20
  Match clauses:
    ip address  102
    ipv6 address net2
  Set clauses:
    ipv6 next-hop 2002::1 2001::1
    ip default next-hop 210.82.12.1 59.78.184.1
```

Show the configuration of IPv6 policy-based routing.

```
DES-7200#show ipv6 policy
Interface                          Route map
GigabitEthernet 0/3                 RM_FOR_PBR

# Show the configuration of IPv4 policy-based routing.
DES-7200#show ip policy
Interface                          Route map
GigabitEthernet 0/3                 RM_FOR_PBR
```

Show the configuration of ACLs.

```
DES-7200#show access-lists
Extended IP access list 101
    10 permit ip 202.112.144.0 0.0.0.255 any
Extended IP access list 102
    10 permit ip 218.62.95.0 0.0.0.255 any
IPv6 access list net1
    permit ipv6 2003::/64 any sequence 10
IPv6 access list net2
    permit ipv6 2004::/64 any sequence 10
```

8 VRF Configuration

8.1 VRF Overview

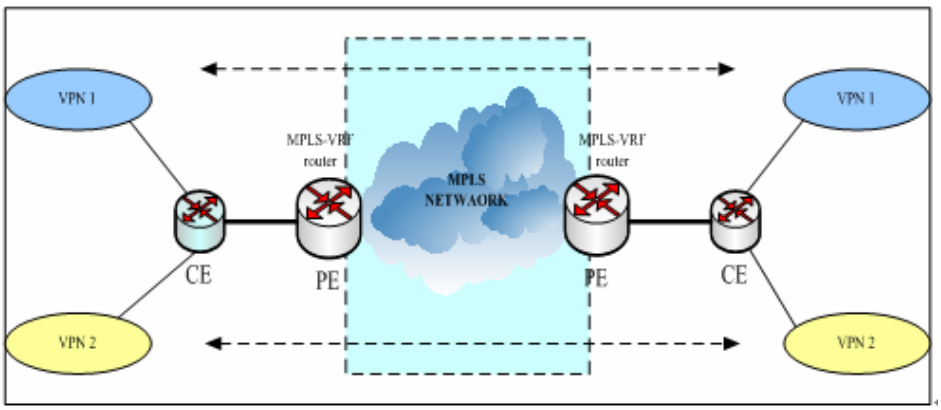
Virtual Private Networks (VPNs) provides a secure way to share bandwidth in the backbone of ISP. One VPN is the collection of the sites sharing routes, which connect to the vendor network through one to multiple interface link, with one VPN routing tabel associated with one interface. The VPN routing table is also referred to as VPN routing/forwarding table.

VRF-lite, also known as multi-VRF CE, or multi-VRF Customer Edge Device, supports multiple VPN routing forwarding instances.

8.2 Working Principle of VRF-lite

VRF-lite mainly includes the following devices:

- Customer edge (CE) devices provide customer access to multiple provider edge (PE) routers. The CE device advertises the site's local routes to the PE router and learns the remote VPN routes from it.
- Provider edge (PE) routers exchange routing information with CE devices by using static routing or dynamic routing protocols (BGP, RIP or OSPF).
- A PE device may have multiple interfaces belonging to a same VPN. PE devices exchange VPN routing information through BGP protocol.
- PE devices are independent of the features of CE devices.
- P device doesn't handle VPN information, namely VPN information is transparent to P device.



VRF-lite Typical Application Model

The packet-forwarding process in a VRF-lite enabled network is shown below:

- When the CE receives a packet from a VPN, it looks up the relevant VRF routing table based on the input interface. When a route is found, the CE forwards the packet to the PE.
- When the ingress PE receives a packet from the CE, it performs a VRF lookup. When a route is found, the router adds a corresponding MPLS label to the packet and sends it to the MPLS network.
- When an egress PE receives a MPLS packet from the MPLS network, it strips the MPLS label and uses the label to identify the correct VPN routing table. Then the egress PE performs the normal route lookup. When a route is found, it forwards the packet to the correct adjacency.
- When a CE receives a packet from an egress PE, it uses the input interface to look up the correct VPN routing table. If a route is found, the CE forwards the packet within the VPN.

8.3 VRF Configuration Task

VRF-Lite usage guidance:

- CE supports multiple users using VRF-lite. Each user owns its routing table;
- Users may use the same IP address (which is not supported at present);
- Many users share the physical lines between CE and PE in many ways via multiple logic interfaces;
- VRF-Lite does not support MPLS-VRF function, which mainly plays a role in CE end;
- On the PE, connections of multiple CEs is similar to using VRF-lite;
- It is recommended to use EBGP for the route interaction between PE and CE. It will be more complicated if use OSPF, RIP, static routing to achieve the route interaction. If you are using OSPF routing interactions, need to be carefully configured, It is recommended to use the capability vrf-lite function when using the OSPF for the route interaction.

8.3.1 Creating VRF

Command	Function
DES-7200(config)# **ip vrf** *vrf-name*	Create VRF. *vrf-name* shall not exceed 31 characters.

Command	Function
DES-7200(config)# **no ip vrf** *vrf-name*	Remove VRF.

8.3.2 Enabling VRF on the Interface

Command	Function
DES-7200(config-if)# **ip vrf forwarding** *vrf-name*	If you don't need to enable IPv6 on the interface, you can associate the interface to single-protocol IPv4 VRF. If you need to enable IPv6 on the interface, you are not suggested to use this command to associate the interface with single-protocol IPv4 VRF.
DES-7200(config-if)# **no ip vrf forwarding** *vrf-name*	Remove the interface from single-protocol IPv4 VRF.

By default, the interface doesn't belong to any VRF; it belongs to the global routing table.

Caution

（1） After associating the interface with the single-protocol VRF supporting IPv4 only, the IPv4 address configured on the original interface will be removed, and the IPv6 address configured on the interface won't be compromised.

（2） On layer-3 switch supporting VRF, if you associate the interface with single-protocol IPv4 VRF and enable IPv6 protocol on this interface at the same time, the switch won't be able to forward the IPv6 packets received on the interface.

8.3.3 Configuring Routing Protocol

Command	Function
DES-7200(config)# **ip route vrf** *vrf-name network mask interface nexthop*	Add the static route.
DES-7200(config-if)# **no ip route vrf** *vrf-name* **network** *mask*	Delete the static route.

The routing protocol can also be used.

8.4 VRF-lite Configuration Example

As shown in Figure-2, CE accesses to 2 VPNs: vpn1 and vpn2.

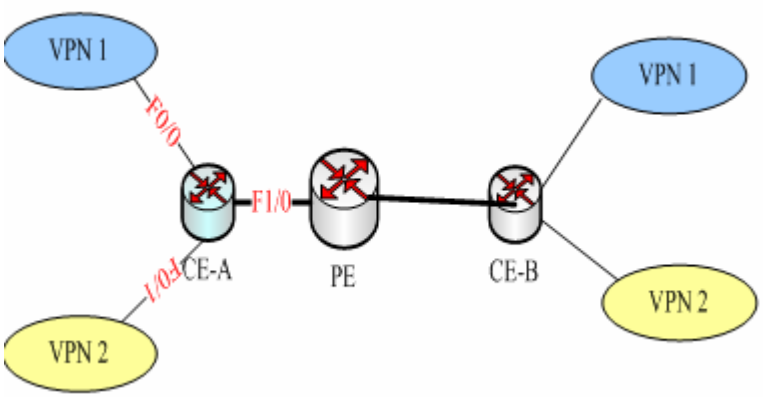


Figure-2

CE-A

```
DES-7200# hostname CE-A
CE-A# configure terminal
```

Create VRF

```
CE-A(config)# ip vrf vpn1
CE-A(config)# ip vrf vpn2
```

Enable VRF on the interface

```
CE-A(config)# interface f0/0
CE-A(config-if)#description connecting-to-vpn1
CE-A(config-if)# ip vrf forwarding vpn1
CE-A(config-if)# ip address 192.168.4.1 255.255.255.0
CE-A(config)# interface f0/1
CE-A(config-if)# ip vrf forwarding vpn2
CE-A(config-if)# ip address 192.168.5.1 255.255.255.0
CE-A(config-if)#description  connecting-to-vpn2
CE-A(config)# interface f1/0
CE-A(config-if)#  no ip address
CE-A(config)# interface f1/0.10
CE-A(config-if)# encapsulation dot1Q 10
CE-A(config-if)# ip vrf forwarding vpn1
CE-A(config-if)# ip address 10.10.1.1 255.255.255.0
CE-A(config)# interface f1/0.20
CE-A(config-if)# encapsulation dot1Q 20
CE-A(config-if)# ip vrf forwarding vpn2
CE-A(config-if)# ip address 10.10.2.1 255.255.255.0
```

Set the VRF static route

```
CE-A(config)# ip route vrf vpn1 192.168.44.0 255.255.255.0 10.10.1.2
CE-A(config)# ip route vrf vpn1 192.168.55.0 255.255.255.0 10.10.2.2
```

CE-B

```
DES-7200# hostname CE-B
CE-B# configure terminal
```

Create VRF

```
CE-B(config)# ip vrf vpn1
CE-B(config)# ip vrf vpn2
```

Enable VRF on the interface

```
CE-B(config)# interface f0/0
CE-Bconfig-if)# ip vrf forwarding vpn1
CE-B(config-if)# ip address 192.168.44.1 255.255.255.0
CE-B(config-if)# description  connecting-to-vpn1
CE-B(config)# interface f0/1
CE-B(config-if)# ip vrf forwarding vpn2
CE-B(config-if)# ip address 192.168.55.1 255.255.255.0
CE-Bconfig-if)# description  connecting-to-vpn2
CE-B(config)# interface f1/0
CE-B(config-if)#  no ip address
CE-B(config)# interface f1/0.10
CE-B(config-if)# encapsulation dot1Q 100
CE-B(config-if)# ip vrf forwarding vpn1
CE-B(config-if)# ip address 172.10.1.1 255.255.255.0
CE-B(config)# interface f1/0.20
CE-B(config-if)# encapsulation dot1Q 200
CE-B(config-if)# ip vrf forwarding vpn2
CE-B(config-if)# ip address 172.10.2.1 255.255.255.0
```

Set the VRF static route

```
CE-B(config)# ip route vrf vpn1 192.168.4.0 255.255.255.0 172.10.1.2
CE-B(config)# ip route vrf vpn1 192.168.5.0 255.255.255.0 172.10.2.2
```

PE

```
Router# configure terminal
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit
Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit
```

```
Router(config)# ip cef
Router(config)# interface Fast Ethernet0/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 10.10.1.2 255.255.255.0
Router(config-if)# exit
Router(config)# interface Fast Ethernet0/0.100
Router(config-if)# encapsulation dot1q 100
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 172.10.1.2 255.255.255.0
Router(config-if)# exit
Router(config)# interface Fast Ethernet0/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 10.10.2.2 255.255.255.0
Router(config-if)# exit
Router(config)# interface Fast Ethernet0/0.200
Router(config-if)# encapsulation dot1q 200
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 172.10.2.2 255.255.255.0
Router(config-if)# exit
Router(config)# ip route vrf v1 192.168.4.0 255.255.255.0 10.10.1.1
Router(config)# ip route vrf v1 192.168.44.0 255.255.255.0 172.10.1.1
Router(config)# ip route vrf v2 192.168.5.0 255.255.255.0 10.10.2.1
Router(config)# ip route vrf v2 192.168.55.0 255.255.255.0 172.10.2.1
```

8.5 VRF Debugging

Use the following command to view the routing table in the VRF:

Command	Function
DES-7200# **show ip route vrf** *vrf-name*	Show the route in the specified VRF.

Use the following command to clear the routing table in the VRF:

Command	Function
DES-7200# **clear ip route vrf** *vrf-name*	Clear the route in the specified VRF.

Use the following command to view the VRF:

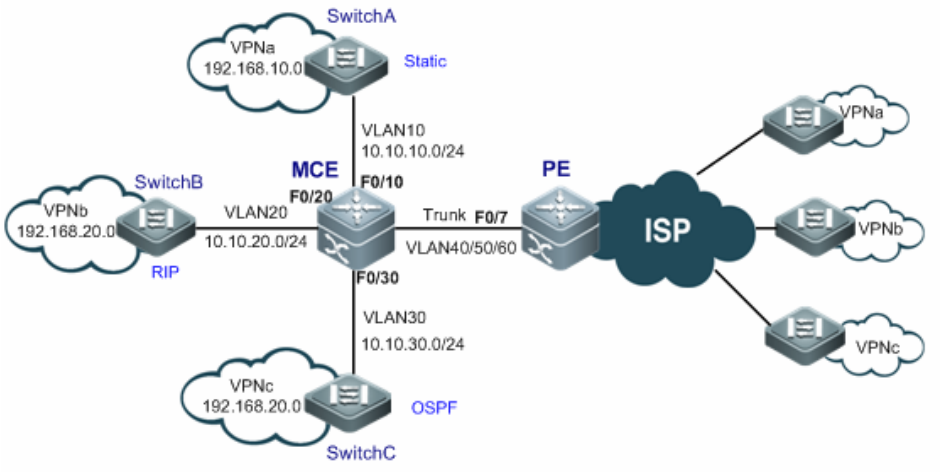
Command	Function
DES-7200# **show ip vrf** [*vrf-name*]	Show the information about VRF with IPv4 enabled.

8.6 Typical MCE Configuration Example

Topological Diagram

As shown below, different sites of VPNa, VPNb and VPNc need to exchange information across the backbone network.

- Each VPN site accesses PE through MCE device.
- Configure a static route between MCE device and VPNa; configure RIP protocol between MCE and VPNb to exchange routes; configure OSPF protocol between MCE and VPNc to exchange routes.



Topological diagram for typical MCE application

Application Requirements

- It is required that MCE device shall be able to isolate the routes of respective VPNs, and advertise the routes of respective VPNs to PE device by configuring static routing, RIP routing protocol and OSPF routing protocol.
- Overlapped IP addresses are allowed in different VPNs.

Configuration Tips

Configuring multiple VRF instances on MCE and PE device, so that the routes of different VPNs can be isolated from each other. Configurations include the following two steps:

Configure VRF instances and associate with the corresponding interfaces

Interface	Associated VRF	IP address of interface
VPNa-connecting interface of MCE device (SVI 10)	VPNa	10.10.10.3

PE-connecting logical interface of MCE device (SVI 40)	VPNa	10.10.40.1
MCE-connecting logical interface of PE device (SVI 40)	VPNa	10.10.40.2
VPNb-connecting interface of MCE device (SVI 20)	VPNb	10.10.20.3
PE-connecting logical interface of MCE device (SVI 50)	VPNb	10.10.50.1
MCE-connecting logical interface of PE device (SVI 50)	VPNb	10.10.50.2
VPNc-connecting interface of MCE device (SVI 30)	VPNc	10.10.30.3
PE-connecting logical interface of MCE device (SVI 60)	VPNc	10.10.60.1
MCE-connecting logical interface of PE device (SVI 60)	VPNc	10.10.60.2

Configure the mutual routing between MCE, VPN sites and PE device

The VRF instances on MCE correspond to the VRF instances on PE. The routing protocol configured between MCE and PE will advertise VPN routes to PE, which will further advertise such routes to other PEs on the network, thus ensuring the intercommunication between remote VPN sites.

Note

In this example, the VRF instances on MCE use the same routing protocol to exchange routes with VPN sites and PE.

If the VRF instances on MCE uses different routing protocols to exchange routes with VPN sites and PE, in order to advertise the routes of VPN sites to the VRF instances on PE and allow the routes advertised by PE to the VRF instances on MCE to be advertised to VPN sites, the routing protocol used by VRF instances on MCE shall redistribute routes to each other, so that VPN routes can be fully exchanged.

Configuration Steps

1) Configure VRF instances and associate with the corresponding interfaces on MCE and PE device

- Create VRF instance on MCE device

Step 1: Create VRF instances named VPNa, VPNb and VPNc on MCE

```
MCE(config)#ip vrf vpna
MCE(config-vrf)#exit
MCE(config)#ip vrf vpnb
```

```
MCE(config-vrf)#exit
MCE(config)#ip vrf vpnc
MCE(config-vrf)#exit
```

Step 2: Create VLAN10 and join the SwitchA-connecting interface (FastEthernet 0/10) of MCE device into VLAN10

```
MCE(config)#interface fastEthernet 0/10
MCE(config-if-FastEthernet 0/10)#switchport access vlan 10
MCE(config-if-FastEthernet 0/10)#exit
```

Step 3: Associate VLAN10 interface (SVI 10) with VPNa, and configure the IP address of interface SVI 10 as 10.10.10.3/24

```
MCE(config)#interface vlan 10
MCE(config-if-VLAN 10)#ip vrf forwarding vpna
MCE(config-if-VLAN 10)#ip address 10.10.10.3 255.255.255.0
MCE(config-if-VLAN 10)#exit
```

Step 4: Execute similar steps (as shown above) to create VLAN 20 and VLAN 30, associate SwitchB-connecting interface (SVI 20) of MCE device with VPNb and associate SwitchC-connecting interface (SVI 30) of MCE device with VPNc. The IP addresses of SVI 20 and SVI 30 are 10.10.20.3 and 10.10.30.3 respectively.

Step 5: Create VLAN 40, 50 and 60; join PE-connecting interface (FastEthernet 0/7) of MCE device into VLAN 40, 50 and 60, and associate SVI 40 with VPNa, SVI 50 with VPNb and SVI 60 with VPNc. The IP addresses of SVI 40, SVI 50 and SVI 60 are 10.10.40.1, 10.10.50.1 and 10.10.60.1 respectively.

```
MCE(config)#vlan 40
MCE(config-vlan)#exit
MCE(config)#vlan 50
MCE(config-vlan)#exit
MCE(config)#vlan 60
MCE(config-vlan)#exit
MCE(config)#interface fastEthernet 0/7
MCE(config-if-FastEthernet 0/7)#switchport mode trunk
MCE(config-if-FastEthernet 0/7)#exit
MCE(config)#interface vlan 40
MCE(config-if-VLAN 40)#ip vrf forwarding vpna
MCE(config-if-VLAN 40)#ip address 10.10.40.1 255.255.255.0
MCE(config-if-VLAN 40)#exit
MCE(config)#interface vlan 50
MCE(config-if-VLAN 50)#ip vrf forwarding vpnb
MCE(config-if-VLAN 50)#ip address 10.10.50.1 255.255.255.0
MCE(config-if-VLAN 50)#exit
MCE(config)#interface vlan 60
MCE(config-if-VLAN 60)#ip vrf forwarding vpnc
```

```
MCE(config-if-VLAN 60)#ip address 10.10.60.1 255.255.255.0
```

By now, VRF instances have been created on MCE device.

- Create VRF instances on PE device

Step 1: Create VRF instances named VPNa, VPNb and VPNc on PE device (same names as used on MCE device)

```
PE(config)#ip vrf vpna
PE(config-vrf)#exit
PE(config)#ip vrf vpnb
PE(config-vrf)#exit
PE(config)#ip vrf vpnc
PE(config-vrf)# exit
```

Step 2: Create VLAN 40, 50 and 60; join MCE-connecting interface (FastEthernet 0/7) of PE device into VLAN 40, 50 and 60, and associate SVI 40 with VPNa, SVI 50 with VPNb and SVI 60 with VPNc. Steps to create VLANs and join interface into VLANs are omitted here.

```
PE (config)#interface vlan 40
PE(config-if-VLAN 40)#ip vrf forwarding vpna
PE(config-if-VLAN 40)#ip address 10.10.40.2 255.255.255.0
PE(config-if-VLAN 40)#exit
PE(config)#interface vlan 50
PE(config-if-VLAN 50)#ip vrf forwarding vpnb
PE(config-if-VLAN 50)#ip address 10.10.50.2 255.255.255.0
PE(config-if-VLAN 50)#exit
PE(config)#interface vlan 60
PE(config-if-VLAN 60)#ip vrf forwarding vpnc
PE(config-if-VLAN 60)#ip address 10.10.60.2 255.255.255.0
```

By now, VRF instances have been created on PE device.

2) Configure the static route from MCE to VPNa site and PE device

- Configure static route on SwitchA (access device of VPNa site)

The address of the interface connecting SwitchA with MCE is 10.10.10.2/24; the address of interface connecting with VPNa is 192.168.10.1/24. Steps to join interface into VLAN and configure IP address for interface are omitted here.

Configure default route on SwitchA, and specify the next-hop for egress packets as 10.10.10.3.

```
SwitchA(config)#ip route 0.0.0.0 0.0.0.0 10.10.10.3
```

- Configure static route on MCE device

Specify static route on MCE; specify the next hop for packets destined to

192.168.10.0 network segment as 10.10.10.2, and associate this route with VPNa instance.

```
MCE(config)#ip route vrf vpna 192.168.10.0 255.255.255.0 10.10.10.2
```

- Configure static route on PE device

Specify static routes associated with VPNa instance on PE; specify the next hop for packets destined to 192.168.10.0 network segment as 10.10.40.1, and specify the next hop for packets destined to 10.10.10.0 network segment as 10.10.40.1.

```
PE (config)#ip route vrf vpna 192.168.10.0 255.255.255.0 10.10.40.1
PE (config)#ip route vrf vpna 10.10.10.0 255.255.255.0 10.10.40.1
```

3) Configure RIP routing bewteen MCE and VPNb site/PE device

- Configure RIP routing protocol on SwitchB (access device of VPNb site)

The address of the interface connecting SwitchB with MCE is 10.10.20.2/24; the address of interface connecting with VPNb is 192.168.20.1/24. Steps to join interface into VLAN and configure IP address for interface are omitted here.

```
SwitchB(config)#router rip
SwitchB(config-router)#version 2
SwitchB(config-router)#no auto-summary
SwitchB(config-router)#network 10.10.20.0 0.0.0.255
SwitchB(config-router)#network 192.168.20.0 0.0.0.255
```

- Configure RIP routing protocol on MCE device

```
MCE(config)#router rip
MCE(config-router)#address-family ipv4 vrf vpnb
MCE(config-router-af)# version 2
MCE(config-router-af)# no auto-summary
MCE(config-router-af)#network 10.10.20.0 0.0.0.255
MCE(config-router-af)#network 10.10.50.0 0.0.0.255
```

- Configure RIP routing protocol on PE device

```
PE(config)#router rip
PE(config-router)#address-family ipv4 vrf vpnb
PE(config-router-af)# version 2
PE(config-router-af)# no auto-summary
PE(config-router-af)#network 10.10.50.0 0.0.0.255
```

4) Configure OSPF routing between MCE and VPNc site/PE device

- Configure OSPF routing protocol on SwitchC (access device of VPNc site)

The address of the interface connecting SwitchC with MCE is 10.10.30.2/24; the address of interface connecting with VPNb is 192.168.20.1/24. Steps to join

interface into VLAN and configure IP address for interface are omitted here.

```
SwitchC(config)#router ospf 1
SwitchC(config-router)#network 10.10.30.0 0.0.0.255 area 0
SwitchC(config-router)#network 192.168.20.0 0.0.0.255 area 0
```

- Configure OSPF routing protocol on MCE device

```
MCE(config)#router ospf 1 vrf vpnc
MCE(config-router)#network 10.10.30.0 0.0.0.255 area 0
MCE(config-router)#network 10.10.60.0 0.0.0.255 area 0
```

- Configure OSPF routing protocol on PE device

```
PE(config)#router ospf 1 vrf vpnc
PE(config-router)#network 10.10.60.0 0.0.0.255 area 0
```

Verify Configurations

1) Display routing information of VPNa instance

- View routing information on SwitchA (access device of VPNa site)

```
SwitchA (config)#show ip route
Gateway of last resort is 10.10.10.3 to network 0.0.0.0
S*   0.0.0.0/0 [1/0] via 10.10.10.3
C    10.10.10.0/24 is directly connected, VLAN 10
C    10.10.10.2/32 is local host.
C    192.168.10.0/24 is directly connected, FastEthernet 0/23
C    192.168.10.1/32 is local host.
```

- View routing information of VPNa instance on MCE device

```
MCE#show ip route vrf vpna
Routing Table: vpna

C    10.10.10.0/24 is directly connected, VLAN 10
C    10.10.10.3/32 is local host.
C    10.10.40.0/24 is directly connected, VLAN 40
C    10.10.40.1/32 is local host.
S    192.168.10.0/24 [1/0] via 10.10.10.2
```

- View routing information of VPNa instance on PE device

```
PE#show ip route vrf vpna
Routing Table: vpna

S    10.10.10.0/24 [1/0] via 10.10.40.1
C    10.10.40.0/24 is directly connected, VLAN 40
C    10.10.40.2/32 is local host.
```

```
S    192.168.10.0/24 [1/0] via 10.10.40.1
```

2) Display routing information of VPNb instance

- View routing information on SwitchB (access device of VPNb site)

```
SwitchB#show ip route vrf vpnb
Routing Table: vpnb

C    10.10.20.0/24 is directly connected, VLAN 20
C    10.10.20.2/32 is local host.
R    10.10.50.0/24 [120/1] via 10.10.20.3, 00:01:20, VLAN 20
C    192.168.20.0/24 is directly connected, FastEthernet 0/23
C    192.168.20.1/32 is local host.
```

- View routing information of VPNb instance on MCE device

```
MCE#show ip route vrf vpnb

Routing Table: vpnb
C    10.10.20.0/24 is directly connected, VLAN 20
C    10.10.20.3/32 is local host.
C    10.10.50.0/24 is directly connected, VLAN 50
C    10.10.50.1/32 is local host.
R    192.168.20.0/24 [120/1] via 10.10.20.2, 00:22:01, VLAN 20
```

From the above information, we can learn that MCE has learned the private-network routes in VPNb, and maintains the routing information of VPNa and VPNc in three different routing tables, effectively accomplishing VPN isolation and allowing the use of overlapped addresses in different VPNs.

- View routing information of VPNb instance on PE device

```
PE#show ip route vrf vpnb

Routing Table: vpnb
R    10.10.20.0/24 [120/1] via 10.10.50.1, 00:04:48, VLAN 50
C    10.10.50.0/24 is directly connected, VLAN 50
C    10.10.50.2/32 is local host.
R    192.168.20.0/24 [120/2] via 10.10.50.1, 00:02:15, VLAN 50
```

From the above information, we can learn that routing information of VPNb instance have been fully propagated to PE.

3) Display routing information of VPNc instance

- View routing information on SwitchC (access device of VPNc site)

```
SwitchC (config-router)#show ip route
```

```
C    10.10.30.0/24 is directly connected, VLAN 30
C    10.10.30.2/32 is local host.
O    10.10.60.0/24 [110/2] via 10.10.30.3, 00:02:42, VLAN 30
C    192.168.20.0/24 is directly connected, FastEthernet 0/23
C    192.168.20.1/32 is local host.
```

- View routing information of VPNc instance on MCE device

```
MCE#show ip route vrf vpnc

Routing Table: vpnc
C    10.10.30.0/24 is directly connected, VLAN 30
C    10.10.30.3/32 is local host.
C    10.10.60.0/24 is directly connected, VLAN 60
C    10.10.60.1/32 is local host.
O    192.168.20.0/24 [110/2] via 10.10.30.2, 00:01:36, VLAN 30
```

From the above information, we can learn that MCE has learned the private-network routes in VPNc through OSPF, and maintains the routing information of VPNa and VPNb in three different routing tables, effectively accomplishing VPN isolation and allowing the use of overlapped addresses in different VPNs.

- View routing information of VPNc instance on PE device

```
PE#show ip route vrf vpnc

Routing Table: vpnc
O    10.10.30.0/24 [110/2] via 10.10.60.1, 00:00:00, VLAN 60
C    10.10.60.0/24 is directly connected, VLAN 60
C    10.10.60.2/32 is local host.
O    192.168.20.0/24 [110/3] via 10.10.60.1, 00:00:00, VLAN 60
```

From the above information, we can learn that routing information of VPNc instance has been fully propagated to PE.

8.7 Abbreviation

Abbreviation	Description
CE	Customer Edge Device
PE	Provider Edge Device
MCE	Multi-CE
VPN	Virtual Private Network
VRF	VPN Routing and Forwarding Table

DES-7200

Multicast Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

Note

The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products.

The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 IPv4 Multicast Configuration

1.1 Overview

This chapter introduces how to configure the IPv4 multicast routing protocol. For the configuration commands of the multicast routing, please refter to the chapter of *Multicast Routing Configuration Commands*.

The traditional IP transmission only allows the unicast or broadcast communication. But the multicast technology allows one host to send the packets to some other hosts, which are called the group members.

Send the packets to the group member destined to the Class-D network address (224.0.0.0~239.255.255.255). Multicast packets are UDP packets with best effort service. It does not provide reliable transmission and error control as TCP.

The multicast environment consists of senders and receivers. The sender sends multicast packets with a multicast group address used to distinguish different multicast flows. However, only the members of a group can receive the message destined to this group.

Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group. If necessary, a host can be a member of more than one multicast group at a time. Therefore, the active status of a group and the number of group members vary from time to time.

Devices run a multicast routing protocol (such as PIM-DM, PIM-SM, etc.) to maintain their routing tables to forward multicast messages, and use the IGMP to learn the status of the members within a group on their directly attached subnets. A host can join or leave an IGMP group by sending corresponding IGMP Report messages.

IP multicast is ideal for “one-to-multiple” multimedia applications.

1.1.1 IP Multicast Routing Implementation

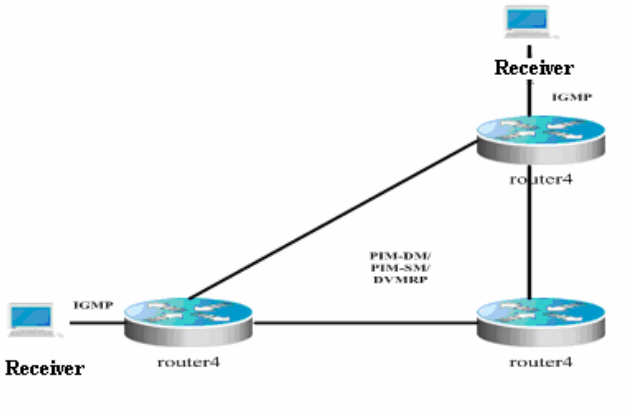
There are the following multicast routing protocols:

- IGMP: Runs between the routers and the hosts in a LAN to track the membership of a group and learn the relation among members.
- PIM-DM: A multicast routing protocol in dense mode, which runs between multicast devices to establish the multicast routing table for forwarding.
- PIM-SM: A multicast routing protocol in sparse mode, which runs between multicast devices to establish the multicast routing table for forwarding.
- DVMRP: Distance Vector Multicast Routing Protocol, which runs between

multicast devices to establish the multicast routing table for forwarding.

The following figure shows the multicast routing protocols used in the IPv4 multicast environment:

Figure 1-1 IP Multicast Routing Protocols within the IP Multicast Environment



1.1.2 RPF Rule

The RPF(Reverse Path Forwarding) check mechanism is used to create the multicast routing entries according to the current unicast routing information, MBGP routing or multicast static routing to ensure the multicast data transmit along the correct path and avoid the various loops.

The following explains the detailed process of searching for the unicast routing table, MBGP routing table and multicast static routing table when using the RPF mechanism:

- **First, select the best routings from the unicast routing table, MBGP routing table and multicast static routing table respectively.**
  - Select the best routing from the unicast routing table for the RPF check:

  Search for the unicast routing table based on the IP address for the source packet as the destination address, and select the best unicast routing.

    - If there is only one next-hop for this unicast routing, you shall check whether the multicast has been enabled on the outbounding interface for the next-hop routing.
      If not, no unicast routing could be used for the RPF check;
      If so, this unicast routing could be used for the RPF check and the corresponding outbounding interface is the RPF interface.
    - If there are multiple next-hops for this unicast routing, all next-hops shall be checked whether the multicast has been enabled on the outbounding interface for the next-hop routing.
      If not, it continues to check the next next-hop routing;
      If so, this unicast routing could be used for the RPF check and the corresponding outbounding interface is the RPF interface.
      However, if the multicast function is not enabled on the outbounding interface for all next-hops, no unicast routing could be used for the RPF check.
    - If there is no best routing, no unicast routing could be used for the RPF check.
  - Select the best routing from the MBGP routing table for the RPF check:

  Search for the MBGP routing table based on the IP address for the source packet

as the destination address, and select the best MBGP routing.

- If there is only one next-hop for this MBGP routing, you shall check whether the multicast has been enabled on the outbounding interface for the next-hop routing.
  If not, no MBGP routing could be used for the RPF check;
  If so, this MBGP routing could be used for the RPF check and the corresponding outbounding interface is the RPF interface.
- If there is no best routing, no MBGP routing could be used for the RPF check.

- Select the best routing from the multicast static routing table for the RPF check:

Search for the multicast static routing table based on the IP address for the source packet as the destination address, and select the best multicast static routing.

- If there is only one next-hop for this multicast static routing, you shall check whether the multicast has been enabled on the outbounding interface for the next-hop routing.
  If not, no multicast static routing could be used for the RPF check;
  If so, you shall check whether there is unicast routing is used for the RPF check.
  - If the next-hop for the multicast static routing does not associate with the unicast protocol number, this multicast static routing could be used for the RPF check.
  - If no unicast routing is used for the RPF check, then the multicast static routing could be used for the RPF check.
  - If the unicast route could be used for the RPF check, and the protocol numbers for this unicast routing and associated next-hop multicast static routing are inconsistent, no multicast static routing could be used for the RPF check.
  - If the unicast route could be used for the RPF check, and the protocol numbers for this unicast routing and associated next-hop multicast static routing are consistent, the multicast static routing could be used for the RPF check.
- If there are multiple next-hops for this multicast static routing, all next-hops shall be checked whether the multicast has been enabled on the outbounding interface for the next-hop routing.
  If not, it continues to check the next next-hop routing;
  If so, you shall check whether there is unicast routing is used for the RPF check.
  - If the next-hop for the multicast static routing does not associate with the unicast protocol number, this multicast static routing could be used for the RPF check.
  - If no unicast routing is used for the RPF check, then the multicast static routing could be used for the RPF check, and the correspondent outbounding interface is the RPF interface.
  - If the unicast route could be used for the RPF check, and the protocol numbers for this unicast routing and associated next-hop multicast static routing are inconsistent, it continues to check the next next-hop routing.
  - If the unicast route could be used for the RPF check, and the protocol numbers for this unicast routing and associated next-hop

multicast static routing are consistent, the multicast static routing could be used for the RPF check, and the correspondent outbounding interface is the RPF interface.

- ◆ If the multicast function is not enabled on the outbounding interface for all next-hops, no multicast static routing could be used for the RPF check.

- If there is no best routing, no multicast static routing could be used for the RPF check.

- **Then, select one routing as the RPF routing from these three best routings.**
  - With the longest-match multicast routing configured, select the longest-match routing from these three routings. If the masks for these three routings are the same, select the routing with the highest priority. If the priority for these routings are the same, select the routing in the sequence of multicast static routing, MBGP routing and unicast routing.
  - Without the longest-match multicast routing configured, select the routing with the highest priority from these three routings. If the priority for these routings are the same, select the routing in the sequence of multicast static routing, MBGP routing and unicast routing.


Caution

1) MBGP routing only depends on the unicast routing for the effective recursiveness. The effectiveness for the MBGP routing does not depend on the distance value. The equivalent routing is not supported for the MBGP protocol.
2) Multicast static routing only depends on the unicast routing for the effective recursiveness. The effectiveness for the multicast static routing does not depend on the distance value.
3) With the unicast routing selected as the RPF routing, the next-hop IP for this unicast routing must be configured. Based on the RPF routing, PIM protocol selects the next-hop IP as the RPF neighbor. Without the next-hop neighbor for the unicast routing configured, PIM protocol fails to obtain the RPF neighbor based on the RPF routing.

1.2 Basic IPv4 Multicast Routing Configuration

1.2.1 Enabling Multicast Routing Forwarding

The multicast protocol can receive and process multicast packets and protocol packets only when the multicast routing forwarding function is enabled.

In the global configuration mode, execute the following command to enable the multicast routing forwarding function:

Command	Function
DES-7200 (config) # **ip multicast-routing**	Enable multicast routing forwarding.
DES-7200 (config) # **no ip multicast-routing**	Disable multicast routing forwarding.


Caution

The multicast routing forwarding function and SVGL mode&IVGL-SVGL mode of IGMP SNOOPING are mutually exclusive. Before enabling the multicast routing forwarding function, please make sure that SVGL mode&IVGL-SVGL mode of IGMP SNOOPING have been disabled. Or it will prompt: `ip multicast-routing conflicts with SVGL mode of IGMP SNOOPING!` he multicast routing forwarding function can be co-used with IVGL mode of IGMP

SNOOPING. The source IP check funciton of IGMP SNOOPING can not be enabled.

1.2.2 Enabling Multicast Routing Protocol

PIM-DM: refer to PIM-DM configuration for the configuration process.

PIM-SM: refer to PIM-SM configuration for the configuration process.

DVMRP: refer to DVMRP configuration for the configuration process.

Note

Only one-mode multicast routing protocol can be enabled on one device.

Caution

After enabling the layer3 multicast on the Private VLAN and Super VLAN, if the multicast source exists in the Sub-VLAN, one more route entry is needed to copy and the ingress is the Sub-VLAN in which the multicast streams enter as the ingress validity check is required when multicast forwarding, resulting in occupying one more multicast hardware entry with 1 less multicast capacity.

1.2.3 Enabling IGMP

Enabling multicast routing forwarding and multicast routing protocol will enable the IGMP function on the interface at the same time.

1.3 Configuring IPv4 Multicast Routing Features

1.3.1 Configuring TTL Threshold

You can configure TTL threshold to limit the TTL of the packets traveling through an interface.

Use the **ip multicast ttl-threshold** command to configure TTL threshold of multicast packet which is allowed to transmit through the interface in the interface configuration mode. The **no ip multicast ttl-threshold** command restores to the default value. The TTL threshold defaults to 0.

Command	Purpose
DES-7200 (config-if) # **ip multicast ttl-threshold** *ttl-value*	Configure TTL threshold in the range 0 to 255.

1.3.2 Limiting the Number of Entries to be Added in the IPv4 Multicast Routing Table

Use the **ip multicast route-limit** *limit* [*threshold*l command to limit the number of entries to be added in the multicast routing table, and use the **no ip multicast route-limit** *limit* [*threshold*l command to restore it to the default value, or 1024.

Command	Purpose

Command	Purpose
DES-7200 (config) # **ip multicast route-limit** *limit* [*threshold*]	Limit the number of entries to be added in the multicast routing table. *limit*: Number of entries to be added in the multicast routing table in the range of 1 to 2147483647, and 1024 by default. *threshold* (optional): Number of routes triggering an alert message, 2147483647 by default. Note: As the hardware is limit for different models, the multicast packets beyond the hardware forwarding table will be forwarded by the software. This will occupy CPU and sacrifice system performance.

1.3.3 Configuring IPv4 Multicast Boundary

Use the **ip multicast boundary** *access-list* command to configure the interface as the multicast boundary of a specific IP group in the interface configuration mode and use the **no ip multicast boundary** command to restore the default value.

Command	Purpose
DES-7200 (config-if) # **ip multicast boundary** *access-list* {**in	out**}	Configuring the IPv4 Multicast Boundary of the specific IP group. Numerical standard ACL or name can be used to specify an IP group. Note that The ACL in this command is specific for matching destination IP address, not group IP address and source IP address.

This command filters the IGMP, PIM-SM and PIM-DM packets associated with the IP group. Multicast packets will not flow in and out from the multicast boundary.

1.3.4 Configuring IPv4 Multicast Static Route

It is the multicast static route that makes multicast forwarding path differ from unicast path. RPF check is always executed for forwarding multicast packets. The actual receiving port is the port expected to receive packets (the port is the next hop of unicast route reaching the sender). RPF check is reasonable if the topologies of unicast and multicast are the same. But in some cases, unicast path is expected to differ from that of multicast.

Configuring multicast static route allows for RPF check based on configuration, not the unicast routing table. Consequently, multicast packets are forwarded through tunnel. Unicast packets are not. Multicast static route is configured locally. It will not be advertised or forwarded.

In the global configuration mode, use the following command to configure multicast static route.

Command	Purpose
DES-7200 (config) # **ip mroute** *source-address mask* [**bgp**	**isis**	**ospf**	**static**] {*v4rpf-address*	*interface-type interface-number*} [*distance*]	Configure multicast static route and specify the routing protocol type. *distance*: In the range of 1 to 255

Note

To set the egress of the static multicast route not to the next hop IP address, the egress must be a point-to-point type interface.

1.3.5 Configuring the Flow Control of Multicast Steams on Layer 2

To enable flow control on an interface, execute this command. More than one command, or a port that is allowed to forward can be configured for a multicast stream. Once enabled, the multicast stream can only be forwarded through these ports.

Command	Purpose
DES-7200 (config) # **ip multicast static** *source-address group-address interface-type interface-number*	Enable flow control on the interface. The static egress must be a layer 2 interface

This command controls only the forwarding of multicast streams on an interface, without direct influence on the multicast protocol's processing packets. However, as some features of some multicast protocol (for example, PIM-DM or PIM-SM) are driven by multicast streams, this may influence the activities of multicast protocols.

1.3.6 Configuring Longest-match Multicast Routing

According to the RPF rule, the multicast static routing, MBGP routing and unicast routing used for the RPF check can be selected from the multicast static routing list, MBGP routing list and unicast routing list.

By default, select the routing with the highest priority from these three routings. If the priority values are the same, the routing will be selected in the sequence of multicast static routing, MBGP routing and unicast routing.

Use the following command to configure and select the longest-match routing from the three routings. If the priority values are the same, the routing will be selected in the sequence of multicast static routing, MBGP routing and unicast routing.

Command	Purpose
DES-7200(config)# **ip multicast rpf longest-match**	According to the RPF rule, the multicast static routing, MBGP routing and unicast routing used for the RPF check can be selected from the multicast static routing list, MBGP routing list and unicast routing list. Select the longest-match routing from the three routings. If the priority values are the same, the routing will be selected in the sequence of multicast static routing, MBGP routing and unicast routing.

1.3.7 Monitoring and Maintenance of Multicast Routing

Execute the following command in the privileged configuration mode to show the IPv4 multicast forwarding table:

Command	Purpose
DES-7200 # **show ip mroute** [*group-address*] [*source-address*] [**dense**| **sparse**] [**summary**	**count**]}	Show the IPv4 multicast forwarding table.

Execute the following command in the privileged configuration mode to clear the IPv4 multicast forwarding table.

Command	Purpose
DES-7200 # **clear ip mroute** [***** **|** *v4group-address* **|** *v4source-address*]	Delete the IPv4 multicast forwarding table.

Execute the following command in the privileged configuration mode to reset the IPv4 multicast forwarding table statistics.

Command	Purpose
DES-7200 # **clear ip mroute statistics** [***** **|** *v4group-address* **|** *v4source-address*]	Reset the IPv4 multicast forwarding table statistics.

Execute the following command in the privileged configuration mode to show the RPF information of specific IPv4 source IP address.

Command	Purpose
DES-7200 # **show ip rpf** *v4source-address*	Show the RPF information of specific IPv4 source address.

Execute the following command in the privileged configuration mode to show the IPv4 multicast interface information.

Command	Purpose
DES-7200 # **show ip mvif** [*interface-type interface-number*]	Show the IPv4 multicast interface information.

Execute the following command in the privileged configuration mode to show the multicast operation.

Command	Purpose
DES-7200 # **debug nsm mcast all**	Show the multicast operation.

Execute the following command in the privileged configuration mode to show the communication between the IPv4 multicast and the routing protocol.

Command	Purpose
DES-7200 # **debug nsm mcast fib-msg**	Show the communication between the iPv4 multicast and the routing protocol.

Execute the following command in the privileged configuration mode to show the multicast operation on the interface.

Command	Purpose
DES-7200 # **debug nsm mcast vrf**	Show the multicast operation on the interface.

Execute the following command in the privileged configuration mode to show the multicast statistics.

Command	Purpose
DES-7200 # **debug nsm mcast stats**	Show the multicast statistics.

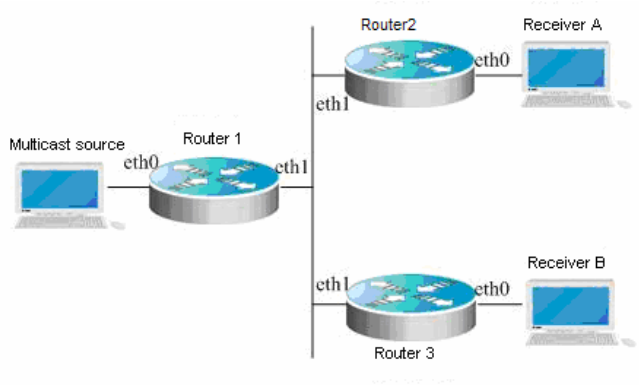
1.4 IPv4 Multicast Configuration Examples

1.4.1 PIM-DM Configuration Example

- **Configuration requirements**

The network topology is shown in Figure 36-6. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network, and device 3 and receiver B locate in the same network. Suppose the devices are connected with the host correctly and the IP addresses are configured.

Example of PIM-DM networking diagram



- **Device Configuration**

Take the device 1 as an example to show how to configure PIM-DM. The steps of device 2 and 3 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7200# configure terminal
DES-7200(config)# ip multicast-routing
```

Step 2: Enable PIM-DM on the interface eth0

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ip pim dense-mode
DES-7200(config-if)# exit
```

Step 3: Enable PIM-DM on the interface eth1 and return to the privileged user mode.

```
DES-7200(config)# interface eth 1
DES-7200(config-if)# ip pim dense-mode
DES-7200(config-if)# end
```

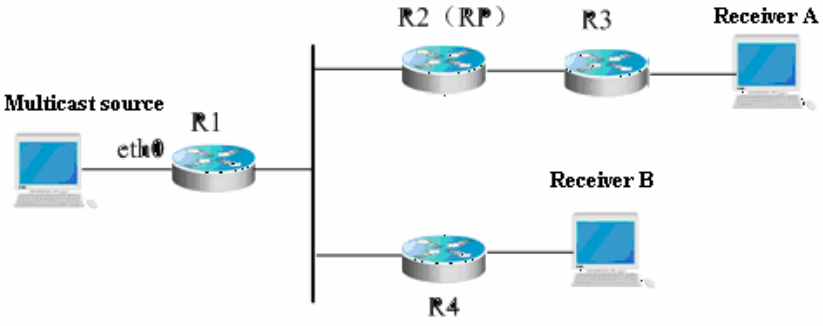
The configuration of device 2 and 3 is similar to device 1.

1.4.2 PIM-SM Configuration Example

- **Configuration requirements**

The network topology is shown in Figure 36-7. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network. Suppose the devices are connected with the host correctly; IP addresses and unicast routes are configured.

Example of PIM-SM networking diagram



- **Device Configuration**

Take the device 1 as an example to show how to configure PIM-SM. The steps of device 2, 3 and 4 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7200# configure terminal
DES-7200(config)# ip multicast-routing
```

Step 2: Enable PIM-SM on the interface eth0

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ip pim sparse-mode
DES-7200(config-if)# end
```

Step 3: Configure the candidate BSR and candidate C-RP.

Set R2's loopback1 to C-BSR and C-RP

```
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ip address 100.1.1.1 255.255.255.0
DES-7200(config-if)# ip pim sparse-mode
DES-7200(config-if)# exit
DES-7200(config)# ip pim bsr-candidate loopback 1
DES-7200(config)# ip pim rp-candidate loopback 1
DES-7200(config-if)# end
```

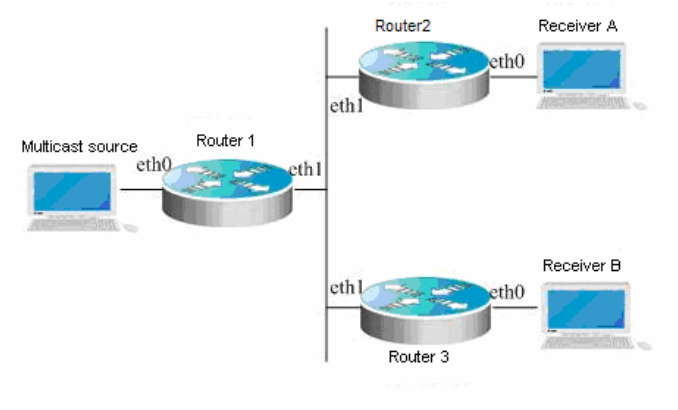
Note that once PIM-SM is enabled, IGMP is enabled on various interfaces automatically without manual configuration.

1.4.3 DVMRP Configuration Example

- **Configuration requirements**

The network topology is shown in the following figure. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network. Suppose the devices are connected with the host correctly; IP addresses and unicast routes are configured.

Example of DVMRP networking diagram



Device Configuration

Take the device 1 as an example to show how to configure DVMRP. The steps of device 2 and 3 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7200# configure terminal
DES-7200(config)# ip multicast-routing
```

Step 2: Enable DVMRP on the interface eth0

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ip dvmrp enable
DES-7200(config-if)# exit
```

Step 3: Enable DVMRP on the interface eth1 and return to the privileged user mode.

```
DES-7200(config)# interface eth 1
DES-7200(config-if)# ip dvmrp enable
DES-7200(config-if)# end
```

The configuration of device 2 and 3 is similar to device 1.

Note

Once the DVMRP is enabled, IGMP is auto-enabled on every interface without manual configuration.

2 IPv6 Multicast Configuration

2.1 Overview

Traditional IP transmission allows one host to transmit packets to a single host (unicast communication) or all hosts (broadcast communication). (Note that IPv6 no longer supports broadcast). Multicast, however, allows one host to send packets to some hosts (also known as group members).

The multicast application consists of the sender and the receiver. The sender can send multicast packets without needing to join a group. In contrast, the receiver can receiver the multicast packets from the group only after joining the group.

Group members are dynamic. A host can join in or leave from a group at any time. Furthermore, there is no limit on the position and number of group members. A host can join in more than one group simultaneously if necessary. Consequently, the active status and the number of members of a group vary with time.

The device maintains the routing table for forwarding multicast packets by running IPv6 multicast routing protocol (for instance, PIM-SMv6) and learns the status of group members on the direct segment by running the MLDv1/v2 protocol. The device joins in an IPv6 multicast group by sending the MLD report message.

IPv6 multicast applies to one-to-many multimedia applications.

2.1.1 Implementation of IPv6 Multicast Routing

The IPv6 multicast routing protocol includes:

- MLD: Runs between the multicast deivce and the host to learn the relation of group members.
- PIM-SMv6: Runs between the multicast devices to enable multicast packet forwarding by setting up the multicast routing table.

The following figure illustrates the function of the multicast protocols used in IPv6 multicast packet forwarding:

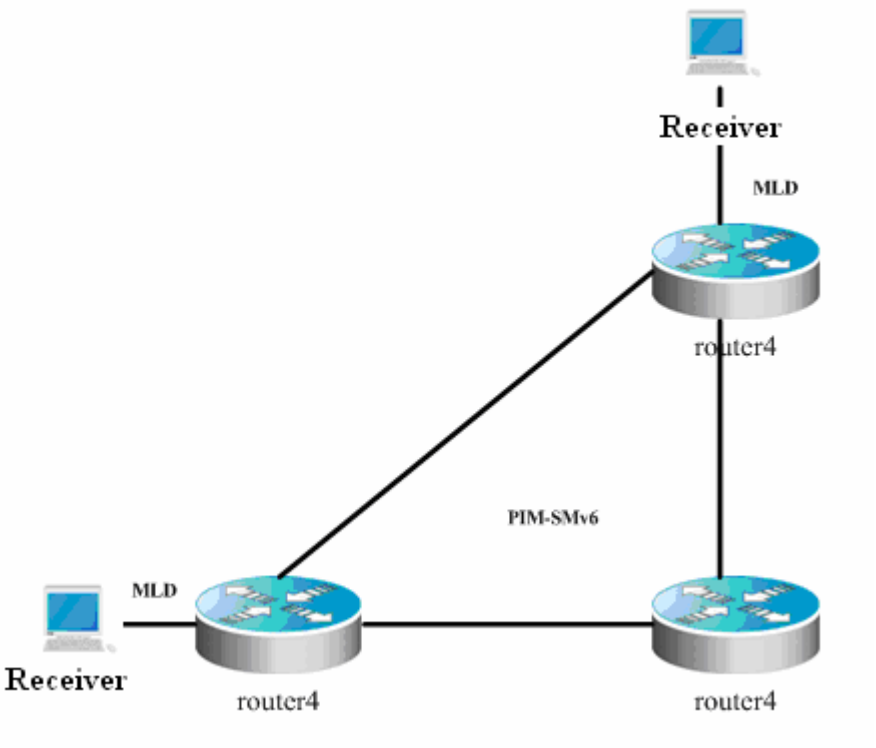


Figure 1 Multicast protocols used in IPv6 multicast environment

2.1.2 RPF Rule

The RPF(Reverse Path Forwarding) check mechanism is used to create the multicast routing entries according to the current unicast routing information, MBGP routing or multicast static routing to ensure the multicast data transmit along the correct path and avoid the various loops.

The following explains the detailed process of searching for the unicast routing table, MBGP routing table and multicast static routing table when using the RPF mechanism:

- **First, select the best routings from the unicast routing table, MBGP routing table and multicast static routing table respectively.**
  - Select the best routing from the unicast routing table for the RPF check:

  Search for the unicast routing table based on the IP address for the source packet as the destination address, and select the best unicast routing.

  - If there is only one next-hop for this unicast routing, you shall check whether the multicast has been enabled on the outbounding interface for the next-hop routing.
    If not, no unicast routing could be used for the RPF check;
    If so, this unicast routing could be used for the RPF check and the corresponding outbounding interface is the RPF interface.
  - If there are multiple next-hops for this unicast routing, all next-hops shall be checked whether the multicast has been enabled on the outbounding interface for the next-hop routing.
    If not, it continues to check the next next-hop routing;
    If so, this unicast routing could be used for the RPF check and the corresponding outbounding interface is the RPF interface.
    However, if the multicast function is not enabled on the outbounding interface for all next-hops, no unicast routing could be used for the RPF check.

- If there is no best routing, no unicast routing could be used for the RPF check.

- Select the best routing from the MBGP routing table for the RPF check:

Search for the MBGP routing table based on the IP address for the source packet as the destination address, and select the best MBGP routing.

- If there is only one next-hop for this MBGP routing, you shall check whether the multicast has been enabled on the outbounding interface for the next-hop routing.
  If not, no MBGP routing could be used for the RPF check;
  If so, this MBGP routing could be used for the RPF check and the corresponding outbounding interface is the RPF interface.

- If there is no best routing, no MBGP routing could be used for the RPF check.

- Select the best routing from the multicast static routing table for the RPF check:

Search for the multicast static routing table based on the IP address for the source packet as the destination address, and select the best multicast static routing.

- If there is only one next-hop for this multicast static routing, you shall check whether the multicast has been enabled on the outbounding interface for the next-hop routing.
  If not, no multicast static routing could be used for the RPF check;
  If so, you shall check whether there is unicast routing is used for the RPF check.

  - If the next-hop for the multicast static routing does not associate with the unicast protocol number, this multicast static routing could be used for the RPF check.

  - If no unicast routing is used for the RPF check, then the multicast static routing could be used for the RPF check.

  - If the unicast route could be used for the RPF check, and the protocol numbers for this unicast routing and associated next-hop multicast static routing are inconsistent, no multicast static routing could be used for the RPF check.

  - If the unicast route could be used for the RPF check, and the protocol numbers for this unicast routing and associated next-hop multicast static routing are consistent, the multicast static routing could be used for the RPF check.

- If there are multiple next-hops for this multicast static routing, all next-hops shall be checked whether the multicast has been enabled on the outbounding interface for the next-hop routing.
  If not, it continues to check the next next-hop routing;
  If so, you shall check whether there is unicast routing is used for the RPF check.

  - If the next-hop for the multicast static routing does not associate with the unicast protocol number, this multicast static routing could be used for the RPF check.

  - If no unicast routing is used for the RPF check, then the multicast static routing could be used for the RPF check, and the correspondent outbounding interface is the RPF interface.

  - If the unicast route could be used for the RPF check, and the

protocol numbers for this unicast routing and associated next-hop multicast static routing are inconsistent, it continues to check the next next-hop routing.

- If the unicast route could be used for the RPF check, and the protocol numbers for this unicast routing and associated next-hop multicast static routing are consistent, the multicast static routing could be used for the RPF check, and the correspondent outbounding interface is the RPF interface.
- If the multicast function is not enabled on the outbounding interface for all next-hops, no multicast static routing could be used for the RPF check.

- If there is no best routing, no multicast static routing could be used for the RPF check.

- **Then, select one routing as the RPF routing from these three best routings.**
  - With the longest-match multicast routing configured, select the longest-match routing from these three routings. If the masks for these three routings are the same, select the routing with the highest priority. If the priority for these routings are the same, select the routing in the sequence of multicast static routing, MBGP routing and unicast routing.
  - Without the longest-match multicast routing configured, select the routing with the highest priority from these three routings. If the priority for these routings are the same, select the routing in the sequence of multicast static routing, MBGP routing and unicast routing.

Caution

The effectiveness of MBGP routes recurs on unicast routes rather than distance. The implementation of current MBGP protocols does not support equal-cost routes.

The effectiveness of static multicast routes recurs on unicast routes rather than distance.

If the static unicast route is selected as RPF route, the route must be configured with the next hop IP address. PIM protocol will select RPF neighbors based on this next hop IP address. If the static unicast route is not configured with the next hop IP address, PIM protocol can get RPF neighbors.

2.2 Basic IPv6 Multicast Route Configuration

2.2.1 Enable IPv6 Multicast Route Forwarding

This function enables software to forward multicast packets.

To enable IPv6 multicast route forwarding, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **ipv6 multicast-routing**	Enable IPv6 multicast routing.

2.2.2 Enable IPv6 Multicast Route Protocol

PIM-SMv6: refer to PIM-SMv6 configuration for the configuration process.

Caution

After enabling the layer3 multicasting on the Private VLAN and Super VLAN, if the multicast source exists in the Sub-VLAN, one more route entry is needed to be duplicated and the ingress is the Sub-VLAN in which the multicast streams enter as the ingress validity check is required when multicast forwarding, resulting in occupying one more multicast hardware entry with 1 less multicast capacity.

2.2.3 Enable MLD

Enabling IPv6 multicast route forwarding and IPv6 multicast route protocol will enable MLD.

2.3 Advanced IPv6 Multicast Core Function Configuration

2.3.1 Limit the Number of the Routes That are Allowed to Join the IPv6 Multicast Routing Table

In the global configuration mode, use the **ipv6 multicast route-limit** *limit* [*threshold*] command to limit the number of the routes that are allowed to join the multicast routing table. Use the no form of this command to resotre it to the default value, or 1024.

Command	Function
DES-7200(config-if)# **ipv6 multicast route-limit** *limit* [*threshold*]	Limits the number of the routes that are allowed to join the multicast routing table. *limit*: Number of the routes that are allowed to join the multicast routing table in the range 1 to 2147483647, 1024 by default. Threshold: (optional) Number of multicast routes triggering alarm, 2147483647 by default. Note: Given the hardware resource for different models of devices, the routes exceeding the hardware entry threshold need to be forwarded through software, and resulting in decrease in performance.

2.3.2 Set IPv6 Multicast Border for Specific IPv6 Group Range

In interface configuration mode, use the **ipv6 multicast boundary** *access-list-name* command to set IPv6 multicast border for specific IPv6 group range. Use no form of this command to restore it to the default value, namely no multicast border.

Command	Function

DES-7200(config-if)# **ipv6 multicast boundary** *access-list-name* [**in | out**]	Set IPv6 multicast border for specific IPv6 group range. ACL can be used to specify the IPv6 group range. Note: The ACL associated with this command supports only matching destination IP address, not mutlciast IP address and source IP address.

This command filters MLD and PIM-SMv6 protocol packets correlating with the specific IPv6 group range. Multicast streams will income and outgoing through the multicast border interface.

2.3.3 Configure Static IPv6 Multicast Route

IPv6 static multicast route enables multicast packet forwarding through a path different from IPv6 unicast path. RPF check is always performed while forwarding. The real interface receiving packets is the expected one, namely the next hop interface of IPv6 unicast route used to transmit to the sender. The check is reasonable when IPv6 unicast topology is in accord with IPv6 multicast topology. In some cases, however, it is better to make difference between IPv6 unicast path and IPv6 multicast path.

Static multicast rotue enables devices to execute RPF check according to configurations rather than the IPv6 unicast routing table. Consequently, tunnel technology is used for IPv6 multicast packet forwarding, not IPv6 unicast packet forwarding. IPv6 static multicast route is stored locally rather than be advertised or forwarded.

In the global configuration mode, use the following command to configure IPv6 static multicast route.

Command	Function
DES-7200(config)# **ipv6 mroute** *ipv6-prefix/prefix-length* [**bgp** | **isis** | **ospfv3** | **ripng** | **static**]{ *ipv6-prefix* | *interface-type interface-number*} [*distance*]	Configures IPv6 static multicast route. Routing protocol can be set at the same time. Distance: <1-255>

Note

To set the egress of the static multicast route not to be the IPv6 address of next hop, the egress must be an point-to-point interface.

2.3.4 Configure Flow Control for Multicast Packets on Layer 2

This command can be used to configure flow control for multicast packets on Layer 2

Many commands can be configured for a multicast stream, namely multiple ports that are allowed for forwarding. Once flow control is configured for a multicast stream, the multicast stream can be forwarded only through these configured ports.

Command	Function

DES-7200(config)# **ipv6 multicast static** *source-address group-address interface-type interface-number*	Configure flow control on the Layer 2 interface. The egress of static multicast route must be a Layer 2 itnerface.

This command controls the forwarding of multicast streams on an interface without influencing multicast protocols' processing of packets. Since some features of multicast protocols like (PIM-SMv6) depend on multicast streams, however, the behavors of multicast protocols may also be influenced.

2.3.5 Configure Longest-match-based Routing

The static multicast route, MBGP route and unicast route used for RPF check are elected from the static multicast routing table, MBGP routing table and unicast routing by RPF rules, respectively.

By default, the one of highest priority is selected from these three routes. If they are of the same priority, select one in the order of static multicast route, MBGP route and unicast route.

Use this command to select the route matching the longest mask from these three routes.

Command	Function
DES-7200(config)# **ipv6 multicast rpf longest-match**	Select the route matching the longest mask.

2.3.6 Multicast Route Monitoring and Maintenance

In the privileged EXEC configuration mode, run the following command to show the information of IPv6 multicast forwarding table.

Command	Function
show ipv6 mroute [*v6group-address*] [*v6source-address*] [**dense**]|[**sparse**] } {[**summary**]|[**count**]}	Show the information of IPv6 multicast forwarding table.

In the privileged EXEC configuration mode, run the following command to delete the IPv6 multicast forwarding table.

Command	Function
clear ipv6 mroute {* | *v6group-address* [*v6source -address*]}	Delete the IPv6 multicast forwarding table.

In the privileged EXEC configuration mode, run the following command to reset the statics of the IPv6 multicast forwarding table.

Command	Function
clear ipv6 mroute statistics {* | *v6group-address* [*v6source-address*]}	Reset the statics of the IPv6 multicast forwarding table.

In the privileged EXEC configuration mode, run the following command to show the RPF information of the specific IPv6 source address.

Command	Function
show ipv6 rpf *v6source-address*	Show the RPF information of the specific IPv6 source address.

In the privileged EXEC configuration mode, run the following command to show the information of static IPv6 multicast route.

Command	Function
show ipv6 mroute static	Show the information of static IPv6 multicast route.

In the privileged EXEC configuration mode, run the following command to show the information of IPv6 multicast interface.

Command	Function
show ipv6 mvif [*interface-type interface-number*]	Show the information of IPv6 multicast interface.

In the privileged EXEC configuration mode, run the following command to show the IPv6 Layer 3 multicast forwarding table.

Command	Function
show ipv6 mrf mfc	Show the IPv6 Layer 3 multicast forwarding table.

In the privileged EXEC configuration mode, run the following command to show the IPv6 multicast forwarding table of multiple layers.

Command	Function
show msf6 msc	Show the IPv6 multicast forwarding table of multiple layers.

In the privileged EXEC configuration mode, run the following command to show the operation of the core of IPv6 multicast.

Command	Function
debug nsm mcast6 all	Show the operation of the core of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the communication between the core of IPv6 multicast and multicast protocols.

Command	Function
debug nsm mcast6 fib-msg	Show the communication between the core of IPv6 multicast and multicast protocols.

In the privileged EXEC configuration mode, run the following command to show the operation on the interface of the core of IPv6 multicast.

Command	Function
debug nsm mcast6 mif	Show the operation on the interface of the core of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the operation of interface and statistics of the core of IPv6 multicast.

Command	Function
debug nsm mcast6 stats	Show the operation of interface and statistics of the core of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the packet forwarding on Layer 3 of IPv6 multicast.

Command	Function
debug ipv6 mrf forwarding	Show the packet forwarding on Layer 3 of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the operation of forwarding entries on Layer 3 of IPv6 multicast.

Command	Function
debug ipv6 mrf mfc	Show the operation of forwarding entries on Layer 3 of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the operation of forwarding events on Layer 3 of IPv6 multicast.

Command	Function
debug ipv6 mrf event	Show the operation of forwarding events on Layer 3 of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the packet forwarding on multiple layers of IPv6 multicast.

Command	Function
debug msf6 forwarding	Show the packet forwarding on multiple layers of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the operation of forwarding entries on multiple layers of IPv6 multicast.

Command	Function
debug msf6 mfc	Show the operation of forwarding entries on multiple layers of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the operation of the baseline hardware on forwarding packets on multiple layers of IPv6 multicast.

Command	Function
debug msf6 ssp	Show the operation of the baseline hardware on forwarding packets on multiple layers of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the process of invoking API interface to forward packets on multiple layers of IPv6 multicast.

Command	Function
debug msf6 api	Show the process of invoking API interface to forward packets on multiple layers of IPv6 multicast.

In the privileged EXEC configuration mode, run the following command to show the operation of forwarding events on multiple layers of IPv6 multicast.

Command	Function

debug msf6 event	Show the operation of forwarding events on multicast layers of IPv6 multicast.

2.4 IPv6 Multicast Configuration Example

- **Configuration Requiremetns**

Figure 3 is network topology. R1 and the multicast soruce are located in one network. R2 is set to be RP. R3 and the Receiver A are located in the same network. R4 and the Receiver B are located in the same network. Assume that devices and hosts are connected properly, IPv6 is enabled on every interface and IPv6 unicast is enabled on every device.

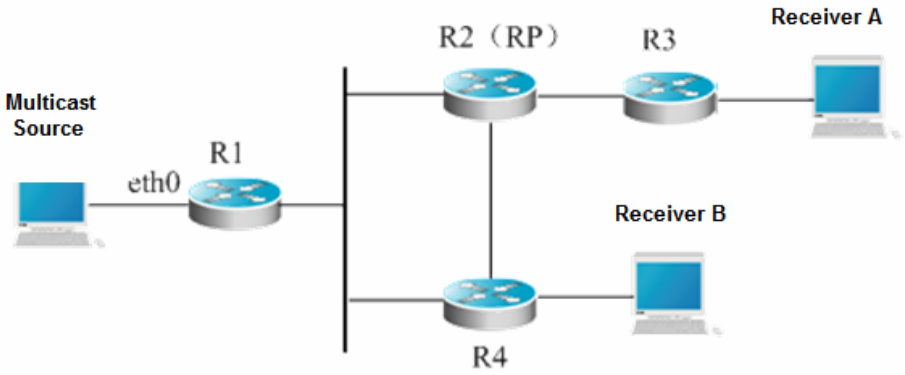


Figure 2 Network topology of PIM-SMv6 configuration example

- **Device Configuration**

Step1: Enable IPv6 multicast rotue.

Enable IPv6 multicast route on R1. The configurations on R2, R3 and R4 are similar.

```
DES-7200# configure terminal
DES-7200(config)# ipv6 multicast-routing
```

Step 2: Enable PIM-SMv6 on the interface.

Enable PIM-SMv6 on R1's eth0. The configurations on R2, R3 and R4 are similar.

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ipv6 pim sparse-mode
DES-7200(config-if)# end
```

Step 3: Configure the candidate BSR and the candidate RP.

Set R2's loopback1 to be C-BSR and C-RP

```
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ipv6 address 2008:1::1/64
DES-7200(config-if)# ipv6 pim sparse-mode
DES-7200(config-if)# exit
DES-7200(config)# ipv6 pim bsr-candidate loopback 1
DES-7200(config)# ipv6 pim rp-candidate loopback 1
DES-7200(config-if)# end
```

Add the receiver into the multicast group. After the multicast source sends multicast streams, you can run **show** commands to monitor operation..

Note

When you enable PIM-SMV6, MLD automatically runs on every interface, respectively.

3 IGMP Configuration

3.1 IGMP Overview

IPv4 multicast refers to a network technology that forwards packets to more than one receiver through a multicast flow. Only the hosts joining the group can receive the packets from the specific multicast group. Multicast can save network bandwidth greatly for there is only single packet transmitting on any link of the network, no matter how many receivers are deployed.

Multicast uses Class-D network address specified by IANA. The highest bits of Class-D network address are 1110. So, the Class-D network address is in the range of 224.0.0.0 to 239.255.255.255. However, not all addresses in this range can be used by users. The addresses in the range 224.0.0.1 to 224.0.0.255 are reserved for protocols. For instance, 224.0.0.1 indicates all multicast host addresses and 224.0.0.2 indicates all multicast device addresses.

Any hosts, no matter whether they are multicast group member or not, can be the multicast source. However, only the multicast group member can receive the multicast frame. The multicast group member is able to dynamically join in or leave the group. The forwarding of multicast frame in the network is processed by the multicst device with multicast routing protocol enabled.

To enable IPv4 multicast, multicast hosts and devices must support IGMP. This protocol is used by the host to notify the multicast device of the multicast membership of the network they connect to determine how to forward multicast traffic. By using the information obtained from the IGMP, the device can maintain an interface and group-based multicast member list. The multicast member list is activated only when at least one host of an interface is a member of the group.

IGMPv1, IGMPv2 and IGMPv3 are supported at present. On the basis of IGMPv1, IGMPv2 has the leaving message so that the host can actively request to leave a multicast group. IGMP activities fall into two parts: host activity and device activity.

3.1.1 IGMPV1

There are only two types of messages defined in IGMP Version 1:

- Membership query
- Membership report

A host sends a report packet to join a group, and the router sends the query packet at periodical intervals to ensure that a group has at least one host. When a group contains no host, the router will delete that group.

3.1.2 IGMPV2

In Version 2, there are only four types of packets:

- Membership query

- Version 1 membership report
- Version 2 membership report
- Leave group

IGMPv2 is basically the same as IGMPv1, except that the leave mechanism of the host has been improved. For V2, the host can send a leave message to notify the device, which then sends a query to verify if there is a host in the multicast group. This makes joining and leaving a group more efficiently.

In the multicast network that runs IGMP, there is a dedicated query multicast device, which is responsible for sending IGMP query messages. This de querier is chosen through an election process. At the beginning, all the devices are queriers. When a device receives a query message, it compares the source IP address of the message. For IGMPv1, the device of the highest IP address is elected as the querier. However, for IGMPv2/v3, the one of the lowest IP address is selected as the querier. Moreover, for the IGMP query messages with different versions, the one sending the IGMP query message of the lowest version is elected as the querier.

If the querier fails, the querier is elected again. The non-querier devices maintain the interval timers of other queriers. Every time when a device receives a membership query packet, it resets the timer. If the timer expires, the device considers itself is the querier and starts to send query messages. The querier election starts again.

The querier must send the membership query request periodically to ensure that other devices in the network know that the querier still works. For this purpose, the querier maintains one query interval timer. When it sends the membership query message, this timer will be reset. When the interval timer times out, the querier sends another membership query.

When the device appears for the first time, that is, a new device is added, it sends a series of general query messages to see which multicast groups will be received on the hosts of which interfaces for rapid convergence. The number of common query packets sent is based on the start query count configured. The querying interval between the initial general query messages is defined through the startup query interval.

When a querier receives a leave packet, it must send a particular group membership query to see if the host is the last one leaving the group. Before the querier stops forwarding packets to the group, it sends a series of such packets, the number of which is equal to the last member query number. The querier sends multiple particular membership queries to ensure that there is no member in the group. Such a query is sent every other the seconds of the last-member query interval to separate the queries. When no response is received, the querier stops forwarding multicast packets to the group on the particular interface.

3.1.3 IGMPV3

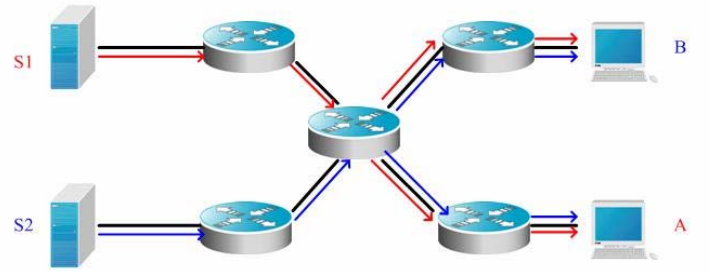
In the applications of the IGMPV1 and V2, there are the following defects:

- Lack of efficient measures to control multicast sources
- Difficult to establish the multicast path due to unknown multicast source
- Difficult to find a unique multicast address. It is possible that multicast groups are using the same multicast address.

On the basis of IGMPV1/V2, IGMPV3 provides an additional source filtering multicast function. In IGMP V1/V2, the host determines to join a group and receive the multicast traffic to the group address from any source only based on

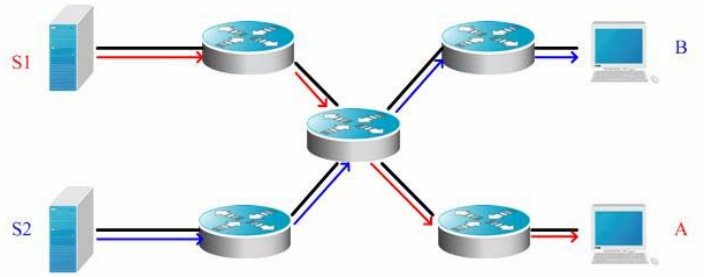
the group address. On the other hand, the host running the IGMP V3 notifies this host the desired multicast group to join, and also the addresses of the multicast sources to receive. The host can indicate that it wants to receive multicast traffic from which sources through an inclusion list or an exclusion list. At the same time, another benefit of the IGMP v3 is that it saves bandwidth to avoid unnecessary, invalid multicast data traffics from occupying network bandwidth. It is particularly useful in the case where multiple multicast sources share one multicast address. The IGMPv1 and IGMPv2 can also implement “source address filter” in some sense, which, however, is performed on the end of receiving the multicast traffic. As shown in the following diagram, there are two multicast sources (S1 and S2), which send the data traffic of the same multicast address (G). The multicast flow of S1 and S2 will be sent to all hosts receiving flows from G. If host A only wants to receive multicast flows from S1, it filters flows by using the related client software.

Figure 1-2 Multicast route forwarding without filtering source



If the equipments in the network support IGMP v3, host A wants to receive the traffic from S1 only. It can send the IGMPv3 packet of join G include S1. If host B wants to receive the traffic from S2 only, it can send the IGMPv3 packet of join G include S2. Therefore, the traffics are forwarded as shown in the following diagram. This saves bandwidth.

Figure 1-3 Multicast route forwarding with filtering source



In contrast to Version 2, Version 3 defines the following two kinds of messages:

- Membership Query
- Version 3 Membership Report

There are three types of Membership Query:

- General Query: Used to query all the multicast members under the interface.
- Group-Specific Query: Used to query the members of the specified group under the interface.
- Group-and source-Specific Query: This type is the new one in the IGMPv3, which is used to query if any member under the interface needs to receive the multicast traffic of the particular group from the sources in the specified source list.

Different from the Membership Report in IGMP Version2, the Membership Report in the IGMP Version3 always has the destination address of 224.0.0.22. The Membership Report packets in IGMP Version3 include the information of multiple

groups. It can carry with one or more group records, each record with group address and source address list. Below shows the types of group record:

IS_IN: Indicates INCLUDE filtering mode between the multicast group and the multicast source list, that is, only the multicast traffic from the specific multicast source list to the multicast group are received. A null multicast source list means leaving the multicast group, which is equivalent to the leave message in IGMPv2.

IS_EX: Indicates EXCLUDE filtering mode between the multicast group and the multicast source list, that is, only the multicast traffic from any multicast source except for the specific multicast source list to the multicast group are received.

TO_IN: Indicates that the filtering mode between the multicast group and the multicast source list changes from EXCLUDE to INCLUDE.

TO_EX: Indicates that the filtering mode between the multicast group and the multicast source list changes from INCLUDE to EXCLUDE.

ALLOW: Indicates receiving multicast traffic from additional multicast sources. For INCLUDE mode, it adds these multicast source to the multicast source list. For EXCLUDE mode, it removes these multicast sources from the multicast source list.

BLOCK: Indicates no longer receiving multicast traffic from some multicast sources. For INCLUDE mode, it removes these multicast source from the multicast source list. For EXCLUDE mode, it adds these multicast sources to the multicast source list.

For the sake of compatibility, IGMPv3 can identify IGMPv1/v2 packets.

Caution

For the specific group on the DES-7200's switching router multicast layer3 interface, up to 1017 specific sources with unicast-allowed by users can be configured.

For the specific group on the DES-7200's switching router multicast layer3 interface, up to 1017 specific sources without the unicast-allowed by users can be filtered.

3.2 IGMP Configuration Task

IGMP configuration includes the following tasks. Only some configuration tasks are mandatory, others are optional. It should be noted that the following commands should be executed on the Layer 3 interface.

3.2.1 Default IGMP Configuration

IGMP version	IGMPv2 is supported on all interfaces.
Query response time	10s
Query interval	125s
Access to multicast group	All multicast groups
Other querier timer	255s
Robustibility variables	2
Query interval of last member	1s
Query count of last member	2
IGMP status	Disabled

3.2.2 Enabling IGMP

Use the following command in the interface configuration mode to enable IGMP:

Command	Purpose
DES-7200 (config-if) # **ip pim** {**sparse-mode** | **dense-mode**}	Enable the multicast routing protocol and IGMP.
DES-7200 (config-if) # **no ip pim** {**sparse-mode** | **dense-mode**}	Disable the multicast routing protocol and IGMP.

Note

Enabling a multicast routing protocol and the multicast routing forwarding function on an interface will enable IGMP.

A device can run only one kind of multicast routing protocol.

3.2.3 Configuring IGMP Version

Use the following command in the interface configuration mode to configure the IGMP version.

Command	Purpose
DES-7200 (config-if) # **ip igmp version**{*1* | *2* | *3*}	Configure the IGMP version, version 2 by default.
DES-7200 (config-if) # **no ip igmp version**	Restore to the default value.

3.2.4 Configuring Query Interval of Last Member

After receiving the message of leaving the multicast group, the querier sends the specific membership query to verify whether there is any member in the group. If no report is received during the last member query interval period, the querier will regard the host that is leaving the group is the last member of that group, and then delete the information of the group. By default the period is 1 s.

Use the following commands in the interface configure mode to configure the query interval of last member:

Command	Function
DES-7200 (config-if) # **ip igmp last-member-query-interval** *interval*	Configure the query interval of the last member. *interval*: in the range 1 to 255 in 0.1s.
DES-7200 (config-if) # **no ip igmp last-member-query-interval** *interval*	Restore to the default value.

3.2.5 Configuring Query Count of Last Member

After receiving the message of leaving the multicast group, the querier device sends the specific membership query for several times to verify whether there is any member in the group. The query times should be larger than 1.

Use the following command in the interface configuration mode to configure the query count of last member:

Command	Function

Command	Function
DES-7200 (config-if) # **ip igmp last-member-query-count** *count*	Configure the query count of last member in the range of 2 to 7, 2 by default.
DES-7200 (config-if) # **no ip igmp last-member-query-count**	Restore to the default value.

3.2.6 Configuring Query Interval of General Member

The querier device sends the general member query message at intervals to all hosts to verify the current membership. The multicast IP address is 224.0.0.1, TTL is 1 and the default value is 125s.

Use the following command in the interface configuration mode to configure the query interval of general member:

Command	Function
DES-7200 (config-if) # **ip igmp query-interval** *seconds*	Configure the query interval of general member in the range of 1 to 18000 seconds, 125s by default.
DES-7200 (config-if) # **no ip igmp query-interval** *seconds*	Restore to the default value.

3.2.7 Configuring the Maximum Response Time

The membership query message sent by the querier device requires the maximum response time. Shorting this response time can make the device know the change of the members earlier, which will result in increase of the member reports diffusing in the network. The network administrator can consider a tradeoff between the two factors and then decide a proper value for the period, 10 seconds by default. Another consideration in configuring the response time is that it shall be shorter than the query interval.

Use the following commands in the interface configuration mode to configure the maximum response time:

Command	Function
DES-7200 (config-if) # **ip igmp query-max-response-time** *seconds*	Configure the maximum response time in the rnage1-25s.
DES-7200 (config-if) # **no ip igmp query-max-response-time** *seconds*	Restore to the default value.

3.2.8 Configuring the Timer of Other Querier

Once the timer times out, the querier considers that there is no other querier on the network. This is helpful for the election of querier. You can short this timer in the circumstance where the querier changes frequently to speed up response.

Use the following commands in the interface configuration mode to configure the timer of other querier:

Command	Function
DES-7200 (config-if) # **ip igmp query-timeout** *seconds*	Configure the timer of other querier in the range of 60 to 300 seconds, 255 seconds by default.
DES-7200 (config-if) # **no ip igmp query-timeout**	Restore to the default value.

3.2.9 Configuring Access to Multicast Groups

By default, the hosts on an interface can join any multicast group. You can restrain the multicast group range that the hosts join by configuring a standard IP ACL and applying it to the specific interface.

Use the following command in the interface configuration mode to configure access to multicast groups:

Command	Function
DES-7200 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7200 (config) # **access-list** *access-list-num* **permit** *A.B.C.D A.B.C.D*	Define an ACL.
DES-7200 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200 (config-if) **# ip igmp access-group** *access-list-name*	Allow for access to the multicast groups in the ACL.
DES-7200 (config-if) # **no ip igmp access-group** *access-list-name*	Allow for access to all multicast groups.

3.2.10 Configuring to Leave the Multicast Group Immediately

In IGMPv2, you can execute this command to short the delay to leave a multicast group. A host leaves a multicast group as long as it sends a leave message without needing the querier to send the specific multicast group query message. This command is available only when there is only one host on an interface.

Use the following command to configure to leave the multicast group immediately:

Command	Function
DES-7200 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7200 (config) # **access-list** *access-list-num* **permit** *A.B.C.D A.B.C.D*	Define an ACL.
DES-7200 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ip igmp immediate-leave group-list** *access-list-name*	Leave the multicast groups in the ACL immediately.
DES-7200 (config-if) # **exit**	Enter the privileged configuration mode.

3.2.11 Configuring join-group

This command configures an interface of the switch with host behaviors and requires the interface to join a multicast group. In this way, the switch can learn the multicast group information.

Use this command in the interface configuration mode to add an interface into a multicast group:

Command	Function
DES-7200 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7200 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ip igmp join-group** *group-address*	Configure the interface to join the multicast group.

Command	Function
DES-7200 (config-if) # **exit**	Enter the privileged configuration mode.

Use the **no ip igmp join-group** *group-address* command to leave the multicast group.

3.2.12 Configuring static-group

Use this command in the interface configuration mode to add an interface into a static group:

Command	Function
DES-7200 (config-if) # **config terminal**	Enter the global configuration mode.
DES-7200 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ip igmp static-group** *group-address*	Configure the interface to join the static group.
DES-7200 (config-if) # **exit**	Enter the privileged configuration mode.

Use the **no ip igmp static-group** *group-address* command to leave the static group.

3.2.13 Configuring the Limit of IGMP Group Members

This command configures the limit of IGMP group members globally. The messages of the members that exceed the limit will not be cached or forwarded.

You can configure this command on interfaces individually in interface mode or globally. The messages of the members that exceed the limit configured on an interface or globally will be ignored.

To configure the limit of IGMP group members, execute the following commands in the interface mode.

Command	Function
DES-7200(config) # **ip igmp limt** *number*	Configure the limit of IGMP members globally. The limit depends on specific products. By default, it is 65536.
DES-7200(config-if) # **ip igmp limit** *number*	Configure the limit of IGMP members on the interface. The limit depends on specific products. By default, it is 1024.

3.2.14 Configuring IGMP PROXY - SERVICE

This command enables service on all the downlink mroute-proxy interfaces. After you configure this command on an interface, the interface becomes the uplink interface of the corresponding mroute-proxy service. Moreover, it associates all its downlink interfaces and maintains their propagated multicast group information.

Up to 32 proxy services can be configured using this command. The interface number with the IGMP Proxy enabled is limited by the multicast interface number supported by the device. Upon the receipt of query message, the proxy-service interface responds accordingly based on the member information that it maintains from the interfaces with mroute-proxy configured. Consequently, configuring proxy-service on an interface equals to performing host behaviors rather than

router behaviors on the interface.

To configure IGMP proxy-service, execute the following commands in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ip igmp proxy-service**	Configure proxy-service on the interface.

3.2.15 Configuring IGMP MROUTE - PROXY

This command lets an interface to forward messages to its corresponding uplink interface.

The uplink interface can forward IGMP messages received from its members only when it is set to a proxy-service interface.

To configure IGMP mroute proxy, execute the following commands in the interface configuration mode.

Command	Function
DES-7200(config-if)# i**p igmp mroute-proxy** *interface name*	Configure mroute-proxy on the interface.

3.2.16 Enabling IGMP SSM-MAP

This command forcibly appends the relevant multicast source messages to the dynamically learned multicast group messages. It is usually used in conjunction with the **ip igmp ssm-map static** command.

To enable IGMP SSM-MAP, execute the following commands in the interface configuration mode.

Command	Function
DES-7200(config)# **ip igmp ssm-map enable**	Enable the SSM-MAP function.

3.2.17 Configuring IGMP SSM-MAP STATIC

This command is used in conjunction with the **ip igmp ssm-map enable** command. After this command is configured, the received messages whose version is earlier than version 3 will be mapped with the corresponding multicast source record.

To configure IGMP SSM-MAP STATIC, execute the following commands in the global configuration mode.

Command	Function
DES-7200(config)# **ip igmp ssm-map static** *11 192.168.2.2*	All groups matched ACL 11will be mapped with 192.168.2.2.

3.3 Monitoring and Maintaining

3.3.1 Clearing the Dynamic Group Membership Message Obtained From the Response Message in IGMP Cache

To clear the dynamic group member messages obtained from the response message in IGMP cache, use the following command in the privileged configuration mode:

Command	Function
DES-7200# **clear ip igmp group**	Clear the dynamic group member messages obtained from the response message in the IGMP cache. Without any parameter, this command clears all the IGMP group messages.

3.3.2 Clearing All Information on Specified Interface in IGMP Cache

To clear all information on the specified interface in IGMP cache, use the following command in the privileged EXEC mode:

Command	Function
DES-7200# **clear ip igmp interface** *interface-type*	Clear all the information on the interface in IGMP cache.

3.3.3 Showing the Status of IGMP Group Members in the Directly-Connected Subnet

Use the following command in privileged EXEC mode to show the status of IGMP group members in the directly-connected subnet:

Command	Function
DES-7200# **show ip igmp groups**	Show the status of all IGMP group members in the directly-connected subnet.
DES-7200# **show ip igmp groups detail**	Show the details of all IGMP group members in the directly-connected subnet.
DES-7200# **show ip igmp groups** *A.B.C.D*	Show the status of the specified group member in the directly-connected subnet.
DES-7200# **show ip igmp groups** *A.B.C.D* **detail**	Show the details of the specified member in the directly-connected subnets.
DES-7200# **show ip igmp interface** *interface-type*	Show the information of the specified interface in the directly-connected subnets.
DES-7200# **show ip igmp groups** *interface-type* **detail**	Show the details of the specified interface in the directly-connected subnets.
DES-7200# **show ip igmp groups** *interface-type A.B.C.D*	Show the information of the specific group of the specified interface in the directly-connected subnets.
DES-7200# **show ip igmp groups** *interface-type A.B.C.D* **detail**	Show the details of the specific group of the specified interface in the directly-connected subnets.

3.3.4 Showing the Configuration Information of the IGMP interface

To show the configurations of the IGMP interface, run the following command in

the privileged mode:

Command	Function
DES-7200# **show ip igmp interface** [*interface-type interface-number*]	Show the configuration information of the IGMP interface.
DES-7200# **show ip igmp interface**	Show the configuration information of all the IGMP interfaces.

3.3.5 Show the Configuration Information of IGMP SSM-MAP

To show the configuration information of IGMP SSM-MAP, use the following command in the privileged EXEC mode:

Command	Function
DES-7200# **show ip igmp ssm-map**	Show the Configuration Information of IGMP SSM-MAP.
DES-7200# **show ip igmp ssm-map** 233.3.3.3	Shown the mapping information from IGMP SSM-MAP to the multicast group 233.3.3.3.

3.3.6 Showing the Status of IGMP Debugging Switch

To show the status of the IGMP debugging switch, use the following command in the privileged mode:

Command	Function
DES-7200# **show debugging**	Show the status of the IGMP debugging switch.

3.3.7 Turning on IGMP Debugging Switch

To turn on IGMP debugging switch, use the following command in the privileged mode:

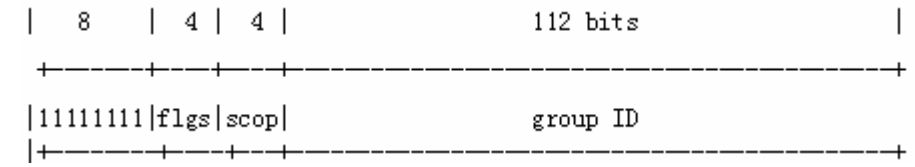
Command	Function
DES-7200# **debug ip igmp all**	Turn on all IGMP debugging switches
DES-7200# **debug ip igmp decode**	Turn on decode debugging switch
DES-7200# **debug ip igmp encode**	Turn on encode debugging switch
DES-7200# **debug ip igmp events**	Turn on event debugging switch
DES-7200# **debug ip igmp fsm**	Turn on final-state-machine debugging switch
DES-7200# **debug igmp tib**	Turn on tree debugging switch.
DES-7200# **debug ip igmp warnning**	Turn on warning debugging switch.

4 MLD Configuration

4.1 MLD Overview

IPv6 multicast is a network technology allowing one or more senders (multicast sources) to send a single packet to multiple receivers (once and simultaneous). The multicast source sends the packet to a specific multicast group, and only hosts having addresses of this multicast group can receive the packet. Multicasting can substantially save network bandwidth, because only one packet is sent on any link of the entire network no matter how many destination addresses exist.

The format of IPv6 multicast address is different from that of IPv6 unicast address, and can only be used for destination address. The first byte of address format all consists of "1" (multicast address). The multicast address occupies 1/256 of the IPv6 address space. Except for parts other than the first byte, the multicast address format includes the following fields:



Flag field: (starting from high-order bit) The first bit is the reserved bit set to 0; the second bit is R flag: R = 1 indicates a multicast address that embeds the address of the RP, while R = 0 indicates a multicast address that does not embed the address of the RP; the third bit is P bit: R = 1 indicates a multicast address is created on basis of unicast prefix, otherwise it is set to 0.

The scop field has 4 bits and indicates the scope of multicasting. According to the definition given in RFC 4291: 1 (hexadecimal number system) indicates interface-local scope, 2 indicates link-local scope, 4 indicates admin-local scope, 5 indicates site-local scope, 8 indicates organization-local scope, and E indicates global scope.

Group ID has 112 bits, and is used to identify the multicast group. According to the multicast address (transient or well-known) and the scope of address, the same multicast ID can indicate different groups. Well-known multicast address uses specific group ID with special meanings.

No matter whether a member of multicast group or not, any host can be a multicast source. However, only the member of multicast group can receive the multicast frames. Members of the multicast group are determined dynamically, and the host can dynamically join or leave the group. The multicast frames are forwarded by the multicast device, which will run the multicast routing protocol.

To participate in IPv6 multicast, the multicast host/device shall be able to support MLD operations. This protocol allows the interactive multicasting of member relationship between host and routing device, so as to decide on the forwarding of multicast steam. By utilizing the information obtained from MLD, the device will maintain a multicast listener state table, which is based on each interface. When the local link of an interface has at least one host being a member of the group,

the multicast listener state table will then be activated.

Currently, MLD has to versions. MLDv2 was developed on the basis of MLDv1 by adding the source filtering mechanism. The behaviors of MLD protocol can be divided into two parts: host behavior and router behavior.

4.1.1 Introduction to Messages of Different MLD versions

4.1.1.1 MLD Version 1

In MLDv1, there are three types of messages:

- Multicast Listener Query
- Multicast Listener Report
- Multicast Listener Done

In the multicast network running MLD protocol, there will be querier responsible for sending MLD query messages. Such querier is determined through election. In the beginning, all devices are of the querier state. When the devices receives multicast listener query from a device with a lower IP address, they will change from querier state to non-querier state. Therefore, only one device will be of the querier state, and this device has the lowest IP address among all multicast devices on the network.

MLDv1 also has the corresponding mechanism to handle the failure of querier device. Non-querier devices will maintain the current interval timer of other queriers. The device will reset this timer when every time it receives the multicast listener query message. If this timer times out, then the corresponding device will restart sending query message, and the new round of querier device election will begin again.

The querier device must periodically send out the multicast listener query to ensure that non-querier devices on the network know that the querier device is still workable. In realize this function, the querier device maintains a query interval timer, which will be reset when the multicast listener query message is sent out. When the query interval timer is set to zero or no longer useful, the querier device will send out another multicast listener query.

When MLD protocol is initiated, it will send a number of general query messages to discover which multicast groups shall be forwarded on the specific interface. The number of ordinary query messages sent by the device will be based on the Startup Query Count configured by the current device. The space between startup general queries will be determined by the value of Startup Query Interval. 。

When the querier device receives the leave message, it must send a group-specific multicast listener query message to see whether the host is the last listener to leave the group. The device will send a number of group-specific query messages before it stops forwarding data messages for the specific group, and the number of messages equals to the number of last listener queries. The device will send multiple group-specific multicast listener queries to ensure there is no more listener in that group. A group-specific query will be sent at every other last listener query interval in order to partition the queries. When no response is received, the device will delete the corresponding group record, and stop forwarding multicast data messages on that specific interface for this group address.

4.1.1.2 MLD Version 2

MLDV1 has the following defects in application:

Lack of effective means to control multicast sources.

Being unaware of the location of multicast source, it is comparatively difficult to establish the multicast route.

It is very difficult to discover an only multicast address. Multiple multicast groups may use the same multicast address.

On the basis of MLDv1, MLDv2 provides the additional multicast source filtering mode (INCLUDE/EXCLUDE). In MLDv1, the host determines to join a certain group only according to the group address, and receives multicast streams sent from any source to this group address. In MLDv2, the host informs the host of the multicast group it desires to join in, and also notifies this host of addresses of multicast sources that it is willing/unwilling to receive. The host can indicate which sources to receive multicast streams via an INCLUDE list or an EXCLUDE list. When the host joins a multicast group:

If the host only needs to receive the data streams sent from source {s1,s2,s3…}, then its Report message can contain the information of INCLUDE{s1,s2,s3…}.

If the host doesn't want to receive the data streams sent from source {s1,s2,s3…}, then its Report message can contain the information of EXCLUDE{s1,s2,s3…}.

Through source address filtering, MLDv2 can save network bandwidth and prevent unnecessary and invalid multicast data streams from occupying the network bandwidth. This is especially useful when multiple multicast sources are sharing one multicast address. Although MLDv1 can also realize "source address filtering" in a certain sense, it is done on the receiving end of multicast streams. As shown in Fig 1, S1 and S2 are multicast sources sending data streams with the same multicast address of G. The multicast streams of S1 and S2 will be sent to all hosts receiving G. If host A only wants to receive the data streams of S1, in order to avoid the disturbance of data streams from S2, we can only use the corresponding Client software to perform filtering.

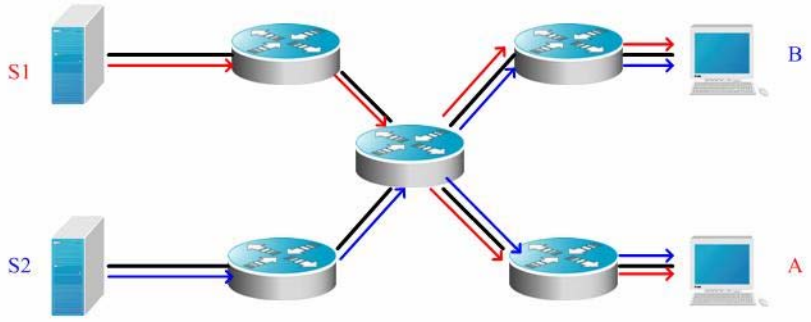


Fig 3 MLDv1 forwarding diagram

If the devices on network can support MLDv2: host A can send the MLDv2 message of join G include {S1} if it only wants to receive data streams from S1, and host B can send the MLDv2 message of join G include {S2} if it only wants to receive data streams from S2. The forwarding of data streams will be shown as follows, allowing the saving of partial bandwidth.

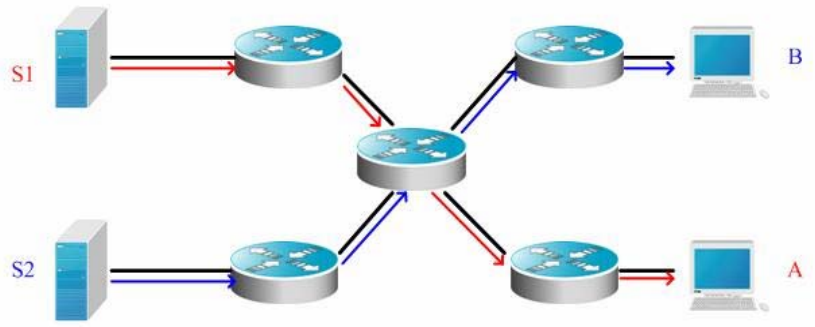


Fig 4 MLDv2 forwarding diagram

Compared with version 2, version 2 defines the following two types of messages:

- Membership Listener Query
- Membership Listener Report

Membership Query can be classified into:

General Query: Used to learn the information of all multicast listeners on the attached link;

Group-Specific Query: Used to learn the information of group-specific listeners on the attached link;

Group-and-Source-Specific Query: This type is newly added by MLDv2, and is used to learn if any of listeners on the attached link needs to receive the group-specific multicast streams sent by the specified source list.

Different from the Membership Report described in MLD Version1, the Membership Report message sent by MLD Version2 may contain the information of multiple groups. The destination address of Report message is FF02::16 in MLDv2, and can carry one ore more group records, each of which contains the group address and source address. The types of group records are shown below:

IS_IN: indicates that filtering mode between multicast group and multicast source list is INCLUDE, i.e., only the multicast data sent from the specified multicast source list to this multicast group will be received.

IS_EX: indicates that filtering mode between multicast group and multicast source list is EXCLUDE, i.e., only the multicast data sent from multicast sources outside the specified multicast source list to this multicast group will be received.

TO_IN: indicates that the filtering mode between multicast group and multicast source list will change from EXCLUDE mode to INCLUDE mode.

TO_EX: indicates that the filtering mode between multicast group and multicast source list will change from INCLUDE mode to EXCLUDE mode.

ALLOW: allows the receipt of multicast data from certain multicast sources. If the current corresponding relationship is INCLUDE, these multicast sources will be added into the existing multicast source list; if the current corresponding relationship is EXCLUDE, these multicast sources will be deleted from the existing multicast source list.

BLOCK: no longer expects to receive multicast data from certain multicast sources. If the current corresponding relationship is INCLUDE, these multicast sources will be deleted from the existing multicast source list; if the current corresponding relationship is EXCLUDE, these multicast sources will be added into the existing multicast source list.

In consideration of compatibility, MLD Version2 can also recognize the

Membership Report message and Done message of version 1.

Caution

The multicast layer-3 interface of DES-7200 router can only allow up to 253 specific sources for specific groups. The user can perform the unicast of allowed specific sources.

The multicast layer-3 interface of DES-7200 router can only filter up to 253 specific sources for specific groups. The user cannot perform the unicast of filtered specific sources.

4.1.2 MLD Protocol Specifications

The current MLD protocols include:

RFC2710: Multicast Listener Discovery (MLD) for IPv6

RFC3810: Multicast Listener Discovery Version 2 (MLDv2) for IPv6

4.2 MLD Configuration Task

MLD configuration tasks include the following items, but only some configurations are compulsory, while other tasks are optional according to the specific needs of the network. Note: The following command must be configured on the layer-3 interface.

4.2.1 Default MLD Configurations

Function	Default setting
MLD version	All interfaces support version 2
Query Response Interval	10 seconds
Query Interval	125 seconds
Multicast Group Access Control	All groups allowed
Other Querier Present Interval	255 seconds
Robustness Variable	2
Last Listener Query Interval	10 (0.1s)
Last Listener Query Count	2
MLD state	Disabled

4.2.2 Enable MLD Protocol

MLD needs to be used with multicast routing protocol. If the multicast routing protocol is enabled, the MLD protocol will also be enabled. Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if) # **ipv6 pim sparse-mode**	Enable the multicast routing protocol and MLD.

DES-7200(config-if) # **no ipv6 pim sparse-mode**	Disable the multicast routing protocol and MLD.

4.2.3 Configure MLD Version

To configure MLD version, run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if) # **ipv6 mld version** {**1|2**}	Configure the MLD version.
DES-7200(config-if) # **no ipv6 mld version**	Recover the MLD version to the default version2.

4.2.4 Configure Last Listener Query Interval

After receiving a group leave message, the querier device will send a group-specific listener query to identify that whether there are still listeners in the group. During the interval of sending last listener query, if no report is received, the device will assume that the leaving device is the last listener of the group, and will the information of this group. The default value is 1s. The Last Listener Query Interval determines the leaving speed of listeners.

Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if) # **ipv6 mld last-member-query-interval** *interval*	Configure the last listener query interval *interval*: the valid range is 1-255, in 0.1s.
DES-7200(config-if) # **no ipv6 mld last-member-query-interval**	Configure Last Listener Query Interval to default value.

4.2.5 Configure Last Listener Query Count

To avoid the loss of group-specific listener query messages sent by the querier device, the messages need to be sent for several times to guarantee reliability. Therefore, the Last Listener Query Count shall be configured.

Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if) # **ipv6 mld last-member-query-count** *count*	Configure the last listener query count. *count:* the valid range is 2-7, and the default value is 2.
DES-7200(config-if) # **no ipv6 mld last-member-query-count**	Configure the last listener query count to the default value.

4.2.6 Configure General Listener Query Interval

At every other listener query interval, the querier will periodically send out the listener query messages to verify the relationship of current listeners. The

destination address of listener query message is all-hosts, the multicast address is FF02::1, and the TTL is 1. The default value is 125 seconds.

Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if) # **ipv6 mld query-interval** *seconds*	Configure the general listener query interval. *seconds:* the valid range is 1-18000.
DES-7200(config-if) # **no ipv6 mld query-interval**	Configure the general listener query interval to the default value of 125s.

4.2.7 Configure Maximum Response Interval

This means the maximum response time required in the multicast listener query messages sent by the querier device. Less time can allow the device to rapidly learn the changes in listeners but will lead to corresponding increase in the number of potential listener reports. The network administrator can consider both factors to determine the most appropriate value, which is 10 seconds by default. Furthermore, this time shall be less than the Query Interval.

Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ipv6 mld query-max-response-time** *seconds*	Configure the maximum response time. *seconds:* the valid range is 1-25.
DES-7200(config-if)# **no ipv6 mld query-max-response-time**	Configure the maximum response time to the default value of 10s.

4.2.8 Configure Other Querier Timer Interval

The configuration of other querier timer interval can help adjust the querier device election time. This value can be decreased to increase the response speed when the querier devices are prone to change.

Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ipv6 mld query-timeout** *seconds*	Configure other querier timer interval. *seconds:* the valid range is 60-300, and the default value is 255s.
DES-7200(config-if)# **no ipv6 mld query-timeout**	Configure other querier timer interval to the default value.

4.2.9 Configure Multicast Group Access Control

By default, the host on one interface can join any multicast group. This feature can be used when the administrator expects to limit the scope of multicast groups which can be joined by the host. Configure an IP access list to allow and limit the scope of multicast group addresses, and apply the list to the specific interface.

Run the following commands:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config) # **ipv6 access-list** *access-list-name* DES-7200(config-std-nacl) # **permit ipv6** source_address *group_address*	Define an access control list.
DES-7200(config)# **interface** *interface-type interface-id*	Enter the interface configuration mode.
DES-7200(config-if) # **ipv6 mld access-group** *access-list-name*	Configure the group addresses or source addresses so that multicast groups covered by the address scope of access-list-name can access this interface.
DES-7200 (config-if) # **no ipv6 mld access-group**	Delete the access control list and allow the access of all groups.

Caution

The Multicast Group Access Control is associated with Extended ACL. When the MLD report message received is (S1,S2,S3…Sn,G), this command will perform the corresponding ACL based check of (0,G) information. Therefore, an explicit entry of (0,G) shall be configured for extended ACL to allow the normal filtering of (S1,S2,S3…Sn,G). This (0,G) mentioned herein refers to all sources of the specific group.

4.2.10 Configure Immediate Leave Group

In MLD, this command can reduce the leave latency. When there is only one host on the attached link needs to receive group information, after the host sends out the leave message, it can leave immediately without the need for the querier to device to send group-specific query. This command is used when one interface has only one receiver host.

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ipv6 mld immediate-leave group-list** *access-list-name*	Configure the immediate leave group list to access-list-name.
DES-7200(config-if) # **exit**	Return to the global configuration mode.
DES-7200(config)# **ipv6 access-list** *access-list-name* DES-7200(config-std-nacl)#**permit** *x:x:x:x::x:x/< 0-128>*	Configure the address scope of group list.

4.2.11 Configure MLD Listener Number Limit

This command can be used to limit the number of listeners that can be learned by MLD. Listener messages will not be learned after the listener number has

exceeded the limit, and no group record will be generated.

This command can be used to configure each interface, and the interface and global can be configured separately. If exceeding the number limit of interface or global configuration, the listener messages will be dropped. Run the following commands:

Command	Function
DES-7200(config)# **ipv6 mld limit** *number*	Global configuration of MLD listener number limit Please note that different models provide different limit ranges. Please identify the default value according to the capacity indicator of different models.
DES-7200(config-if) **# ipv6 mld limit** *number*	Interface configuration of MLD listener number limit Please note that different models provide different limit ranges. The default value is 1024.
DES-7200(config-if) **# ipv6 mld limit** *number* **except** *access-list-name*	The key word of Except indicates that groups covered by ACL will be limited in number.

Use the **no ipv6 mld limit** command to restore the relevant configurations to the default values.

4.2.12 Configure Host-Behavior Multicast Group Joining

Use this command to configure relevant switch interfaces to implement host behavior and join the corresponding multicast group. In this way, the sub-switches can initiatively learn the corresponding group information. This configuration can be used when a listener is required to be assigned to the interface. Use the **no** form of this command to cancel the joining operation.

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ipv6 mld join-group** *group-address*	Enable the interface to join host group.
DES-7200 (config-if) # **exit**	Return to the global configuration mode.

Use the **no ipv6 mld join-group** *group-address* command to leave the corresponding multicast group.

Caution

Some of the local link addresses have been reserved for use by the IP layer. If such addresses are used as the local link address, no group record will be generated.

4.2.13 Configure Static Multicast Group Joining

Use this command to directly assign a listener to the relevant switch interface when a listener is required to be assigned to the interface. Use the **no** form of this command to cancel the joining operation.

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200 (config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ipv6 mld static-group** *group-address*	Enable the interface to join static group.
DES-7200 (config-if) # **exit**	Return to the global configuration mode.

Use the **no ipv6 mld static-group** *group-address* command to delete the static group assigned to the interface.

4.2.14 Configure MLD Proxy-service

Use this command to enable the service of all downlink mroute-proxy interfaces, enabling the interface to become the uplink interface of corresponding mroute-proxy. It will bind all attached downlink interfaces and maintain the group information advertised by the downlink interface.

The maximum configurable number of this command is limited to 32. The number of interfaces with MLD Proxy function enabled depends on the number of multicast interfaces supported by the device. When the interface receives the query message, the proxy-service interface will give the corresponding reply according to the listener information it maintains. Such information is acquired from the mroute-proxy interface. Therefore, proxy-service interface means that it will only implement host behavior instead of router behavior. Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ipv6 mld proxy-service**	Configure the interface to proxy-service state.

Use the **no ipv6 mld proxy-service** command to disable the proxy function on the corresponding interface.

4.2.15 Configure MLD Mroute-proxy

This command will allow the interface to forward messages to the corresponding uplink interface. When the corresponding uplink interface is configured to proxy-service interface, this interface can then forward various MLD protocol messages forwarded by its listeners.

Run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if）# **ipv6 mld mroute-proxy** *interfacename*	*Interfname:* Configure the name of the corresponding uplink interface.

Use the **no ipv6 mld mroute-proxy** command to cancel the binding between downlink interface and uplink interface, and disable the proxy function of downlink interface.

4.2.16 Enable MLD SSM-MAP

Use this command to add the dynamically learned group information to the bound source record information, and is generally co-used with the **ipv6 mld ssm-map**

static command.

Run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **ipv6 mld ssm-map enable**	Enable the ssm-map function.

Use the **no ipv6 mld ssm-map enable** command to disable the SSM-MAP function.

4.2.17 Configure MLD SSM-MAP Static

Use this command together with the **ipv6 mld ssm-map enable** command. After configuring this command, the MLDv1 messages received will be mapped to the corresponding source records.

Run the following command in the global configuration mode:

Command	Function
DES-7200(config）# **ipv6 mld ssm-map static** *acl_name src_address*	Map all group records complying with acl_name to the source address of src_address.

Use the **no ipv6 mld ssm-map static** command to cancel the mapping relationship between related group record and source address.

4.3 Monitor and Maintain MLD State and Listener Information

4.3.1 Clear the dynamic listener information in the MLD cache

Use this comamnd to clear the dynamic listener information in the MLD cache. Note that this command cannot delete the statically added listener information. Run the following command in the privilege mode:

Command	Function
DES-7200# **clear ipv6 mld group** [*group-address*] [*interface-type interface-number*]	Clear all dynamic listener information in the MLD cache learned from response message. Clear all mld group information if there is no parameter.

4.3.2 Clear all information in MLD cache on the specific interface

To clear all information in MLD cache on the specific interface, run the following command in the privilege mode:

Command	Function
DES-7200# **clear ipv6 mld interface** *interface-type*	Clear all information in MLD cache on the interface.

4.3.3 Display the state of listeners on the attached subnetwork

To display the state of all listeners on the attached subnetwork, run the following commands in the privilege mode:

Command	Function
DES-7200# **show ipv6 mld groups**	Display the information of all listeners learned by MLD.
DES-7200# **show ipv6 mld groups detail**	Display the detailed information of all listeners learned by MLD.
DES-7200# **show ipv6 mld groups** *x:x:x:x::x*	Display the information of group-specific listeners learned by MLD.
DES-7200# **show ipv6 mld groups** *x:x:x:x::x* **detail**	Display the detailed information of group-specific listeners learned by MLD.
DES-7200# **show ipv6 mld ssm-mapping**	Display the configuration information of ssm-mapping.
DES-7200# **show ipv6 mld ssm-mapping** *x:x:x:x::x*	Display the source address mapping information of specific group.
DES-7200# **show ipv6 mld groups** *interface-type* **detail**	Display the detailed information of all groups on the specific interface.
DES-7200# **show ipv6 mld groups** *interface-type x:x:x:x::x*	Display the information of specific groups on the specific interface.
DES-7200# **show ipv6 mld groups** *interface-type x:x:x:x::x* **detail**	Display the detailed information of specific groups on the specific interface.

4.3.4 Display the configuration information of MLD interface

To display the configuration information of MLD interface, run the following commands in the privilege mode:

Command	Function
DES-7200# **show ipv6 mld interface** *interface-type interface-number*	Display the MLD interface configurations.
DES-7200# **show ipv6 mld interface**	Display the configurations of all MLD interfaces.

4.3.5 Display the on/off state of MLD debug switch

To display the on/off state of MLD debug switch, run the following command in the privilege mode:

Command	Function
DES-7200# **show debugging**	Display the on/off state of MLD debug switch.

4.3.6 Turn on MLD debug information switch and observe MLD behaviors

To turn on MLD debug information switch and observe MLD behaviors, run the following command in the privilege mode:

Command	Function
DES-7200# **debug ipv6 mld all**	Turn on all MLD debug information switches
DES-7200# **debug ipv6 mld decode**	Turn on MLD debug message decoding switch.
DES-7200# **debug ipv6 mld encode**	Turn on MLD debug message encoding switch.
DES-7200# **debug ipv6 mld events**	Turn on MLD debug event information switch.
DES-7200# **debug ipv6 mld fsm**	Turn on MLD debug state switch.
DES-7200# **debug ipv6 mld tib**	Turn on MLD debug member tree structure information switch.
DES-7200# **debug ipv6 mld warnning**	Turn on MLD debug warning switch.

5 PIM-DM Configuration

5.1 PIM-DM Overview

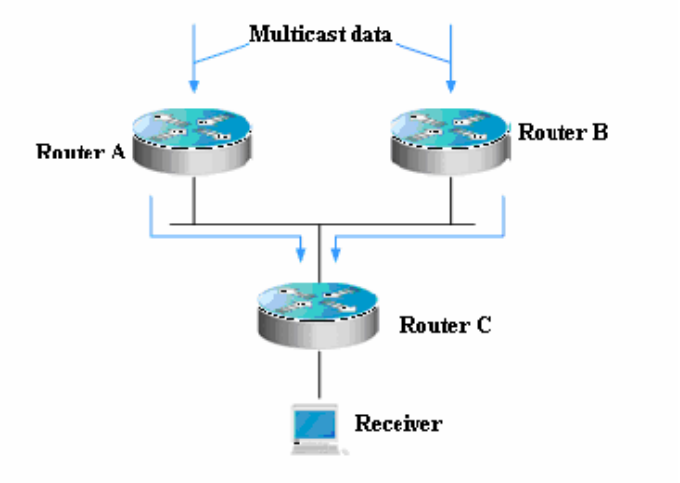
PIM-DM (Protocol Independent Multicast-Dense Mode), a multicast routing protocol in dense mode, is suitable for the environments of small network size and centralized multicast members. Since PIM-DM does not rely on any specific unicast routing protocol, it is called protocol independent multicast routing protocol. PIM-DM is defined in RFC 3973.

PIM-DM devices discover neighbors through Hello messages. After start, a PIM-DM device sends a Hello message to the PIM-DM-enabled interface periodically. The Hello message has a field called Hello Hold Time, which defines the period that a neighbor waits for the next message. If the neighbor has not received the next Hello message from the sender within this period, it announces the device's death.

PIM-DM sets up a multicast tree through flood and prune. Assume that when a multicast source begins to send a multicast packet, all the systems in the network need to receive this packet. As a result, this packet is forwarded to every system. The reverse path forwarding check is done for the packets received from the upstream interface. Those packets who fail to pass the check will be dropped. For the packets passing the check, the egress is calculated based on the (S, G) pair of the packets, or 从 source address and group address. If the egress exists, an egress entry is set up fro the (S, G) pair and the multicast packet is forwarded through this egress. If the calculated egress is null, a prune message is sent to RPF, informing the upstream neighbor not to forward the multicast packets from the (S, G) pair to this egress. Upon receiving the prune message, the upstream interface marks the sending interface as pruned status, and set a pruned state timer. In this way, a multicast forwarding tree at the root of multicast source is set up.

PIM-DM utilizes the Assert mechanism to eliminate redundant routes.

Figure 1-4 Figure 4 PIM-DM's Assert mechanism



As shown in the above figure, the multicast data arrives at Router A and B at the same time, which forward the data to Router C. In this case, Router C receives two copies of the data. This is not allowed. So there must be a mechanism to select Router A or B to forward the multicast data to Router C. This is the Assert mechanism of PIM-DM.

PIM-DM uses the state refresh message to update network state. The device directly connecting to the multicast source sends the state refresh message to the downstream devices periodically to inform topology change. The devices receiving the message add their topology state to the state refresh message by modifying some fields, and then send to the downstream devices. When the refresh message arrives the leaf devices, the whole network state is updated.

PIM-DM utilizes the Graft mechanism to reestablish the connection with upstream devices. If the network topology of a downstream device in pruned state changes and needs to receive multicast data from a (S, G) pair, it sends the graft message to the upstream device. Upon receiving the graft message, the upstream device responds with a Graft-Ack message and forwards the multicast data to the downstream device again.

5.2 PIM-DM Configuration Task

The PIM-DM configuration covers the following items. However, only the first and second one are mandatory, and others are optional.

5.2.1 Enabling Multicast Routing

The multicast protocol can receive and process multicast packets and protocol packets only when the multicast routing forwarding function is enabled.

In the global configuration mode, execute the following command to enable the multicast routing forwarding function:

Command	Function
DES-7200 (config) # **ip multicast-routing**	Enable multicast routing forwarding.
DES-7200 (config) # **no ip multicast-routing**	Disable multicast routing forwarding.

5.2.2 Enabling PIM-DM

PIM-DM should be enabled on individual interface. Once PIM-DM is enabled on an interface of a device, the device can exchange PIM-DM control messages with other devices, maintain and update the multicast route table and forward multicast messages.

To configure PIM-DM on an interface, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip pim dense-mode**	Enable the PIM-DM protocol on the interface.
DES-7200(config-if)# **no ip pim dense-mode**	Disable the PIM-DM protocol on the interface.

The following example shows how to enable PIM-DM on GigabitEthernet 4/3.

```
DES-7200(config)# ip multicast-routing
DES-7200(config)# interface gigabitEthernet 4/3
DES-7200(config-if)# ip address 192.168.194.2 255.255.255.0
DES-7200(config-if)# ip pim dense-mode
```

Note

Enabling PIM-DM will take effect on an interface only when the multicast routing is enabled in the global configuration mode.

When this command is configured, if the “Failed to enable PIM-DM on <interface name>, resource temporarily unavailable, please try again” occurs, retry to configure this command.

When this command is configured, if the “PIM-DM Configure failed! VIF limit exceeded in NSM!!!” appears, It indicates current allowed interface configuration exceeds the upper limit of the multicast interfaces. Please remove some unnecessary PIM-SM or DVMRP interface.

It is not recommended to configure different IPv4 multicast routing protocols on different interfaces of a switch or router.

If the interface is of tunnel-type, only 4Over4 configuration tunnel, 4Over4GRE tunnel, 4Over6 configuration tunnel and 4Over6 GRE tunnel support the IPv4 multicasting at the moment. The multicasting can be also enabled on other tunnel interfaces that doe not support the multicasting, but no error message will be displayed and no multicast packets will be received and sent.

The multicast tunnel can be created on the Ethernet interface only, nested tunnel and multicast data Qos/ACL are not supported.

5.2.3 Setting the Interval of Sending the Hello Message

After the PIM-DM is enabled on an interface, the interface will send the Hello message to the interfaces of adjacent devices at an interval. You can modify the interval according to the real network circumstances.

To configure the interval of sending the Hello message, use the following command in the interface configuration mode:

Command	Function
DES-7200(config-if）# **ip pimquery-interval** *interval-seconds*	Set the interval of sending the Hello message on the interface. *interval-seconds*: in the range 1 to 65535
DES-7200(config-if）# **no ip pimquery-interval**	Restore the interval of sending the Hello message on the interface to the default value.

By default, the interval of sending the Hello message on the interface is 30s.

Note

When the interval of sending the Hello message is updated, the Hello hold time will be updated as 3.5 times of the Hello sending interval automatically. If the interval of sending Hello message multiplying 3.5 is larger than 65535, the Hello message hold time should be updated to 65535.

5.2.4 Configuring the propagation-delay of Hello Message

To configure the propogation delay of Hello message, run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip pim propagation-delay** *interval-milliseconds*	Set the propagation delay in the range of 1 to 32767 milliseconds.
DES-7200(config-if)# **no ip pim propagation-delay**	Restore the setting to the default value, 500 milliseconds by default.

5.2.5 Configuring the override-interval of Hello Message

To configure the override-interval, run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if)# **ip pim override-interval** *interval-milliseconds*	Set the override interval in the range of 1 to 65535 milliseconds.
DES-7200(config-if)# **no ip pim override-interval**	Restore the setting to the default value, 2500 milliseconds by default.

5.2.6 Configuring PIM-DM Neighbor Filtering

Neighbor filtering function can be configured on the interface to enhance network security. With neighbor filtering enabled, the PIM-DM will not establish the neighborhood relationship with the neighbor or stop the currently established neighborhood relationship with the neighbor as long as a neighbor is denied by the access list.

To configure the PIM neighbor filtering function, run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if）#**ip pim neighbor-filter** *access-list*	Enable the PIM neighbor filtering function on the current interface.
DES-7200(config-if）#**no ip pim neighbor-filter** *access-list*	Disable the PIM neighbor filtering function on the current interface.

The PIM neighbor filtering function is disabled by default on an interface.

Note

ip pim neighbor-filter command description:

When the associated ACL rule is set to permit, only the neighbor addresses in the ACL list can be considered to be the PIM neighbor of the current interface. When the associated ACL rule is set to deny, the neighbor addresses in the ACL list cannot be considered to be the PIM neighbor of the current interface.

5.2.7 Configuring PIM-DM Status Refresh

At administration mode, it is permitted to forward PIM-DM state refresh control message by default. For the first-hop router directly connected to the source, the interface configuration state refresh interval is the interval at which the state refresh packets are sent. In this case, it is only effective for the upstream interfaces. For subsequent routers, it is the interval at which the interfaces are allowed to receive and process the state refresh packets.

Command	Function
DES-7200(config-if）#**no ip pim state-refresh disable**	Enable processing or forwarding PIM-DM status refresh messages.
DES-7200(config-if）# **ip pim state-refresh disable**	Disable processing or forwarding PIM-DM status refresh message.

The PIM-DM status refresh function is enabled by default.

Caution

Disabling the status update messages may cause the re-convergence of the converged PIM-DM multicast forward tree, resulting in unnecessary bandwidth waste and routing table vibration. Therefore, it is better not to disable the status update function.

5.2.8 Configuring the Interval of Sending PIM-DM Status Refresh Message

When the PIM-DM is enabled on the device, if some interface is directly connected with the multicast source, the status refresh messages will be sent to the downstream device on regular basis, so as to refresh the statuses of the whole network. You can modify the interval of sending PIM status refresh message on an interface according to the real network circumstances.

To configure the interval of sending PIM status message on the interface, run the following command in the interface configuration mode:

Command	Function
DES-7200(config-if）#**ip pim state-refresh origination-interval** *seconds*	Configure the interval of sending PIM status refresh message on the current interface as “seconds”, where “seconds” is an integer within 1-100, in seconds.
DES-7200(config-if）#**no ip pim state-refresh origination-interval**	Cancel the configuration of the PIM flood delay on the current interface.

By default, the interval of sending PIM status refresh message on the interface is 60 seconds.

Note

Only the devices directly connected to multicast source can periodically send the PIM status updated message to the downward interfaces. Thus, if the devices are not directly connected to the multicast source, the forwarding interval of PIM status update message configured on the downstream interface is invalid.

5.3 Monitoring and Maintaining PIM-DM

5.3.1 Viewing PIM-DM Status Information

Command	Function

Command	Function
DES-7200 # **show ip pim dense-mode interface** [*interface-type interface-number]* [**detail**]	Show the PIM-DM information on the interface.
DES-7200 # **show ip pim dense-mode neighbor** [*interface-type interface-number*]	Show the PIM-DM neighbor information.
DES-7200 # **show ip pim dense-mode nexthop**	Show the next hop information of PIM-DM.
DES-7200#**show ip pim dense-mode mroute** [*A.B.C.D A.B.C.D*] [**summary**]	Show the PIM-DM routing table.
DES-7200 #**show ip pim dense-mode track**	Show the number of PIM packets transmitted from the statistical beginning time.

For details on the use of the above command, see *PIM-DM Command References*.

Here are some examples of the commands:

show ip pim dense-mode interface detail command:

```
DES-7200# show ip pim dense-mode interface detail
FastEthernet 0/45 (vif-id: 3):
Address 10.10.10.10
Hello period 30 seconds, Next Hello in 15 seconds
Over-ride interval 2500 milli-seconds
Propagation-delay 500 milli-seconds
Neighbors:
10.10.10.1
VLAN 4 (vif-id: 2):
Address 50.50.50.50
Hello period 30 seconds, Next Hello in 2 seconds
Over-ride interval 2500 milli-seconds
Propagation-delay 500 milli-seconds
Neighbors:
50.50.50.1
```

In the example above, the IP address of FastEthernet 0/45 is 10.10.10.10, the Hello message sent interval 30 seconds, next Hello message to be sent in 15 seconds, and the neighbor address 10.10.10.1. The VLAN4 has similar information as FastEthernet 0/45.

show ip pim dense-mode neighbor command:

```
DES-7200# show ip pim dense-mode neighbor
Neighbor-Address Interface            Uptime/Expires    Ver
10.10.10.1      FastEthernet 0/45     00:19:29/00:01:21  v2
50.50.50.1      VLAN 4                00:22:09/00:01:39  v2
```

In the example above, the device has two neighbors, where neighbor 10.10.10.1 is connected with FastEthernet 0/45 and has survived for 19 minutes and 29 seconds, with neighbor survival period to expire in one minute and 21 seconds. Neighbor 50.50.50.1 is similar.

show ip pim dense-mode nexthop command:

```
DES-7200# show ip pim dense-mode nexthop
Destination  Nexthop   Nexthop      Nexthop       Metric Pref
               Num      Addr        Interface
1.1.1.111      1      50.50.50.1    VLAN 4          0     1
```

As shown in the above example, the next hop neighbor address to the multicast source 1.1.1.111 is 50.50.50.1 and the egress is VLAN4.

show ip pim dense-mode mroute command:

```
DES-7200# show ip pim dense-mode mroute
PIM-DM Multicast Routing Table
(1.1.1.111, 229.1.1.1)
MRT lifetime expires in 205 seconds
```

```
RPF Neighbor: 50.50.50.1, Nexthop: 50.50.50.1, VLAN 4
Upstream IF: VLAN 4
Upstream State: Pruned, PLT:200
Assert State: NoInfo
Downstream IF List:
FastEthernet 0/45:
Downstream State: NoInfo
Assert State: Loser, AT:170
```

The above example shows two entries: 1.1.1.111 and 229.1.1.1, where MRG aging time is 205 seconds, RPF neighbor is 50.50.50.1, the next hop is 50.50.50.1, the egress to the next hop is VLAN 4. The upstream interface of these entries is VLAN 4 in Pruned status at present, indicating that there is no downstream forwarding egress. The downstream interface is FastEthernet 0/45 in Noinfor status. The Assert state of the interface is Loser. FastEthernet is not included in the forwarding egress.

show ip pim dense-mode track Command:

```
DES-7200# show ip pim dense-mode track
PIM packet counters
Elapsed time since counters cleared: 00:04:03

                           received    sent
Valid PIMDM packets:         1           8
Hello:                       1           8
Join/Prune:                  0           0
Graft:                              0              0
Graft-Ack:                   0              0
Assert:                          0              0
State-Refresh:               0              0
PIM-SM-Register:             0              0
PIM-SM-Register-Stop:       0               0
PIM-SM-BSM:                  0              0
PIM-SM-C-RP-ADV:             0              0
Unknown Type:                    0

Errors:
Malformed packets:           0
Bad checksums:               0
Unknown PIM version:         0
Send errors:                     0
```

5.3.2 Deleting PIM-DM Status Information

Use the following command to delete the PIM-DM status information:

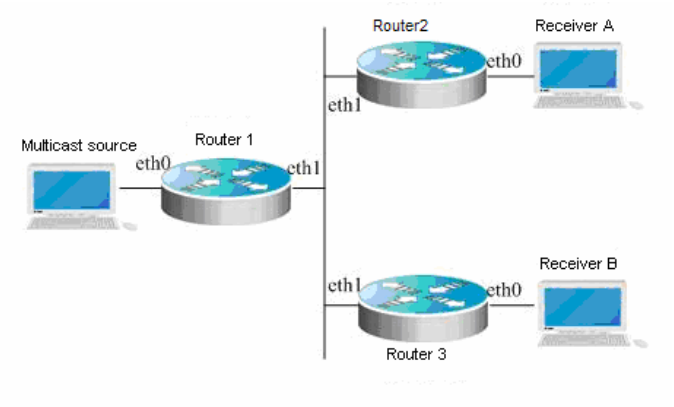
Command	Function
DES-7200# **clear ip pim dense-mode track**	Reset the statistical beginning time and clear the counter for the PIM packets.

5.4 PIM-DM Configuration Example

- **Configuration Requirements**

The network topology is shown in the following figure. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network, and device 3 and receiver B locate in the same network. Suppose the devices are connected with the host correctly and the IP addresses are configured.

Example of PIM-DM networking diagram



Device Configuration

Take the device 1 as an example to show how to configure PIM-DM. The steps of device 2 and 3 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7200# configure terminal
DES-7200(config)# ip multicast-routing
```

Step 2: Enable PIM-DM on the interface eth0

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ip pim dense-mode
DES-7200(config-if)# exit
```

Step 3: Enable PIM-DM on the interface eth1 and return to the privileged user mode.

```
DES-7200(config)# interface eth 1
DES-7200(config-if)# ip pim dense-mode
DES-7200(config-if)# end
```

The configuration of device 2 and 3 is similar to device 1.

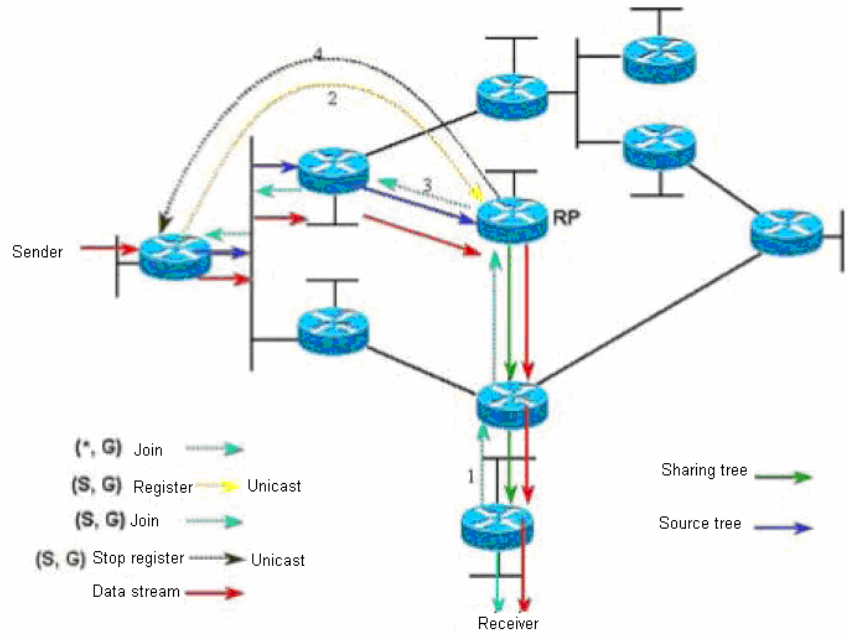
Note that once PIM-DM is enabled, IGMP is enabled on various interfaces automatically without manual configuration.

6 PIM-SM Configuration

6.1 PIM-SM Overview

The Protocol Independent Multicast Sparse Mode (PIM-SM) is a protocol independent multicast sparse mode. In a PIM-SM domain, the PIM-SM-enabled device sends the Hello message to discover adjacent PIM-SM devices and selects the designated router (DR) in a multi-access network. The DR is responsible for sending the join/prune message in the root node of the multicast distribution tree direction for the direct connection group member, or sending the data of the direct connection multicast source to the multicast distribution tree.

Join/Prune Mechanism of PIM-SM



The PIM-SM forwards multicast data packets by establishing a multicast distribution tree. The multicast distribution tree is divided into two types: Shared Tree that takes the RP of the group G as the root and Shortest Path Tree that takes the multicast source as the root. The PIM-SM establishes and maintains the multicast distribution tree with the explicit join/prune mechanism.

As shown in the above figure, when the DR receives a join request from the receiving terminal, it will multicast a (*.G) join message hop-by-hop to the RP of the group G to join the shared tree. When the source host sends multicast data to the group, the source data is encapsulated into the registration message and unicasted by the DR to the RP. Then the RP will forward the decapsulated data packets to group members along the shared tree. The RP will send a (S, G) join message to the first hop on the source direction to join the shortest path tree of this source. In this way, the source's data packets are sent to the RP without encapsulation along its shortest path tree. When the first multicast data reaches

along this tree, the RP will send the registration stop message to the DR of the source, notifying the DR of stopping registration. Consequently, the source's multicast data packets are sent to the RP along its shortest path tree rather than being registered and encapsulated. Then the RP forwards the data packets to group members along the shared tree. When there is no need of multicast data packets, the DR multicasts a prune message to the RP of the group G hop-by-hop to prune the shared tree.

The PIM-SM also offers a mechanism of select the root point (RP). One or more Candidate-BSRs are configured in a PIM-SM domain. The PIM-SM selects a BSR by following a certain rule. There are also Candidate-RPs in a PIM-SM domain that unicast the packets including their IP addresses and available multicast groups to the BSR. The BSR will periodically generate a BSR message which includes a system candidate RP and the corresponding multicast group address. The BSR messages are sent hop-by-hop within the whole domain. The device receives and saves these BSR messages. If the DR receives a report on the member relationship of a multicast group from its directly connected host but has no route entries of the multicast group, the DR will use one Hash algorithm to map the multicast group address to a candidate RP that can serve this group. Then, the DR multicasts the Join/Prune message to the RP hop-by-hop. If the DR receives multicast data packets from its directly connected host but has no route entries of the multicast group, the DR will use one Hash algorithm to map the multicast group address to a candidate RP that can serve this group. Then the DR encapsulates multicast data packets into the registration message and unicasts it to the RP.

The main difference between the PIM-SM and the broadcast/prune model-based PIM-DM is that the PIM-SM is based on the explicit join model. In other words, the receiver sends the join message to the RP, while the router only forwards the packets of that multicast group on the outbound interface that has joined a multicast group. The PIM-SM uses the shared tree to forward multicast packets. Each group has a Rendezvous Point (RP). The multicast source sends the data to the RP along the shortest path, and then the RP sends the data to the receivers along the shortest path. This is similar to the CBT, but the PIM-SM does not use the concept of core. One of the major advantages of the PIM-SM is that it not only receives multicast messages through the shared tree but also provides a shared tree-to-SPT conversion mechanism. Such conversion reduces network delay and possible congestion on the RP, but it consumes enormous router resources. So it is suitable for the case where there are only a few multicast data sources and network groups.

The PIM-SM uses the shared tree and SPT to distribute multicast frames. At this time, it is assumed that other devices don't want to receive these multicasts unless otherwise stated definitely. When a host joins a group, the equipment connected to the host must notify the root (or the RP) by using the PIM join message. This join message is transferred one after another through the routers to create a shared tree structure. Therefore, the RP records the transfer path and also the registration message from the first hop router (DR) of the multicast source, and improves the shared tree upon these two messages. The branch/leaf messages are updated by periodically querying messages. With the shared tree, the multicast source first sends multicast packets to the RP, guaranteeing that all the receivers can receive them.

The PIMv2 BSR is a method of distributing the group-to-RP message to all devices without the need of setting the RP for them. The BSR uses the hop-by-hop broadcast BSR message to distribute the mapping message. At first, the BSR is selected among routers in the same process as selecting a root bridge based on priority level among layer 2 bridges. Each BSR checks the BSR messages and only forwards those having a priority higher than or equal to its own (higher IP address). The selected BSR sends its BSR message to the all-PIM-routers multicast group (224.0.0.13), where TTL is 1. After the adjacent

PIMv2 router receives the message, it multicasts it while setting the TTL to 1. In this way, the BSR message is received by all devices hop-by-hop. Since the message contains the IP address of the BSR, the candidate BSR can know which router is the current RP based on this message. The candidate RPs send candidate RP advertisements to announce in which address ranges they can become an RP. The BSR stores them in its local candidate RP cache. The BSP notifies all PIM routers of its local candidate RPs periodically. These messages reach various devices hop-by-hop in the same way.

6.2 Configuration Preparation

Before configuring the PIM-SM, you shall enable a unicast routing protocol to find the routing automatically.

6.3 PIM-SM Configuration Task

The PIM-SM configuration covers the following items. However, only the first one is mandatory, and others are optional.

6.3.1 Configuring Multicast Routing

Multicast packets can be forwarded only after multicast routing is enabled and enabling PIM-SM makes sense.

To enable multicast routing, run the following command in the global configuration mode.

Command	Function
ip multicast-routing	Enable multicast routing globally.
no ip multicast-routing	Disable multicast routing globally.

6.3.2 Enabling PIM-SM

The PIM-SM must be enabled on every port. Only after the PIM-SM is enabled on its ports can the device exchange PIM-SM control messages with other devices, maintain and update multicast routing table, and forward multicast packets.

To enable the PIM-SM on the interface, execute the following command in the interface mode:

Command	Function
DES-7200(config-if)# **ip pim sparse-mode**	Enable the PIM-SM protocol on the interface.
DES-7200(config-if)# **no ip pim sparse-mode**	Disable the PIM-SM protocol on the interface.

Note

Enabling the PIM-SM on the interface takes effect only when the multicast routing is enabled in the global configuration mode.

When the system prompts "Failed to enable PIM-SM on <Interface Name>, resource temporarily unavailable, please try again", re-execute this command.

When the system prompts "PIM-SM Configure failed! VIF limit exceeded in NSM!!!", it indicates that the configured interfaces exceed the upper limit of the multicast interfaces. In this case, delete the unnecessary PIM-SM interfaces.

It is not recommended to configure different IPv4 multicast protocols on different interfaces of a switch/router.

If the interface is of tunnel-type, only 4Over4 configuration tunnel, 4Over4GRE tunnel, 4Over6 configuration tunnel and 4Over6 GRE tunnel support the IPv4 multicasting at the moment. The multicasting can be also enabled on other tunnel interfaces that doe not support the multicasting, but no error message will be displayed and no multicast packets will be received and sent.

The multicast tunnel can be created on the Ethernet interface only, nested tunnel and multicast data Qos/ACL are not supported.

6.3.3 Configuring the Interval of Sending the Hello Message

When the PIM-SM is enabled on the interface, the device periodically sends Hello messages to the interfaces of neighbors. You can set the interval of sending Hello messages according to real network environment.

To configure the interval of sending the Hello message, execute following commands in the interface mode:

Command	Function
DES-7200(config-if)# **ip pim query-interval** *interval-seconds*	Set the interval of sending the Hello message. *interval-seconds*: in the range of 1 to 65535 seconds
DES-7200(config-if)# **no ip pim query-interval**	Restore the interval of sending the Hello message to the default value.

The interval of sending the Hello message on the interface is 30 second by default.

Note

When the interval of sending Hello message is changed, the hold time of Hello message also changes by the following rule. The hold time becomes 3.5 times of the interval of sending Hello message. If the interval multiplying 3.5 is larger than 65535, the hold time is set to 65535.

6.3.4 Configuring the Propagation Delay of the Hello Message

To configure the propagation delay of the hello message, execute following commands in the interface mode:

Command	Function
ip pim propagation-delay *interval-milliseconds*	Set the propagation delay in the range of 1 to 32767 milliseconds.
no ip pim propagation-delay	Restore the setting to the default value, 500 milliseconds by default.

Note

Modifying propagation delay or prune deny delay will affect J/P-override-interval. As specified in the protocol, J/P-override-interval must be less than the hold time of Join-Prune message, or otherwise streams may be interrupted temporarily.

6.3.5 Configuring the Override Interval of the Hello Message

To configure the override interval of the hello message, execute following commands in the interface mode:

Command	Function

Command	Function
ip pim override-interval *interval-milliseconds*	Set the override interval in the range of 1 to 65535 milliseconds.
no ip pim override-interval *interval-milliseconds*	Restore the setting to the default value, 2500 milliseconds by default.

Note

Modifying propagation delay or prune deny delay will affect J/P-override-interval. As specified in the protocol, J/P-override-interval must be less than the hold time of Join-Prune message, or otherwise streams may be interrupted temporarily.

6.3.6 Configuring the Neighbor Tracking of the Hello Message

The T bit of the LAN Prune Delay Option of the Hello message indicates whether to enable join restriction on the interface. When join restriction is enabled on the interface, the Join message sending to the upstream neighbor will be restricted on the interface, namely it will not be sent to the upstream neighbor, upon the receipt of the Join message from its neighbor to the upstream neighbor. If this function is disabled, the Join message sending to the upstream neighbor will still be sent on the interface upon the receipt of the Join message from its neighbor to the upstream neighbor. Moreover, if join restriction is enabled on all downstream receivers, the upstream router can track these receivers by received Join messages. By default, this function is disabled on the interface.

To disable join restriction on the interface, execute following commands in the interface mode:

Command	Function
ip pim neighbor-tracking	Disable join restriction on the interface.
no ip pim neighbor-tracking	Enable join restriction on the interface.

6.3.7 Configuring the Triggered Hello Delay of the Hello Message

When a router starts or detects new neighbor, the router will send the Hello message at random to avoid blocking. This random interval can be calculated based on triggered hello delay, which is 5 seconds by default.

To set triggered hello delay, execute following commands in the interface mode:

Command	Function
ip pim triggered-hello-delay *interval-seconds*	Set the triggered hello delay in the range of 1 to 5 seconds.
no ip pim triggered-hello-delay	Restore the setting to the default value.

Note

Modifying propagation delay or prune deny delay will affect J/P-override-interval. As specified in the protocol, J/P-override-interval must be less than the hold time of Join-Prune message, or otherwise streams may be interrupted temporarily.

6.3.8 Configuring PIM-SM Neighbor Filtering

You can filter neighbors on an interface to enhance network security. With this function enabled, when a neighbor is denied by an ACL, the PIM-SM will not establish the adjacency relationship with that neighbor or remove the currently

established adjacency relationship with that neighbor.

To configure the PIM-SM neighbor filtering function, run the following command in the interface mode:

Command	Function
DES-7200(config-if)# **ip pim neighbor-filter** *access-list*	Enable the PIM neighbor filtering function on the interface.
DES-7200(config-if)# **no ip pim neighbor-filter** *access-list*	Disable the PIM neighbor filtering function on the interface.

The PIM-SM neighbor filtering function is disabled by default on an interface.

Note

A device can become the PIM-SM neighbor of the interface only when its IP address matches the associated ACL whose rule is permit.

6.3.9 Configuring the Priority of DR

This command is used to configure the priority of the designated router (DR), higher weight means higher priority.

To configure the priority of DR, run the following commands in the interface mode:

Command	Function
DES-7200(config-if)# **ip pim dr-priority** *priority-value*	Configure the priority in the range of 0 to 4294967294.
DES-7200(config-if)# **no ip pim dr-priority** *priority*	Restore the DR priority to the default value, namely 1.

6.3.10 Configuring Static RP

In a small network, you can configure static RP to use PIM-SM. This requires all the devices in the PIM-SM domain have the same static RP configuration and ensure no ambiguity of the PIM-SM multicast routes.

To configure static RP, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim rp-address** *rp-address* [*access-list*]	Configure static RP on the local device.
DES-7200(config)# **no ip pim rp-address** *rp-address* [*access-list*]	Remove the static RP configuration.

Caution

Attention should be attained to following points when using this command:

If both the BSR and static RP configurations take effect simultaneously, the static RP takes precedence.

The static RP address can be configured for multiple multicast groups (by ACL) or all multicast groups (not by ACL). However, a static RP address cannot be configured for several times.

If more than one static RP are configured for a multicast group, the one with the highest IP address takes effect.

Only the permitted addresses defined in the ACL are invalid multicast groups. By default, 0.0.0.0/0 refers to filter all multicast groups (224/4).

After configuration, the static RP source address is inserted into the tree of

group-based static RP group. Each static multicast group maintains the link table structure of a static RP group. The link tables are ordered in descending sequence by IP addresses. When a RP is selected for a group, the first element, namely, the RP with the highest IP address is firstly selected.

Deleting a static RP address deletes the address from all groups that has this address, and one address is selected from the existing tree structure as the RP address.

6.3.11 Configuring the Device as the Candidate BSR

This command configures a device to be a candidate BSR to generate the globally-unique BSR in the PIM-SM domain, which will collect and distribute RPs in the domain so as to ensure the uniqueness of RP mapping in the domain.

To configure the device as the candidate BSR, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority-value*]	Configure the device as the candidate BSR to learn and contest the global BSR role through BSM messages. *hash-mask-length*: in the range 0 to 32, 10 by default *priority-value*: in the range 0 to 255, 64 by default
DES-7200(config)# **no ip pim bsr-candidate** *interface-type interface-number*	Remove the configuration.

6.3.12 Configure the BSR Border

To restrict BSM flooding, you can set the BSR border on the interface so that BSM will be dropped immediately rather than being forwarded.

To configure the BSR border, execute the following commands in the interface configuration mode:

Command	Function
ip pim bsr-border	Set the BSR border.
no ip pim bsr-border	Remove the configuration.

6.3.13 Ignoring the RP Priority in RP-SET

When you compare two RPs to select one for a multicast IP address, execute this command to ignore the RP priority. Otherwise, the RP priority would be taken into account during comparison.

To ignore the RP priority, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim ignore-rp-set-priority**	Ignore the RP priority in the RP-Set.
DES-7200(config)# **no ip pim ignore-rp-set-priority**	Take into account the RP priority in the RP-Set.

6.3.14 Configuring Candidate RP

Candidate RP advertisement is sent to the BSR at intervals and then propagated to all the PIM-SM devices in the domain, and thus ensuring the uniqueness of RP mapping.

To configure the candidate RP, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *access-list*]	Configure the device as the candidate RP. *priority-value*: in the range of 0 to 255, 192 by default *interval-seconds*: in the range 1 to 16383, 60s by default *access-list*: All multicast groups are permitted, that is 224/4
DES-7200(config)# **no ip pim rp-candidate** *interface-type interface-number*	Remove the candidate RP configuration.

Note

You can use the ACL to specify a port as the candidate RP of a particular group. It should be noted that the group calculation is based on the permit ACE only, not the deny ACE.

Caution

The source IP address of ACE is used as the specific group range for matching.

6.3.15 Checking the Reachability for RPs

This command detects whether the RPs sent from DR can reach the destination device.

To check the reachability of RPs, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim register-rp-reachability**	Check the reachability of RPs.
DES-7200(config)# **no ip pim register-rp-reachability**	Disable this function.

6.3.16 Filtering the Addresses of Register Packets

Execute the **ip pim accept-register list** *access list* command to filter the pair of source IP address and multicast group IP address of reached register packets. Otherwise, every reached register packet is permitted.

To filter the addresses of register packets, execute the following commands in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **ip pim accept-register list** *access-list*	Filter the pair of source IP address and multicast group IP address of register packets.
DES-7200(config)# **no pim accept-register**	Remove the configuration.

6.3.17 Configuring the Speed Limit on Sending RPs

This command configures the speed at which the DR sends registration packets in (S, G). No speed limit is configured by default.

To configure the speed limit on sending RPs, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim register-rate-limit** <*1-65535*>	Set the maximum number of RP packets sent per second in the range of 1-65535.
DES-7200(config)# **no ip pim rp-candidate**	Remove the configuration.

6.3.18 Calculating the Checksum of Register Packets in Cisco 's Way

Execute the **ip pim cisco-register-checksum** command to calculate the checksum of register packets in Cisco's way. Otherwise, the checksum of register packets is calculated in default way specified by the protocol.

To calculate the checksum of register packets in Cisco's way, execute the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ip pim cisco-register-checksum** [**group-list** *access-list*]	Calculate the checksum of register packets in Cisco's way. **group-list** *access-list*: Apply this configuration to all multicast addresses by default.
DES-7200(config)# **no ip pim cisco-register-checksum** [**group-list** *access-list*]	Remove the configuration.

6.3.19 Configuring the RP to Forward Multicast Packets to Downstream Interfaces after Decapsulating Register Packets

To decapsulate the register packet and forward its multicast packets, execute the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ip pim register-decapsulate-forward**	Decapsulate the register packet and forward its multicast packets
DES-7200(config)# **no ip pim register-decapsulate-forward**	Remove the configuration.

In case of decapsulation and forwarding of many register packets, this function incurs additional workload to CPU. So it is not recommended.

Caution

6.3.20 Limiting the Range of Legal BSRs

To limit the range of legal BSRs, execute the following command in the global configuration mode. Without this function, PIM-SM-enabled routers will receive all external BSM messages.

Command	Function
ip pim accept-bsr list { <1-99> | <1300-1999> | WORD }	Configure the legal BSR range.
no ip pim accept-bsr list	Remove the configuration.

Caution

This command filters the BSR field of the BSM message. If this address is denied by ACL, the BSM message is filtered.

6.3.21 Configuring the Electing BSR to Limit the Legal CRP Address Range and the Multicast Group Range It Serves

To configure the electing BSR to limit the legal CRP address range and the multicast group range it serves, execute the following command in the global configuration mode. Without this function, the electing BSR will receive all external advertisement messages of candidate RPs.

With this command, the source parameter of ACL rule sets the CRP address and the destination parameter sets the multicast group range the CRP serves. If both addresses are denied by ACL, the group of the CRP will be filtered.

Command	Function
ip pim accept-crp list { *<100-199>* | *<2000-2699>* | *WORD* }	Filter the advertisement of candidate RP.
no ip pim accept-crp list	Remove the configuration.

6.3.22 Configuring the Electing BSR to Receive the C-RP-ADV Message whose Prefix-count is 0

To configure the electing BSR to receive the C-RP-ADV message whose prefix-count is 0, execute the following command in the global configuration mode. With this function, the electing BSR considers the CRP supports all groups after receiving the C-RP-ADV message whose prefix-count is 0.

Command	Function
ip pim accept-crp-with-null-group	Configure the electing BSR to receive the C-RP-ADV message whose prefix-count is 0.
no ip pim accept-crp-with-null-group	Remove the configuration.

6.3.23 Configuring the Source IP Address of RPs

This command sets the source IP address of RPs sent from DR. The **no** form of this command sets the RPF interface address as the default source address for the response when the PR sent from DR to the source host. The configured

address must be reachable for the response to the correct Register-Stop information in the RP. The address is generally a loop address of the interface. It also can be other physical address. Such address must be advertised by unicast route on the DR port.

To configure the source IP address of RPs, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim register-source** { *local_address* | *Interface-type interface-number*}	Configure the source IP address used in RPs.
DES-7200(config)# **no ip pim register-source**	Set the RPF interface address as the source IP address of RPs.

6.3.24 Configuring the RP Suppression Time

This command configures the RP suppression time. It will modify the RP suppression time defined on the DR. If the **ip pim rp-register-kat** is not configured, defining the RP suppression time in the RP will change RP keepalive period.

To configure the RP suppression time, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config）# **ip pim register-suppression** *seconds*	Configure the RP suppression time.
DES-7200(config）# **no ip pim register-suppression**	Set the suppression time to 60 seconds.

6.3.25 Configuring the Detect Time of Null Register Packet

The source DR can send null register packet to the RP in a period of time before the RP suppression time expires. This period is detect time, 5s by default.

To configure the detect time of null register packet, execute the following commands in the global configuration mode:

Command	Function
ip pim probe-interval *interval-seconds*	Configure the detect time. *interval-seconds*: in the range of 1 to 65535 seconds.
no ip pim probe-interval	Restore the detect time to 5s.

Caution

The detect time should be less than half of RP suppression time. Moreover, the 3* RP suppression time plus detect time should be no more than 65535 seconds or otherwise the system issues a warning.

6.3.26 Configuring KAT Timer

The KAT timer is used for monitoring PIM RP.

To configure KAT timer, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip pim rp-register-kat** *seconds*	Configure KAT timer. *seconds*: in the range of 1 to 65535.
DES-7200(config) # **no ip pim rp-register-kat**	Use the default KAT value

6.3.27 Configuring the Interval of Sending the Join/Prune Message

By default, the Join/Prune message is sent at the interval of 60s by default. Execute this command to modify this interval.

To modify the interval of sending the Join/Prune message, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config) # **ip pim jp-timer** *interval-seconds*	Set the interval of sending the Join/Prune message, in the range of 1 to 65535 seconds.
DES-7200(config) # **no ip pim jp-timer** *interval-seconds*	Restore the setting to the default value, or 60s.

6.3.28 Allowing the Last Hop Device to Switch from the Shared Tree to the Shortest Path Tree

The last-hop device is allowed to switch from the shared tree to the shortest path tree.

When the sending speed of a source is higher than equal to the transmission speed, a PIM join message is triggered and a source tree is constructed. If the final key word is defined, all the sources in this group use the shared tree. If the transmission speed is lower than the threshold, the leaf device re-diverts to the shared tree and sends a prune packet to the source.

To allow the last hop device to switch from the shared tree to the shortest path tree, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config) # **ip pim spt-threshold**	Allow the last-hop device to switch from the shared tree to the shortest path tree.
DES-7200(config) # **no ip pim spt-threshold**	Disable this function.

6.3.29 Using the MIB of PIM-DM

Execute this command to use the MIB of PIM-DM. Otherwise, the MIB of PIM-SM will be used.

To use the MIB of PIM-DM, execute the following command in the global configuration mode:

Command	Function
DES-7200(config) # **ip pim mib dense-mode**	Use the MIB of PIM-DM.
DES-7200(config) # **no ip pim mib dense-mode**	Use the MIB of PIM-SM.

6.3.30 Configuring the Particular Multicast Source

Configuring a particular multicast source enables you directly receive multicast data packets from the source without following the RP tree. To configure a particular source multicast, run the following command.

Command	Function
DES-7200(config）# **ip pim ssm {default |range** access-list]}	Configuring a particular multicast source.
DES-7200(config）# **no ip pim ssm**	Remove the configuration.

6.3.31 Monitoring and Maintaining PIM-SM

6.3.31.1 Showing the Status of PIM-SM

Command	Function
DES-7200 # **show debugging**	Show the status of the debugging switch
DES-7200 # **show ip pim interface** [*interface-type interface-number*] [**detail**]	Show the PIM-SM information of the interface.
DES-7200 # **show ip pim neighbor** [*interface-type interface-number*]	Show the PIM neighbor information.
DES-7200 # **show ip sparse-mode mroute**	Show the multicast routing table information of PIM-SM
DES-7200 # **show ip pim sparse-mode bsr-router**	Use this command to show the detailed information of BSR.
DES-7200 # **show ip pim sparse-mode rp-hash** *group-address*	Use this command to show the RP information selected.
DES-7200 # **show ip pim sparse-mode rp mapping**	Show the group-RP mapping information and RP settings
DES-7200 # **show ip sparse-mode nexthop**	Show the next hop of PIM-SM from NSM.
DES-7200 # **show memory pim sparse-mode**	Show the memory statistics information of PIM-SM background program

6.3.31.2 Clearing the PIM-SM Information

The following commands are available to clear the PIM-SM information:

Command	Function
DES-7200# **clear ip mroute** {*** |** *group_address* [*source_address*] }	Clear multicast route entries.
DES-7200# **clear ip mroute statistics** {*** |** *group_address* [*source_address*] }	Clear the statistics of multicast route entries.
DES-7200 #**clear ip pim sparse-mode bsr rp-set ***	Clear RP-SET.

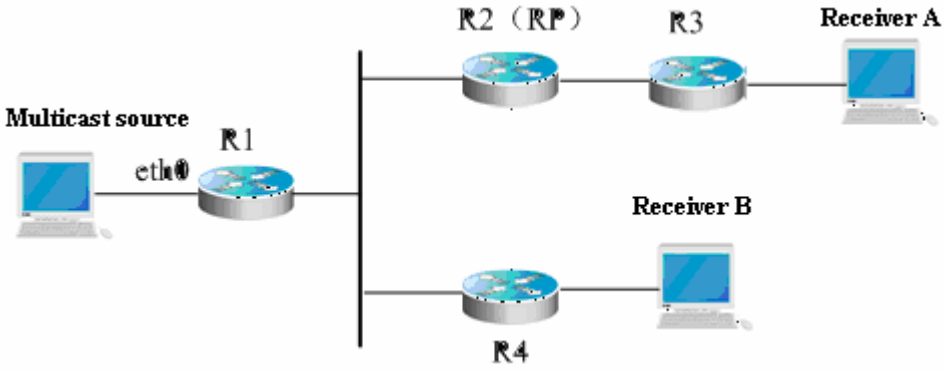
6.4 PIM-SM Configuration Example

- **Configuration Requirements**

  The network topology is shown in Figure 36-7. Device 1 and the multicast source locate in the same network, device 2 and receiver A locate in the same network.

Suppose the devices are connected with the host correctly; IP addresses and unicast routes are configured.

Example of PIM-SM networking diagram



- **Device Configuration**

Take the device 1 as an example to show how to configure PIM-SM. The steps of device 2, 3 and 4 are similar with device 1.

Step 1: Enable multicast routing

```
DES-7200# configure terminal
DES-7200(config)# ip multicast-routing
```

Step 2: Enable PIM-SM on the interface eth0

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ip pim sparse-mode
DES-7200(config-if)# end
```

Step 3: Configure the candidate BSR and candidate C-RP.

Set R2's loopback1 to C-BSR and C-RP

```
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ip address 100.1.1.1 255.255.255.0
DES-7200(config-if)# ip pim sparse-mode
DES-7200(config-if)# exit
DES-7200(config)# ip pim bsr-candidate loopback 1
DES-7200(config)# ip pim rp-candidate loopback 1
DES-7200(config-if)# end
```

7 PIM-SMv6 Configuration

7.1 PIM-SM Overview

PIM (Protocol Independent Multicast) is designed by IDMR (Inter-domain Multicast Routing) working group. As its name implied, PIM does not depend on a specific unicast routing protocol. It utilizes the unicast routing table established by various unicast routing protocols to enable the RPF check function instead of maintaining a separate multicast routing table for forwarding multicast packets. Compared with other multicast protocols, PIM overhead falls down at large extent for PIM does not need to receive and send multicast route update. The concept behind PIM design is that support and flexible transformation between SPT and the shared tree is enabled for higher multicast efficiency. There are two kinds of PIM modes-dense mode and sparse mode.

PIM-SM (Protocol Independent Multicast Sparse Mode) is a multicast routing protocol in sparse mode. In the PIM-SM domain, the device running PIM-SM sends the Hello message at a specific interval to discover adjacent devices running PIM-SM and be in charge of DR election. Here DR sends the “join/prune” message to its direct group members in the direction of the root node of the multicast distribution tree or sends the data from the direct multicast source to the multicast distribution tree.

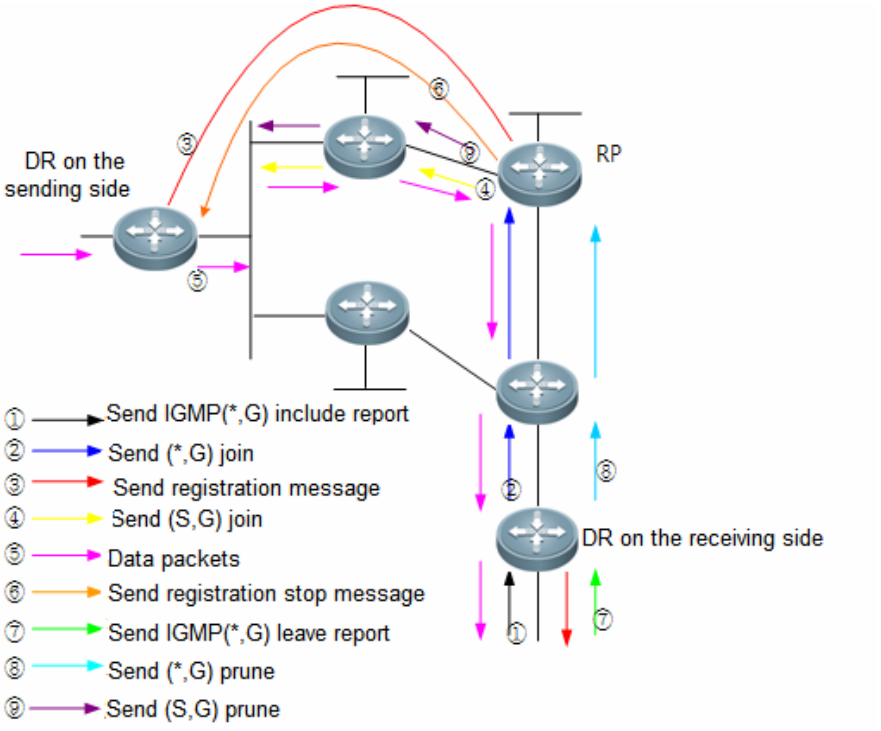


Figure 5 PIM-SM explicit join/prune mechanism

PIM-SM forwards multicast data packets by setting up a multicast distribution tree. There are two kinds of multicast distribution tree: the shared tree using G's RP as root and the shortest path tree using the multicast source as root. With the explicit join/prune mechanism, PIM-SM sets up and maintains the multicast distribution tree.

As illustrated in the above figure:

1 The DR on the receiving side receives the MLD (*,G) report message from a host on the same side.

2 If the DR on the receiving side is not the RP of G, it will send a (*.G) Join message to the RP. Upon receiving this message, the upstream router will send the (*.G) Join message to the RP without the forwarding entry of the corresponding group. In this way, the (*,G) Join message is transmitted hop to hop until G's RP receives the (*,G) Join message, indicating that the DR joins the shared tree.

3 When the source host sends multicast data to a group, the data is encapsulated in the registration message and sent by the DR on the source side to the RP in unicast form. Then, the RP decapsulates the registration message, extracts the data and forwards the data to every member of the group along the shared tree.

4 The RP sends the (S,G) Join message to the DR on the source side to join its shortest path tree.

5 After the shortest path tree from the RP to the DR on the source side is established, data packets are sent to the RP along this STP without encapsulation.

6 When the first multicast data arrives along the SPT, the RP sends the registration stop message to the DR on the source side, notifying the DR of stopping registration and encapsulation. Upon receiving the registration stop message, the DR no longer registers and encapsulates data packets. In stead, it sends data packets to the RP along the shortest path tree, which then forwards data packets to every group member along the shared tree.

7 When a receiving end does not need multicast packets, it sends the MLD leave message.

8 The DR on the receiving side sends the prune message in multicast form hop by hop to G's RP, the prune message arrives at the RP or the router along the way to the RP which has other (*,G) receiver so that data packets are not sent to this receiving side any more.

9 If the RP has no downstream receiver at present, it sends (S,G) prune message to the DR of the data source hop by hop. Consequently, the DR on the source side prunes the interface receiving this (S,G) prune message. In this way, data packets are filtered on the DR of the data source.

RP election is also involved in PIM-SM. when there is one or more candidate BSRs configured in the PIM-SM domain, some rule is applied to elect BSR. Candidate RPs are also configured in the PIM-SM domain, which send the packets containing their addresses and serviceable multicast groups to BSRs in unicast form. BSRs generate bootstrap messages with a series of candidate RPs and the addresses of corresponding multicast groups periodically. These bootstrap messages are transmitted in the overall domain hop by hop. Devices will receive and save these bootstrap messages. Upon receiving the member relation report of a multicast group from the directly connected device, the DR will use a hash algorithm and map the multicast group address to a candidate RP who can serve this group if it has not the routing entry of this group. Then the DR will send the join/prune message in multicast form hop by hop along the way to the RP. On the other hand, upon receiving multicast packets from the directly connected device, the DR will use a hash algorithm and map the multicast group address to a candidate RP who can serve this group, and then encapsulate these

multicast packets in the registration message and send it to the PR in unicast form.

The essential difference between PIM-SM and PIM-DM is that PIM-SM is based on explicit join mode and PIM-DM is based on flood/prune mode. For PIM-SM, the receiver sends a join message to the PR, but the device forwards the packets of a multicast group only on the interface joining this multicast group. PIM-SM forwards multicast packets through the shared tree. Each multicast group has a rendezvous point. The multicast source sends packets to the RP along the shortest path, and then the RP sends the packets to every receiver along the shortest path. This process is similar to CBT. However, the core concept is not used in PIM-SMv6. One of the main advantages of PIM-SMv6 is that it not only receives multicast packets through the shared tree but also offers the shared tree-to-SPT transformation mechanism. This transformation consumes a lot number of resources, even though it reduces network delay and possible block on the RP. It is suitable for the environment where there are many pairs of multicast sources yet fewer networks.

PIM-SM distributes multicast packets through the shared tree and SPT. Assume that other devices do not need to receive these multicast packets, unless otherwise specified. When a host joins a multicast group, the devices connecting to the host notify the root (or RP) through the PIM join message. This message is transferred among these devices in order to set up the structure of a shared tree. So, the RP records this transmission path and the registration message from the first hop device (DR) of the sending multicast source, and perfects the shared tree based on these two messages. Update of leaf messages is enabled on periodic query message. For the shared tree, the multicast source sends multicast packets to the RP so that all receivers can receive these multicast packets.

*.G indicates a tree, in which * indicates all sources and G indicates the specific multicast address. The prune message is also used in the shared tree when leafs do not need to receive multicast packets.

PIMv2 BSR distributes the group-to-RP message to all devices without the necessity for configuring RP for every device. The BSR distributes the mapping message through the hop-by-hop flooding BSR message. First of all, the BSR is elected among devices. This election procedure is similar to electing the root bridge in STP by priority. Every BSR device checks the BSR message, and only forwards the BSR messages with higher or equivalent priority (or higher IP address). The elected BSR sends the BSR message to the all-PIM-routers multicast group (ff02::d) with TTL 1. Upon receiving the BSR message, the adjacent PIMv2 device sends it out in multicast form and then reset TTL to 1. In this way, the BSR message is sent to all devices hop by hop. Since the BSR message includes the IP addresses of BSR devices, the candidate BSR can determine which device is the current BSR device. The candidate RP sends the candidate RP advertisement and alleges in which address ranges it can become RP. The BSR stores the advertisement message in its local candidate RP cache, and notifies all PIM devices of local candidate RPs periodically. Also in this way, the message is sent to all devices hop by hop.

7.2 PIM-SMv6 Configuration Task

PIM-SMv6 Configuration Preparation：Enable a unicast routing protocol, for instance OSPFv3, to automatically discover routes.

PIM-SMv6 configuration includes the following tasks, but only the first and the second tasks are mandatory, others are optional.

7.2.1 Enable Multicast Routing

Multicast packets can be forwarded and enabling PIM-SMv6 makes sense only after multicast routing is enabled.

To enable or disable multicast routing, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 multicast-routing**	Enable multicast routing.
DES-7200(config)# **no ipv6 multicast-routing**	Disable multicast routing.

7.2.2 Enable PIM-SMv6

In order for one device to interact with other devices on PIM-SMv6 control messages, maintain and update the multicast routing table and forward multicast packets, PIM-SMv6 must be enabled on every interface.

To enable PIM-SMv6 on the interface, run the following commands in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim sparse-mode**	Enable PIM-SMv6 on the interface.
DES-7200(config-if)# **no ipv6 pim sparse-mode**	Disable PIM-SMv6 on the interface.

Caution

Enabling PIM-SMv6 brings into effect only after multicast routing is enabled globally.

7.2.3 Configure the Hello Message Transmission Interval

After enabling PIM-SMv6, the interface sends the Hello message to the ones of adjacent devices at an interval. This transmission interval can be set as required.

To configure the Hello message transmission interval, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim query-interval** *interval-seconds*	Set the Hello message transmission interval. *interval-seconds*: in the range 1 to 65535 seconds
DES-7200(config-if)# **no ipv6 pim query-interval**	Restore the setting to the default value.

By default, the Hello message transmission interval is 30 seconds on the interface.

Note

When the Hello message transmission interval is updated every time, the Hello message hold time is updated 3.5 times of the Hello message transmission interval. If the Hello message transmission interval multiplying 3.5 is larger than 65535, the Hello message hold time is updated to 65535.

7.2.4 Configure the Propagation Delay of the Hello Message

After the interface sends the Hello message, you can set the options of the Hello message. For LAN prune delay, the Propagation_Delay field is 500ms by default.

To configure the propagation delay, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim propagation-delay** *interval-milliseconds*	Set the propagation delay. *interval-milliseconds:* in the range of 1-32767 ms.
DES-7200(config-if)# **no ipv6 pim propagation-delay**	Restore the propagation delay setting to the default value, namely 500ms.

Note

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

7.2.5 Configure the Override Interval of the Hello Message

After the interface sends the Hello message, you can set the options of the Hello message. For LAN prune delay, the override-interval field is defaulted to 2500ms.

To configure the override-interval field, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim override-interval** *interval-milliseconds*	Set the override-interval. *interval-milliseconds:* In the range of 1 to 65535 seconds.
DES-7200(config-if)# **no ipv6 pim override-interval**	Restore the setting to the default value.

Note

Change of propagation delay or prune delay will influence the override interval of Join/prune message. As specified in the protocol, the override interval of Join/prune message must be less than its hold time or otherwise this will cause temporary interruption.

7.2.6 Configure the Neighbor Tracking of the Hello Message

After an interface sends the Hello message, the LAN Prune Delay option of the Hello message has a T bit, indicating whether join constraint is enabled on the interface. With join constraint enabled, the interface is constrained not to send its Join message to the upstream neighbor when it receives the Join message that

its neighbor sends to the upstream neighbor. On the other hand, with join constrain disabled, the interface will send its Join message to the upstream neighbor when it receives the Join message that its neighbor sends to the upstream neighbor. This function allows upstream routers to track how many receivers in downstream in accord with all received Join messages. Join constraint is enabled on the interface by default.

To disable join constraint on the interface, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim neighbor-tracking**	Disable join constraint on the interface.
DES-7200(config-if)# **no ipv6 pim neighbor-tracking**	Enable join constraint on the interface

7.2.7 Configure the Triggered Hello Delay of the Hello Message

When the router starts or detects a new neighbor starts, it sends the Hello message. To avoid congestion, the router will send the Hello message at random. This random time is calculated by triggered hello delay, which is 5s by default.

To configure triggered hello delay, run the command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim triggered-hello-delay** *interval-seconds*	Configure triggered hello delay. *interval-seconds*: In the range of 1 to 5 seconds
DES-7200(config-if)# **no ipv6 pim triggered-hello-delay**	Restore the setting to the default value.

7.2.8 Configure PIM-SMv6 Neighbor Filtering

Neighbor filtering can be enabled on the interface for security. PIM-SMv6 will not establish adjacency relation with a neighbor device and delete the established adjacency relation as long as the neighbor device is denied by the filtering access list.

To configure neighbor filtering, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim neighbor-filter** *ipv6_access-list*	Enable neighbor filtering on the interface.
DES-7200(config-if)# **no ipv6 pim neighbor-filter** *ipv6_access-list*	Disable neighbor filtering on the interface.

By default, neighbor filtering is disabled on the interface.

Note

Only the neighbors whose IP address matches ACL filtering can serve as the PIM neighbors of the interface.

7.2.9 Configure DR Priority

To configure DR priority, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim dr-priority** *priority-value*	Configure DR priority in the range of 0 to 4294967294.
DES-7200(config-if)# **no ipv6 pim dr-priority** *priority-value*	Restore DR priority to the default value, namely 1.

7.2.10 Configure Static RP

In a smaller network, you can use PIM-SMv6 by configuring static RP. All devices in the PIM-SMv6 domain should be configured with similar static RP for consistent PIM-SMv6 multicast routes.

To configure static RP, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim rp-address** *ipv6_rp-address* [*ipv6_access-list*]	Configure static RP.
DES-7200(config)# **no ipv6 pim rp-address** *ipv6_rp-address* [*ipv6_access-list*]	Remove the configuration.

Note that:

- When BSR and static RP take effect simultaneously, static RP is preferred.
- Static RP can be configured for many multicast groups (by using ACL) or all multicast groups. However, one static RP can be configured only once.
- If more than one IPv6 address is configured to be RP, the highest IPv6 address is adapted first.
- Only the IPv6 addresses defined and permitted by ACL are valid multicast groups. By default, all multicast groups are permitted.
- After configuration, the source address of static RP is inserted in the tree structure of the group range-based static RP group. Each group range-based static RP group maintains a chain structure that lists static RP groups in the descending order of IPv6 addresses. When a group range selects a RP, the first element, or the highest IPv6 address is selected.
- Deleting a static RP will delete it from all multicast groups and a new one is selected from the static RP tree structure as static RP.

7.2.11 Configure Candidate BSR

Configuration of candidate BSR produces globally unique BSR in the PIM-SMv6 domain, which collects and distributes the RPs in the domain for the uniqueness of RP mapping.

To configure candidate BSR, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim bsr-candidate** *interface-type interface-number* [*hash-mask-length*] [*priority-value*]	Set the device as the candidate BSR. *hash-mask-length:* In the range 0 to 128, 126 by default. *priority-value:* In the range 0 to 255, 64 by default.
DES-7200(config)# **no ipv6 pim bsr-candidate** *interface-type interface-number*	Remove the configuration.

Note

To set an interface as the candidate BSR, it must be configured with a global unicast address used for unicast routes or a local address. The first global unicast address or local address is elected as the candidate BSR.

7.2.12 Configure BSR Border

To restrain BSM flooding, configure BSR border on the interface so that the interface drops BSM messages upon receiving them.

To configure BSR border, run the following command in the interface configuration mode.

Command	Function
DES-7200(config-if)# **ipv6 pim bsr-border**	Set the interface to be BSR border.
DES-7200(config-if)# **no ipv6 pim bsr-border**	Remove the configuration.

7.2.13 Ignore the RP Priority of RP-Set

When you select a RP for a multicast address, ignore their priorities in comparison if there are more than one RP.

To ignore RP priority, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim ignore-rp-set-priority**	Ignore RP priority of RP-SET.
DES-7200(config)# **no ipv6 pim ignore-rp-set-priority**	Remove the configuration.

7.2.14 Configure Candidate RP

Configure candidate RP to periodically send candidate RP advertisement to the BSR so that the candidate RP advertisement is propagated to all PIM-SMv6 devices in the domain and guarantee the uniqueness of RP mapping.

To configure candidate RP, run the following command in the global configuration mode.

Command	Function

DES-7200(config)# **ipv6 pim rp-candidate** *interface-type interface-number* [**priority** *priority-value*] [**interval** *interval-seconds*] [**group-list** *ipv6_access-list*]	Configure candidate RP. *priority-value*: In the range 0 to 255, 192 by default *interval-seconds*: In the range 1 to 16383s, 60s by default *ipv6_access-list*: All multicast groups are allowed by default.
DES-7200(config)# **no ipv6 pim rp-candidate**	Remove the configuration.

Note

To set an interface as the candidate RP of the specific group range, use this command with ACL option. Note that the calculation of group range is only based on the ACE with permit rule, not deny rule.

7.2.15 Check the Reachability of RP Registration Message

This command can be used to check whether the RP is reachable before the DR sends the registration message to the RP.

To check the reachability of RP, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim register-rp-reachability**	Check the reachability of the RP.
DES-7200(config)# **no ipv6 pim register-rp-reachability**	Remove the configuration.

Caution

If there is a static multicast route to the RP and the next hop of this static multicast route is reachable in the unicast routing table, PIM-SMv6 considers that the RP is reachable, even though the RP is not reachable in the unicast routing table.

7.2.16 Filter the Addresses of Registration Packets on RP

This command filters the source addresses and group addresses of the registration packets arrived on RP. Only the registration packets whose source addresses and group addresses are permitted by ACL or the route map are processed. Other registration packets are filtered and the Register-stop message is sent back.

To filter the source addresses and group addresses of registration packets on RP, run the following command in global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim accept-register** {**list** *ipv6_access-list* | **route-map** *map-name* }	Filter the source addresses and group addresses of registration packets.
DES-7200(config)# **no ipv6 pim accept-register**	Remove the configuration.

7.2.17 Limit the Rate to Send Registration Packets

This command applies to the registration packets in (S, G) state, not the overall system.

To limit the rate to send registration packets, run the following commands in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim register-rate-limit** *rate*	Set the maximum number of registration packets sent per second, in the range of 1 to 65535.
DES-7200(config)# **no ipv6 pim register-rate-limit**	Remove the configuration.

7.2.18 Configure the Calculation Method of Checksum of Registration Packets

This command calculates the checksum of all the packets of PIM protocol, including encapsulated multicast packets.

Without this command, the checksum of registration packets is calculated by default methods of PIM protocol.

To configure the calculation method of checksum of registration packets, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim register-checksum-wholepkt** [**group-list** *ipv6_access-list*]	Calculate the checksum of all packets. **group-list** *ipv6_access-list*: All multicast packets by default.
DES-7200(config)# **no ipv6 pim register-checksum- wholepkt** [**group-list** *ipv6_access-list*]	Remove the configuration. **group-list** *ipv6_access-list*: All multicast packets by default.

7.2.19 Limit the Range of Legal BSRs

This command limits the range of legal BSRs. Without this command the PIM-SMv6 enabled router receives all external BSM packets.

To limit the range of legal BSRs, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim accept-bsr list** *WORD*	Filter the BSM packets of BSRs.
DES-7200(config)# **no ipv6 pim accept-bsr list**	Remove the configuration.

Note

This command filters the BSR address field of BSM packets. If the address of a BSM packet is denied by ACL, the BSM packet is filtered.

7.2.20 Configure Elected BSR to Limit the Address Range of Legal Candidate RP and the Multicast Group Range it Serves

This command configures elected BSR to limit the address range of legal candidate RP and the multicast group range it serves. Without this command, the elected BSR receives all external advertisements of candidate RPs.

For the ACL rule of this command, source specifies the address of candidate RP, and destination specifies the multicast group range that the candidate RP serves. If the ACL denies both addresses, the multicast group range of the candidate RP is filtered.

To configure elected BSR to limit the address range of legal candidate RP and the multicast group range it serves, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim accept-crp list** *WORD*	Elected BSR filters the advertisement of candidate RP.
DES-7200(config)# **no ipv6 pim accept-crp list**	Remove the configuration.

7.2.21 Enable Elected BSR to Receive the Candidate RP Advertisement whose prefix-count is 0

This command enables the elected BSR to receive the candidate RP advertisement whose prefix-count is 0. Without this command, the elected BSR will not process this kind of packets. Once configured, the elected BSR considers that the candidate RP supports all multicast groups upon receiving the candidate RP advertisement whose prefix-count is 0.

To enable the elected BSR to receive the candidate RP advertisement whose prefix-count is 0, run this command in the global configuration mode.

Command	Function
ipv6 pim accept-crp-with-null-group	Enable the elected BSR to receive the candidate RP advertisement whose prefix-count is 0.
No ipv6 pim accept-crp-with-null-group	Remove the configuration.

7.2.22 Configure the Source Address of Registration Packets

This command configures the source address of registration packets. Without this command or with the no form of this command, the interface address of DR connecting to the multicast source is used. For address parameter of this command, the address to be set must be reachable to unicast routes. For interface parameter of this command, the interface to be set must be loopback interface or other type of interface whose address is advertised by unicast routes, in which the first non-local link address of the interface serves as the source address of registration packets.

To configure the source address of registration packets, run the following command in the global configuration mode.

Command	Function

DES-7200(config)# **ipv6 pim register-source** {*ipv6_local_address* | *interface-type interface-number*}	Configure the source address of registration packets.
DES-7200(config)# **no ipv6 pim register-source**	Use the RPF's interface address as the source address of registration packets.

7.2.23 Configure the Suppression Time of Registration Packets

When the receiver does not receive the data packets destined to a multicast group from RP (namely RP does not serve this multicast group) or RP begins to receive multicast packets from the multicast source, RP sends the registration stop message to the DR on the multicast source side. Upon receiving this message, DR stops sending the registration packets encapsulated with multicast packets and transfers into the register suppression state.

During registration suppression, DR sends null registration packets, namely registration packets not encapsulated with multicast packets), to DR, indicating that the multicast source is still active. Probe time refers to the period that DR is allowed to send null registration packets before the registration suppression state is timed out. When registration suppression is timed out, DR starts to send registration packets. The smaller registration suppression timeout means the higher frequency that RP receives multicast packets; the larger timeout means the higher delay for a receiver to join a multicast group.

Running this command on DR will change the registration packet suppression time defined on DR.

To configure the registration packet suppression time, run this command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim register-suppression** *seconds*	Configure registration packet suppression time. *Seconds*: in the range *1 to 65535*s
DES-7200(config)# **no ipv6 pim register-suppression**	Restore the setting to the default value.

7.2.24 Configure the Probe Time of Null Registration Packet

The DR can send the null registration message to the RP in a period before the registration suppression time expires. This period is call probe time, 5 seconds by default

To configure the probe time of null registration packet, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim probe-interval** *interval-seconds*	Configure the probe time of null registration packet. *interval-seconds*: in the range 1 to 65535 seconds
DES-7200(config)# **no ipv6 pim probe-interval**	Restore the setting to the default value.

Note

The probe time must be less than half of registration suppression time. Furthermore, 3* registration suppression time plus registration probe time should be no more than 65535s or otherwise the system triggers an alarm.

7.2.25 Configure RP KAT Timer

This command configures the hold time of (S, G) state that registration packets set up on RP.

To configure RP KAT timer, run this command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim rp-register-kat** *seconds*	Configure KAT timer. *Seconds*: in the range *1 to 65535*
DES-7200(config)# **no ipv6 pim rp-register-kat**	Restore the setting to the default value, namely 3* registration suppression time plus registration probe time.

Caution

The timer should be larger than 3* registration suppression time plus registration probe time on the source DR, or otherwise the RP may time out the (S, G) state before the source DR sends the registration packet and thus leading to temporary interruption of multicast packets.

7.2.26 Configure the Join/Prune Message Sending Interval

By default, the Join/Prune message is sent at the interval of 60s.

To configure the Join/Prune message sending interval, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim jp-timer** *interval-seconds*	Configure the Join/Prune message sending interval. *interval-seconds*: in the range 1 to 65535s
DES-7200(config)# **no ipv6 pim jp-timer** [*interval-seconds*]	Restore the setting to the default value, namely 60s.

Note

When you configure the Join/Prune message sending interval, if the sending interval * 3.5 is larger than 65535s, the system triggers an alarm and the sending interval is changed to be 65535/3.5 seconds.

7.2.27 Enable the Last Hop Device to Transfer from the Shared Tree to the Shortest Path Tree

With this command, a PIM join message is triggered and a source tree is constructed upon the receipt of the first (S, G) message. The keyword **group-list** means all the groups in the list transfer to the source tree. The no form of this command enables the device to transfer to the shared tree and send a prune message.

To enable the last hop device to transfer from the shared tree to the shortest path tee, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim spt-threshold** [**group-list** *ipv6_access-list*]	If group-list is configured, the last hop device of this multicast group is enabled to transfer from the shared tree to the shortest path tree. Without group-list, all multicast groups are permitted.
DES-7200(config)# **no ipv6 pim spt-threshold** [**group-lis**t *ipv6_access-list*]	Disable this function.

7.2.28 Configure the Specific Source multicast

This command enables the device to directly receive multicast packets from the specific multicast source rather than the PR tree.

To configure the specific source multicast, run the following command in the global configuration mode..

Command	Function
DES-7200(config)# **ipv6 pim ssm** {**default** |**range** *ipv6_access-list*]}	Configure the specific source multicast, 232.0.0.1~232.255.255.255 by default.
DES-7200(config)# **no ipv6 pim ssm**	Remove the configuration.

7.2.29 Configure Static RP Preference

To configure the static RP's priority higher than the one elected through BSR mechanism, run the following command in the global configuration mode.

Command	Function
DES-7200(config)# **ipv6 pim static-rp-preferred**	Configure the static RP's priority higher than the one elected through BSR mechanism.
DES-7200(config)# **no ipv6 pim static-rp-preferred**	Remove the configuration.

7.2.30 Enable Embedded RP

Embedded RP is the special RP discovery mechanism for IPv6 PIM that uses its IPv6 multicast address, from which the multicast router can directly resolve RP's address.

By default, embedded RP is enabled for the IPv6 multicast addresses of all embedded RP addresses. To enable embedded RP for the IPv6 multicast address of some embedded RP address, run this command in the global configuration mode.

Command	Function

DES-7200(config)# **ipv6 pim rp embedded** [**group-list** *ipv6_acl_name*]	Without *ipv6_acl_name,* enable embedded RP for the IPv6 multicast addresses of all embedded RP addresses. With *ipv6_acl_name,* enable embedded RP for the IPv6 multicast address of some embedded RP address.
DES-7200(config)# **no ipv6 pim rp embedded**	Disable embedded.

Note

In addition to enabling embedded RP on the device, you also need to configure static RP, or otherwise the device cannot serve as RP, even though its interface has the same address as embedded RP.

7.3 PIM-SMv6 Monitoring and Maintenance

PIM-SMv6 offers show commands to show the information on PIM-SMv6 interface, multicast group and multicast routing table.

7.3.1 Show PIM-SMv6 Status

Use the following commands to show PIM-SMv6 status.

Command	Function
DES-7200# **show debugging**	Show debugging switches.
DES-7200# **show ipv6 pim sparse-mode bsr-router**	Show BSR details.
DES-7200# **show ipv6 pim sparse-mode interface** [i*nterface-type interface-number* [**detail**]]	Show PIM-SMv6 interface information.
DES-7200# **show ipv6 pim sparse-mode local-members** [*interface-type interface-number*]	Show local MLD information of PIM-SMv6 interface.
DES-7200# **show ipv6 pim sparse-mode mroute** {*ipv6_group_address* | *ipv6_source_address* | }	Show PIM-SMv6 multicast routing information.
DES-7200# **show ipv6 pim sparse-mode neighbor** [**detail**]	Show PIM-SMv6 neighbors.
DES-7200# **show ipv6 pim sparse-mode nexthop**	Show PIM-SMv6 next hop information from NSM.
DES-7200# **show ipv6 pim sparse-mode rp-hash** *ipv6_group-address*	Show the RP information of the specific multicast group address.
DES-7200# **show ipv6 pim sparse-mode rp mapping**	Show all RPs and the groups they serve.
DES-7200# **show ipv6 pim sparse-mode track**	Show the number of received and sent PIMv6 packets.

7.3.2 Delete Internal PIM-SMv6 Messages

The following commands delete internal PIM-SMv6 messages.

Command	Function
DES-7200# **clear ipv6 mroute**	Clear multicast routing entries.
DES-7200# **clear ipv6 mroute statistics**	Clear multicast routing entry statistics.
DES-7200# **clear ipv6 pim sparse-mode bsr rp-set**	Clear RP-SET.
DES-7200# **clear ipv6 pim sparse-mode track**	Reset the beginning time of statistics and reset PIMv6 packet counter.

For details, refer to PIM-SMv6 Command Reference.

7.4 PIM-SMv6 Configuration Example

- **Configuration Requirements**

Figure 2 illustrates network topology. R1 and the multicast source are located in one network. R2 is set to be RP. R3 and receiver A are located in the same network. R4 and receiver B are in the same network. Assume that devices are connected properly, IPv6 is enabled on each interface and IPv6 unicast is enabled on every device.

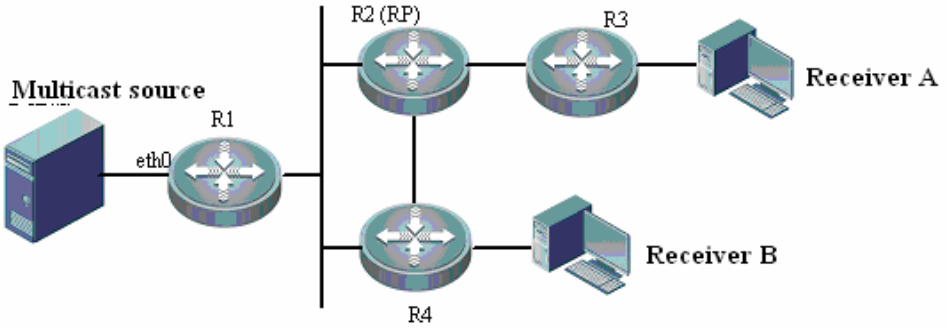


Figure 6 PIM-SMv6 topology

- **Configuration steps**

Step1: Enable multicast routing

Enable IPv6 multicast routing on R1. The configuration is similar on R2, R3 and R4.

```
DES-7200# configure terminal
DES-7200(config)# ipv6 multicast-routing
```

Step 2: Enable PIM-SMv6 on the interface

Enable PIM-SMv6 on R1's eth0. This configuration is similar on the interfaces of R1, R2, R3 and R4.

```
DES-7200(config)# interface eth 0
DES-7200(config-if)# ipv6 pim sparse-mode
DES-7200(config-if)# end
```

Step 3: Configure candidate BSR and candidate RP.

Set R2's loopback1 to be C-BSR and C-RP

```
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ipv6 address 2008:1::1/64
DES-7200(config-if)# ipv6 pim sparse-mode
```

```
DES-7200(config-if)# exit
DES-7200(config)# ipv6 pim bsr-candidate loopback 1
DES-7200(config)# ipv6 pim rp-candidate loopback 1
```

After the receiver joins the multicast group and the multicast source sends multicast packets, you can use show commands to monitor operation status.

Note

MLD is automatically enabled on each interface while PIM-SMv6 is enabled.

8 IGMP Snooping Configuration

8.1 Overview

8.1.1 Understanding IGMP Snooping

Internet Group Management Protocol, abbreviated as IGMP Snooping, is an IP multicast flow mechanism running in the VLAN, and used to manage and control the IP multicast flow forwarding in the VLAN and belongs to the Layer2 multicast funtion. The IGMP Snooping function described below is in the VLAN, and the related ports are the member ports in the VLAN.

The device running IGMP Snooping sets up the mapping for the port and the multicast address by analyzing the received IGMP packets, and forwards the IP multicast packets based on the mapping. As shown in the Figure-1, with IGMP Snooping enabled, the IP multicast packets are broadcasted in the VLAN; while without IGMP Snooping enabled, the known IP multicast packets are not broadcasted in the VLAN but sent to the specified recipient.

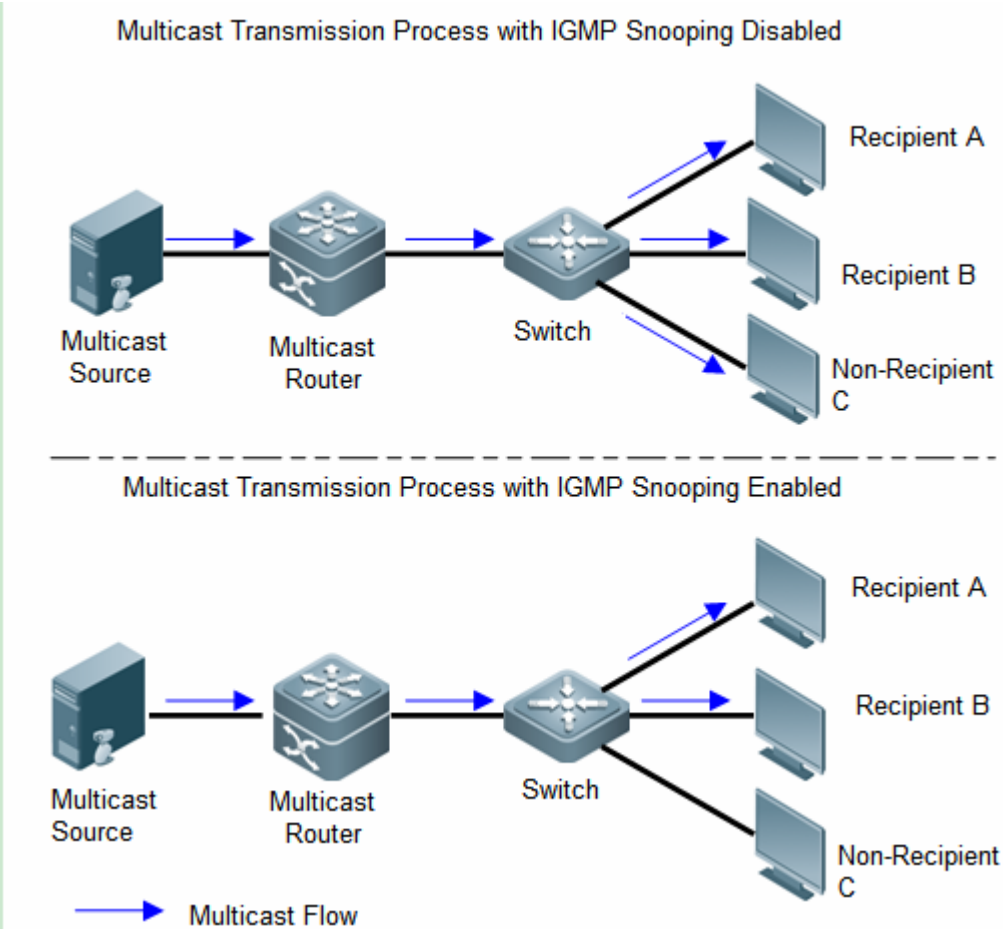


Figure 1

DES-7200 multicast products support both the layer 2 multicast(IGMP Snooping) function and the layer 3 multicast(Multicast-routing) function. That is to say, to realize better packet forwarding function, DES-7200 device supports not only the layer 3 multicast route forwarding, but also the snooping in the VLAN.

8.1.2 Understanding the Type of IGMP Snooping Ports

As shown in the Figure 2, the Router is connected with the multicast source. The IGMP Snooping is enabled on the SwitchA. HostA and HostC are receives (that is, the IP multicast group member)

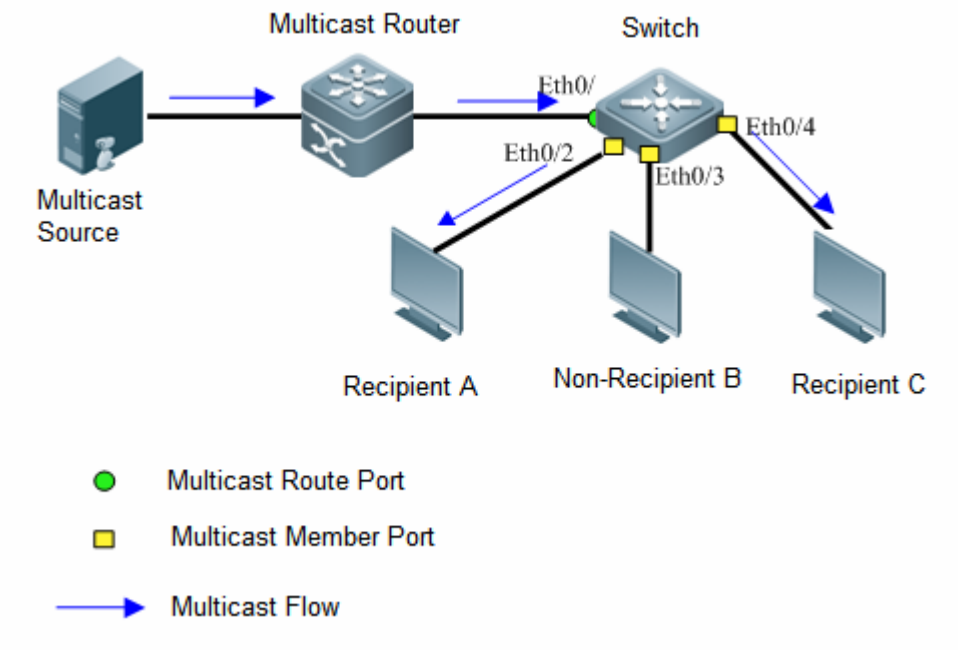


Figure 2 IGMP Snooping Port Type

Multicast Router Port: the switch is connected with the multicast router(the Layer3 multicast device), take the SwitchA interface Eth0/1 for example. All router ports on the switch(including the dynamic and static ports) are recorded in the router port list. By default, the router port corresponds to the recipient of the multicast data in the VLAN, and can also be added to the IGMP Snooping forwarding list.

Member Port: the abbreviation of the IP multicast group member port, also named Listener Port, representing the port connected with the IP multicast group member on the switch, take the SwitchA interface Eth0/2, Eth0/3 and Eth0/4 for example. All member ports on the switch(including the dynamic and static ports) are recorded in the IGMP Snooping forwarding list.

8.1.3 Understanding the Aging Timer of Dynamic Port

Table-1 Aging timer of dynamic port

Type	Description	Events triggering timer	Activity after timeout
Aging timer for the dynamic router port	Enable a timer for each dynamic router port. The timeout time is the aging time of the dynamic router port.	Receive the IGMP general query packet or the IP PIM Hello packet.	Remove the port from the router port list.
Aging timer for the dynamic member port	Enable a timer for each dynamic member port. The timeout time is the aging time of the dynamic member port.	Receive the IGMP query packet.	Remove the port from the IGMP Snooping multicast group forwarding list.

8.1.4 Understanding Operation Mechanism of IGMP Snooping

8.1.4.1 General Group Query and Specific Group Query

IGMP querier sends the general query packets to all hosts and routers(with the address: 224.0.0.1) in the local network segment periodically to query for the IP multicast group member in the network segment. Upon receiving the IGMP general query packets, the switch forwards those query packets to all ports in this VLAN, and processes the packet-receiving port as follows:

If this port has already been in the router port list, reset the aging timer.

If this port has not been in the router port list, add the port to the list and enable the aging timer.

After receiving the IGMP general query packets, the multicast device enable the aging timer for all member ports. Set the aging time as the maximum respond time of the IGMP query packets. When the aging time is 0, no member port receives the multicast flow and the port will be removed from the IGMP Snooping forwarding list.

After receiving the IGMP specific-group query packets, the multicast device enable the aging timer for all member ports in the specific group. Set the aging time as the maximum respond time of the IGMP query packets. When the aging time is 0, no member port receives the multicast flow and the port will be removed from the IGMP Snooping forwardin.

For the IGMP specific-group source query packets, it is no need to update the aging timer.

8.1.4.2 Membership Report

In the following circumstances, the host sends the IGMP membership report to the IGMP querier:

After receiving the IGMP query(general or specific-group query) packets, the IP multicast group member host responds to the received packets.

If the host wants to join in an IP multicast group, it will take the initiative to send the IGMP membership report to the IGMP querier and claim to join in the IP multicast group.

Upon receiving the IGMP membership report message, the switch forwards the message through all router ports in the VLAN, analyzes the IP multicast group address from the message to add to the host, and deals with the packet-receiving port as follows:

If the corresponding forwarding entry of IP multicast group is inexistent, create a forwarding entry, add the dynamic member port to the outgoing port list, and enable the aging timer.

If the corresponding forwarding entry of IP multicast group exists but the outgoing port list excludes the port, add the dynamic member port to the outgoing port list, and enable the aging timer.

If the corresponding forwarding entry of IP multicast group exists and the outgoing port list includes the port, reset the aging timer.

8.1.4.3 Leaving the Multicast Group

When leaving the IP multicast group, the host notifies the multicast router of the leave event by sending the IGMP leave group packets. Upon receiving the IGMP leave group packets on a dynamic member port, the switch forwards those packets to the router ports.

8.1.5 Understanding IGMP Profiles

IGMP Profiles is the group filterings actually, defines a series of multicast address range and the access to those multicast addresses(permit/deny), including “Multicast address range in the SVGL mode”, “Filtering multicast data range of router port”, “IGMP Filtering range”.

8.1.6 Understanding Working Modes of IGMP Snooping

DISABLE: The IGMP Snooping does not work in this mode. That is, the switch does not snoop the IGMP messages between the host and the router. Multicast frames are forwarded in the VLAN in the broadcast form.

IVGL(Independent VLAN Group Learning): In this mode, the multicast flows in different VLANs are independent. A host can only request multicast flows to the router interface in the same VLAN. Upon receiving the multicast flow in any VLAN, the switch forwards the flow to the member port in the same VLAN.

SVGL(Shared VLAN Group Learning): In this mode, the hosts in different VLANs share the same multicast flow. A host can request multicst flows across VLANs. By designating a Shared VLAN, you can only forward the multicast flows received in this Shared VLAN to other member ports in different VLANs. In the SVGL mode, IGMP Profile must be used to divide the multicast address range, within which the multicast flow can be forwarded across VLANs. By default, all group range is not within the SVGL range and all multicast flows are dropped. As shown in Figure-3:

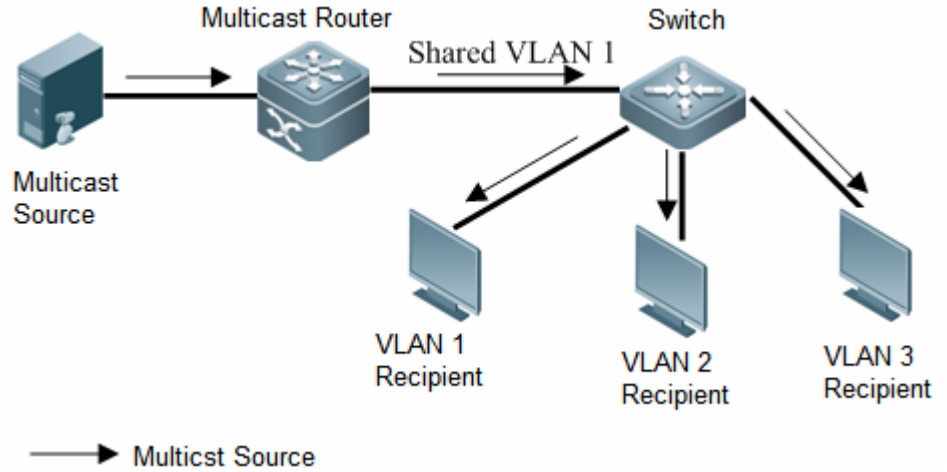


Figure-3 Multicast Flow in the Shared VLAN forwarding across VLANs

Promiscuous mode: also known as IVGL-SVGL mode. In this mode, the IVGL mode and the SVGL mode can co-exist. Use IGMP Profile to divide a set of multicast address range to the SVGL, within which the member port of the multicast forwarding entry can be forwarded across VLANs and without which the member ports are forwarded in the same VLAN.

8.1.7 Understanding Relationship between IGMP Snooping and QinQ

After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, IGMP packets received from dot1q-tunnel port will be handled in two ways through IGMP Snooping:

1st way: Create multicast entries on the VLAN to which IMGP packets belong, and forward IMGP packets on such VLAN. For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10.

2nd way: Create multicast entries on the default VLAN to which dot1q-tunnel belong, and forward multicast packets on the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port. For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1.

By default, the 2nd way is used.

8.1.8 Understanding IGMP Snooping Querier

In a multicast network running IGMP, a Layer-3 multicast device acting as the IGMP querier is responsible for sending IGMP general queries, so that all Layer-3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer.

However, in a network without layer-3 multicast device, a layer-2 multicast device does not support IGMP, and therefore cannot realize the relevant functions of IGMP querier. By enabling IGMP snooping on a layer-2 device, the layer-2 device can establish and maintain multicast forwarding entries at the data link layer, thus to forward multicast traffic correctly at the data link layer.

8.1.9 Understanding Multicast VLAN

As shown in Figure 3, in the traditional multicast programs-on-demand mode, when hosts, Host A, Host B and Host C, belonging to different VLANs require multicast programs-on-demand service, the multicast router needs to copy the multicast traffic in each VLAN as multicast snooping is only carried out in the VLAN. This results in not only waste of network bandwidth but also extra burden on the Layer 3 device.

To solve this problem, we can configure multicast VLAN feature on the switch (namely IMGP Snooping will be running in SVGL mode or hybrid mode), which means that the VLANs to which these hosts belong will be configured as the sub-VLANs of a multicast VLAN. In this way, the multicast router needs to replicate the multicast traffic only in the multicast VLAN instead of making a separate copy of the multicast traffic in each user VLAN. This lessens the burden of the Layer 3 device.

When running on the multicast VLAN, the master multicast VLAN (namely SVGL VLAN) and the multicast address of multicast VLAN must be specified for the devices. Meanwhile, the sub-VLANs associated with the multicast VLAN may also need to be specified. Only the traffic from master multicast VLAN can be

forwarded to the sub-VLANs needing to receive the multicast traffic.

Caution

The concept of sub-VLAN is introduced only after release 10.4(3).

If sub-VLAN is not specified, all VLANs can receive the multicast traffic from multicast VLAN.

8.1.10 Understanding Multicast Security Control

8.1.10.1 Understanding Multicast Access Control

IGMP itself cannot control whether or not a user can join a specific multicast group. Since the multicast traffic is replicated at the access node, it is important to control whether or not a user can obtain a multicast video stream at the access node as it can guarantee the security of video data and benefit of the carrier and avoid illegal users. Currently, the customized Profile can be preconfigured on the user port through the feature of device management, so as to permit or deny user joining, control multicast service and avoid illegal users from occupying network resources when controlling the access to one or multiple multicast programs. Through similar functions, precise control of user access to multicast programs can also be realized at the access node, such as multicast preview. We can also control the number of programs accessible to a specific user, thus effectively protecting the network bandwidth resources.

The multicast devices released by DES-7200 can realize diversified control of users:

Port-based control of user access to multicast traffic

Under certain circumstances, you may need to control user’s access to multicast traffic on the port. By this time, you can configure the port-based multicast filter. Detailed configurations are described in the section of "Configure port filter".

VLAN-based control of user access to multicast traffic

Under certain circumstances, you may need to control VLAN's access to multicast traffic. By this time, you can configure the VLAN-based multicast filter. Detailed configurations are described in the section of "Configure VLAN filter".

Caution

VLAN-based user access control is introduced only after release 10.4(3).

Port-based control of the amount of multicast traffic accessible to user

If the user requests multiple multicast programs on the same port, it will impose great pressure on network bandwidth. By configuring the number of multicast programs allowed on the port, we can effectively control the multicast programs that can be requested by the user. Detailed configurations are given in the section of "Configure IGMP Filtering".

Multicast preview

For certain multicast video streams, if the user doesn't have access to such video streams but the service provider wants to the user to preview such video streams within the preview interval, the device shall be able to support user-based multicast preview.

Caution

Multicast preview is supported only after release 10.4(3).

8.1.10.2 Understanding Source Port Check

Among the multicast devices released by DES-7200, certain products support IGMP SNOOPING source port check, further enhancing network security.

IGMP SNOOPING source port check is intended to limit the ingress of IGMP multicast traffic. When IGMP Snooping source port check is disabled, video streams entering from any port are considered valid, the multicast device will forward them to registered member ports as per IGMP Snooping forwarding table. When IGMP Snooping source port check is enabled, only the multicast traffic entering from router port will be considered valid, and layer-2 multicast device will then forward them to the registered ports. Multicast traffic entering from non-router port will be considered invalid and discarded.

Caution

IGMP Snooping source port check needs to use Masks. The definition of Masks is detailed in "Access Control List Configuration". Masks are shared among address binding, source port check and ACL, and the total number of available masks depends on the product. Since masks are limited in number, these three features will be affected by each other. Enabling address binding needs to occupy two masks, and enabling source port check will also occupy two masks; the available masks for ACL depends on the fact that whether these two features have been enabled. Assuming that ACL can by default use up to 8 masks, if address binding or source port check is enabled, the total number of masks available to ACL will drop to 6. If address binding and source port check are enabled at the same time, the masks available to ACL will drop to 4. In contrast, if ACL uses multiple masks and the remaining number of masks cannot meet the needs of these two applications, the system will prompt that masks resource is used up when enabling address binding and source port check. When one of these three features cannot run normally due to the restriction in masks, normal application of such feature can be achieved by reducing the masks used by other two features. For example, when three features are enabled at the same time, the system will prompt that masks are used up when enabling port check. You can disable address binding (remove all address bindings) or delete the ACE of ACL occupying multiple masks, so that the source port check can be enabled normally.

When enabling IGMP Snooping or configuring router port, if source port check is enabled, source port check may fail due to the inadequate masks resources. The system will prompt: Source port check applying failed for hardware out of resources. At this time, other resources shall be released first and then source port check shall be enabled again.

8.1.10.3 Understanding Source IP Check

Among the multicast devices released by DES-7200, certain products support IGMP SNOOPING source IP check, further enhancing network security.

IGMP SNOOPING source IP check is intended to limit the source IP address of IGMP multicast traffic. When IGMP Snooping source IP check is disabled, all incoming video streams are considered valid, the layer-2 multicast device will forward them to registered member ports as per IGMP Snooping forwarding table. When IGMP Snooping source IP check is enabled, only the multicast traffic with the configured source IP address will be considered valid, and the multicast

device will then forward them to the registered ports. Multicast traffic with other source IP addresses will be considered invalid and discarded.

8.2 Configuring IGMP Snooping

We will describe how to configure IGMP snooping in the following sections

Function Configuration		Description
Configure Basic IGMP Snooping Function	Enable IGMP Snooping	Required
	Set the aging timer for the dynamic port	Optional
	Set the maximum respond time of the IGMP Query Packet	Optional
Configure IGMP Snooping Port Funtion	Set the router port.	Optional
	Set the member port.	Optional
	Set the port fast-leave	Optional
	Set the IGMP membership report packet suppression.	Optional
Configure the IP Multicast Group Policy on the Port	Set the IP multicst group filtering	Optional
	Set the source port check.	Optional
	Set the source IP check.	Optional

8.2.1 Enabling IGMP Snooping

By default, when enabling IGMP Snooping, the IGMP Snooping working mode(IVGL、SVGL and IVGL-SVGL) must be specified.

Caution

The Layer2 multicast device does not support IGMP Snooping if the device works in the private VLAN mode.

8.2.2 Configuring IVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping IVGL mode:

Command	Function
DES-7200(config)# **ip igmp snooping ivgl**	Enable the IGMP Snooping IVGL mode. By default, the IGMP Snooping is disabled.
DES-7200 (config)#**show ip igmp snooping**	Verify the configuration.
DES-7200(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.

This example sets the IGMP Snooping IVGL mode:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping ivgl
DES-7200(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 0
```

```
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

8.2.3 Configuring SVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping SVGL mode:

Command	Function
DES-7200(config)# **ip igmp snooping svgl**	Enable the IGMP Snooping SVGL mode. By default, the IGMP Snooping is disabled.
DES-7200 (config)#**show ip igmp snooping**	Verify the configuration.
DES-7200(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.

This example sets the IGMP Snooping SVGL mode:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping svgl
DES-7200(config)# show ip igmp snooping
IGMP Snooping running mode: SVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

Note

In the SVGL mode, an IGMP Profile must be associated to specify the multicast address range in the SVGL mode, or the configuration related to the SVGL mode will not take effect. For the details, see the chapter of "Configuring the Multicast Address Range in the SVGL mode".

The layer 3 multicast-routing function cannot be enabled, or the command **ip multicast-routing** cannot be executed when the running mode is SVGL. Similarly, you cannot enter the SVGL mode when the layer 3 multicast-routing function has been enabled.

8.2.4 Configuring IVGL-SVGL Mode

In the global configuration mode, run the following commands to configure the IGMP Snooping IVGL-SVGL mode:

Command	Function
DES-7200(config)# **ip igmp snooping ivgl-svgl**	Enable the IGMP Snooping IVGL-SVGL mode. By default, the IGMP Snooping is disabled.
DES-7200 (config)#**show ip igmp snooping**	Verify the configuration.
DES-7200(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.

This example sets the IGMP Snooping IVGL-SVGL mode:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping ivgl-svgl
DES-7200(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL SVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

Note

In the SVGL mode, an IGMP Profile must be associated to specify the multicast address range in the SVGL mode, or the configuration related to the SVGL mode will not take effect. For the details, see the chapter of “Configuring the Multicast Address Range in the SVGL mode”.

The layer 3 multicast-routing function cannot be enabled, or the command **ip multicast-routing** cannot be executed when the running mode is SVGL. Similarly, you cannot enter the SVGL mode when the layer 3 multicast-routing function has been enabled.

8.2.5 Disabling IGMP Snooping

In the global configuration mode, run the following command to disable IGMP Snooping:

Command	Function
DES-7200(config)# **no ip igmp snooping**	Disable the IGMP Snooping function.
DES-7200 (config)#**show ip igmp snooping**	Verify the configuration.

This example disables the IGMP Snooping:

```
DES-7200# configure terminal
DES-7200(config)# no ip igmp snooping svgl
DES-7200(config)# show ip igmp snooping
IGMP Snooping running mode: DISABLE
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

8.2.6 Enabling IGMP Snooping in the Specific VLAN

By default, with IGMP Snooping globally enabled, the IGMP Snooping function is auto-enabled in all VLANs. To disable the IGMP Snooping in the specified VLAN, run the following command.

In the global configuration mode, run the following command to disable IGMP Snooping:

Command	Function
DES-7200(config)# **no ip igmp snooping vlan** *num*	Disable the IGMP Snooping in the specified VLAN. By default, the IGMP Snooping in the VLAN is enabled.
DES-7200 (config)# **ip igmp snooping vlan** *num*	Enable the IGMP Snooping in the specified VLAN.

This example disables the IGMP Snooping in the VLAN3:

```
DES-7200# configure terminal
DES-7200(config)# no ip igmp snooping vlan 3
DES-7200(config)# show ip igmp snooping
IGMP Snooping running mode: IVGL
SVGL vlan: 1
SVGL profile number: 11
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable

vlan 1
-------------
IGMP Snooping                :Enabled
```

```
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave         :Disabled

vlan 2
-------------
IGMP Snooping                 :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave         :Disabled

vlan 3
-------------
IGMP Snooping                 :Disabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave         :Disabled

vlan 4
-------------
IGMP Snooping                 :Enabled
Multicast router learning mode  :pim-dvmrp
IGMPv2 immediate leave         :Disabled
```

Note

With the IGMP Snooping enabled in the VLAN, the MLD Snooping function must also be enabled if the IPv6 multicast is applied in the VLAN.

8.2.7 Configuring the Aging Time for the Dynamic Route Port

If no IGMP general query packets or PIM Hello packets are received on the dynamic router port within the aging time, the router port will be deleted.

To configure the aging time for the dynamic router port, execute the following commands in the global configuration mode.

Command	Function
DES-7200(config)# **ip igmp snooping dyn-mr-aging-time** *time*	Configure the aging time for the dynamic router port. *Time:* aging time in the range of 1 to 3600s. Default value: 300s.
DES-7200(config)# **no ip igmp snooping dyn-mr-aging-time**	Return the aging time to the default value.

The following example configures the aging time of the dynamically learned router interface to 100s:

```
DES-7200# configure terminal
DES-7200 (config) # ip igmp snooping dyn-mr-aging-time 100
```

8.2.8 Configuring the Maximum Response Time of the IGMP Query Message

The multicast router periodically sends an IGMP Query message to query whether a multicast member exists or not. If the multicast router has not received the IGMP Report message from a host within a period of time, the switch will think this port no longer receives multicast frames, and delete this port from the multicast forwarding table. The default time is 10 seconds.

To configure the maximum response time of the IGMP Query message, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip igmp Snooping query-max-response-time** *seconds*	Set the maximum response time of the IGMP Query message in the range of 1 to 65535 seconds. The default time is 10 seconds.

Command	Function
DES-7200(config)# **no ip igmp Snooping query-max-response-time**	Restore the maximum response time to the default value.

The following example configures the maximum response time of the IGMP Query message to 15s:

```
DES-7200# configure terminal
DES-7200 (config) # ip igmp snooping query-max-response-time 15
```

8.2.9 Configuring IGMP Profiles

An IGMP Profile entry defines a set of multicast address range and permit/deny activity for the funcitons like multicast address range for SVGL mode, multicast data range filtered on the router interface, and IGMP Filtering range. Note that modifying an IGMP Profile after associating it with a function will influence the multicast forwarding table generated by the function.

To configure an IGMP profile, execute the following commands:

Command	Function
DES-7200(config)# **ip igmp profile** *profile-number*	Enter the IGMP Profile mode. Assign a number in the range of 1 to 1024 to identify. By default, no profile is configured.
DES-7200 (config-profile)# **permit** | **deny**	(Optional) Permit or deny this range of multicast addresses while deny or permit other multicast addresses. The default value is deny.
DES-7200(config-profile)# **range** *ip multicast-address*	Add one or more multicast address ranges.
DES-7200# **end**	Return to the privileged mode.

To delete an IGMP Profile, use **no ip igmp profile** *profile-number*.

To delete a range of the IGMP Profile, use **no range** *ip multicast address*.

This example shows the IGMP Profile configuration process:

```
DES-7200(config)# ip igmp profile 1
DES-7200 (config-profile) # permit
DES-7200 (config-profile) # range 224.0.1.0 239.255.255.255
DES-7200 (config-profile) # end
DES-7200# show ip igmp profile 1
IGMP Profile 1
permit
range 224.0.1.0 239.255.255.255
```

As you can see, the rule of the IGMP Profile is to permit the multicast addresses from 224.0.1.0 to 239.255.255.255, while all other multicast addresses are denied.

8.2.10 Configuring the Multicast Address Range in the SVGL /IVGL-SVGL Mode

When the IGMP Snooping works in the SVGL or IVGL-SVGL mode, a profile shall be associated to specify the multicast group address range applied in the SVGL or IVGL-SVGL mode. That is to say, the member ports of the multicast forwarding entry can be forwarded across VLANs while the member ports of the multicast forwarding entry in the other multicast address range must belong to the same VLAN. By default, no profile is associated.

Command	Function

Command	Function
DES-7200(config)# **ip igmp snooping svgl profile** *profile name*	Set a profile associated with the SVGL.
DES-7200(config)# **no ip igmp snooping svgl profile**	Remove a profile associated with the SVGL. The default value is 0.

This example configures the multicast address range in the SVGL or IVGL-SVGL mode:

```
DES-7200# configure terminal
DES-7200 (config) # ip igmp snooping ivgl-svgl
DES-7200 (config) # ip igmp snooping svgl profile 1
DES-7200 (config) # end
DES-7200# show ip igmp snooping
IGMP-snooping mode       :IVGL
SVGL vlan-id            : 1
SVGL profile number     : 1
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

8.2.11 Configuring the Ports of IGMP Snooping

8.2.11.1 Configuring the Route Port

By default, the router port is dynamically learned in the VLAN. Use the **no** option of the command to disable the dynamic learning function for the router interface in the VLAN and clear all router ports learned dynamically.

Use the command to set the switch port as the static router port.

To configure a router port, execute the following command:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	Set the interface as the static router interface.
DES-7200(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter interface** *interface-id*	Cancel the static router interface setting.
DES-7200(config)# **ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	Enable the dynamic learning function for the router interface in the VLAN. By default, the dynamic learning function is enabled.
DES-7200(config)# **no ip igmp snooping vlan** *vlan-id* **mrouter learn pim-dvmrp**	Disable the dynamic learning function for the router interface in the VLAN and clear all router ports learned dynamically.

This example sets GigabitEthernet 1/1 as the router port and enables dynamic learning function in the VLAN1:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 1 mrouter interface gigabitEthernet
0/7
DES-7200(config)# ip igmp snooping vlan 1 mrouter learn pim-dvmrp
DES-7200(config)# end
DES-7200# show ip igmp snooping mrouter
Vlan    Interface        State       IGMP profile
----    ---------        ------      -------------
1   GigabitEthernet 0/7   static          0
1   GigabitEthernet 0/12  dynamic         0
DES-7200# show ip igmp snooping mrouter learn
Vlan   learn method
----   ------------------
1      pim-dvmrp
```

8.2.11.2 Configuring Static Member Port

When IGMP Snooping is enabled, you can statically configure a port to receive a specific multicast flow in disregard of various IGMP packets.

To configure a static member port of IGMP Snooping, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip igmp Snooping ivgl**	Enable IGMP Snooping and set it as the IVGL mode.
DES-7200(config)# **ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *[interface-id]*	Statically configure a port to receive a certain multicast flow. • *vlan-id*: vid of multicast flow • *ip-addr* : multicast group address • *interface-id:* Interface ID
DES-7200(config)# **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *[interface-id]*	Remove a static member port. • *vlan-id*: vid of multicast flow • *ip-addr* : multicast group address • *interface-id:* Interface ID

Use **no ip igmp snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* to delete the static member of IGMP Snooping.

This example configures a static member port of IGMP snooping:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 1 static 233.3.3.4 interface
GigabitEthernet 0/7
DES-7200(config)# end
DES-7200(config)# show ip igmp snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address              Member ports
---- --------------   ----------------------------
1    233.3.3.4            GigabitEthernet 0/7(S)
```

8.2.11.3 Configuring Fast-Leave

According to the IGMP protocol, a port cannot leave a multicat group immediately after the host sends the IGMP Leave message. Instead, the multicast router should first send an IGMP Query packet and lets a port leave the group only when the host does not respond. However, in specific environments (for example, one port is connected to only one multicast user), the port can immediately leave the multicast group after the multicast router receives the IGMP Leave message, a mechanism known as Fast Leave.

To enable fast-leave, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip igmp snooping fast-leave enable**	Enable the fast-leave function.
DES-7200(config)# **no ip igmp snooping fast-leave enable**	Disable the fast-leave function.

The following example enables the fast–leave function:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping fast–leave enalbe
DES-7200(config)# end
```

8.2.11.4 Configuring IGMP Snooping Suppression

For IGMP Snooping-enabled devices, a multicast group address may have multiple IGMP users. When a user joins the multicast group and receives the IGMP Query message, he or she will send an IGMP Report message. DES-7200 switches will forward every IGMP Query message to the multicast router. In this way, the multicast router will receive multiple IGMP Report messages when it sends an IGMP Query message to the ports on the IGMP Snooping-enabled devices.

To reduce the pressure of the server on processing the IGMP Report messages, the switch only forwards the first received IGMP Report message to the router port while suppressing other IGMP Report messages. This is called IGMP Snooping Suppression.

To enable IGMP Snooping suppression, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip igmp snooping suppression enable**	Enable IGMP Snooping suppression. By default, this function is enabled.
DES-7200(config)# **no ip igmp snooping suppression enable**	Disable IGMP Snooping suppression.

The following example enables the IGMP Snooping suppression function:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping suppression enalbe
DES-7200(config)# end
```

8.2.12 Configuring the Multicast Security Control

- (Optional) Configure source port check
- (Optional) Configure source IP check
- (Optional) Configure port filter
- (Optional) Configure VLAN filter
- (Optional) Configure multicast preview

8.2.12.1 Configuring Source Port Check

In global configuration mode, execute the following steps to configure source port check:

Command	Function
DES-7200(config)# **ip igmp snooping source-check port**	Enable source port check.
DES-7200(config)# **no ip igmp snooping source-check port**	Disable source port check.

The following example shows how to enable source port check:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping source-check port
```

8.2.12.2 Configuring Source IP Check

Source IP check corresponds to two commands: 1) configuration of default source IP address of valid multicast traffic for all multicast groups; 2) configuration of the source IP address of valid multicast traffic for a specific multicast group belonging to specific VLAN. The source IP address of valid multicast server can only be configured for a specific group after enabling default source IP check of all groups.

In global configuration mode, execute the following steps to enable IGMP Snooping source IP check:

Command	Function
DES-7200(config)# **ip igmp snooping source-check default-server** *address*	Enable source IP check and configure the default source IP address of valid multicast traffic for all groups. This feature is disabled by default.
DES-7200(config)# **no ip igmp snooping source-check default-server**	Disable source IP check.
DES-7200(config)# **ip igmp snooping limit-ipmc vlan** *vid* **address** *address* **server** *address*	Configure the source IP address of valid multicast traffic for specific group address. By default, the source IP address of the valid multicast traffic for this group address is the same as the IP address of default-server.
DES-7200(config)# **no ip igmp snooping limit-ipmc vlan** *vid* **address** *address*	Remove the configuration of limit-ipmc.

The following example shows how to enable source IP check and configure the default source IP to 1.1.1.1, and how to configure the source IP address of valid multicast traffic for group 233.3.3.3 belonging to VLAN1 to 1.1.1.2.

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping source-check default-server 1.1.1.1
```
DES-7200(config)# ip igmp snooping limit-ipmc vlan *1* address *233.3.3.3* server *1.1.1.2*

Caution

IGMP Snooping source IP check cannot be shared with layer-3 multicasting, which means layer-3 multicast forwarding will be compromised after enabling layer-3 multicasting and source IP check at the same time.

8.2.12.3 Configuring Port Filter

Under certain circumstances, you may need to control a specific port to only receive a group of specific multicast traffic and control the maximum number of groups that can be joined on this port. IGMP Filtering well meets such needs.

You can apply an IMGP Profile to a port. If IMGP Report packets are received on the port, the layer-2 multicast device will verify whether the multicast address to be joined by this port falls within the range permitted by IGMP Profile. If yes, the port will join and process subsequently.

You can also configure the maximum number of groups that can be joined by the port. If the threshold is exceeded, the layer-2 multicast device will no longer receive and process IGMP Report packets.

In global configuration mode, execute the following steps to configure IGMP Filtering:

Command	Function
DES-7200(config)# **interface** *interface-id*	Enter the interface to be configured.
DES-7200(config-if)# **ip igmp snooping filter** *profile-number*	(Optional) Apply Profile to this interface. The range of profile number if 1-1024. By default, a port is not associated with any profile.
DES-7200(config-if)# **no ip igmp snooping filter**	(Optional) Delete the profile associated to the interface, which will then permit all groups.
DES-7200(config-if)# **ip igmp snooping max-groups** *number*	(Optional) Configure the maximum number (0-1024) of groups that can be joined on this port. The number is not restricted by default.

The following example shows how to configure the filter:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip igmp snooping filter 1
DES-7200(config-if)# ip igmp snooping max-groups 1000
DES-7200(config-if)# end
DES-7200# show ip igmp snooping interface fastEthernet 0/1
Interface            Filter profile number       max-group
---------------      ---------------------       ---------
FastEthernet 0/1            1                        1000
```

8.2.12.4 Configuring VLAN Filter

Under certain circumstances, you may need to control the reception of multicast traffic on the egress of specific VLAN. VLAN-based filter well meets such need.

You can apply an IMGP Profile to a VLAN. If IMGP Report packets are received on the port belong to this VLAN, the layer-2 multicast device will verify whether the multicast address to be joined by this port falls within the range permitted by IGMP Profile. If yes, the port will join and process subsequently.

In global configuration mode, execute the following steps to configure IGMP Filtering:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *num* **filter** *profile-number*	(Optional) Apply Profile to this VLAN. The range of profile number if 1-1024. By default, a VLAN is not associated with any profile.
DES-7200(config-if)# **no ip igmp snooping vlan** *num* **filter**	(Optional) Delete the profile associated to the VLAN, which will then permit all groups.

The following example shows how to configure the VLAN filter:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip igmp snooping vlan 2 filter 1
```

8.2.12.5 Configuring Multicast Preview

To configure multicast preview, the following information must be configured: the multicast group that can be previewed, and the preview interval.

In global configuration mode, execute the following steps to configure multicast preview:

Command	Function

DES-7200(config)# **ip igmp snooping preview** *profile-number*	(Optional) Apply Profile to this preview. The range of profile number if 1-1024. By default, a multicast traffic can be previewed.
DES-7200(config)# **ip igmp snooping preview interval** *num*	(Optional) Configure preview interval. The range of num is 1-300, and the default value is 60 seconds.
DES-7200(config)# **no ip igmp snooping preview**	(Optional) No preview.

The following example shows how to configure multicast preview. Multicast traffic failing to match profiles1 but matching profiles2 can be previewed.

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping preview 2
DES-7200(config)# int fa 0/1
DES-7200(config-if)# ip igmp snooping filter 1
```

8.2.13 Configuring the Relationship Between IGMP Snooping and QinQ

By default, IGMP Passthrough is disabled. In global configuration mode, execute the following steps to configure the relationship between IGMP Snooping and QinQ:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **ip igmp snooping tunnel**	Enable IGMP Passthrough: After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, create multicast entries on the VLAN to which IMGP packets belong, and forward IMGP packets on such VLAN. For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 10 and forward the multicast requests to the router port of VLAN 10. By default, IGMP Passthrough is disabled.
DES-7200(config)# **no ip igmp snooping tunnel**	Disable IGMP Passthrough. After IGMP Snooping is enabled and dot1q-tunnel port is configured on the device, create multicast entries on the default VLAN to which dot1q-tunnel belong, and forward multicast packets on the default VLAN of dot1q-tunnel port after inserting the VLAN Tag of the default VLAN of dot1q-tunnel port. For example: It is assumed that IGMP Snooping has been enabled on the device; port A is a dot1q-tunnel port; the default VLAN of port A is VLAN 1, and packets from VLAN 1 and VLAN 10 can pass through port A. When multicast requests of VLAN 10 are sent to port A, IGMP Snooping will create the multicast entry of VLAN 1 and insert the VLAN Tag of VLAN 1 into multicast requests before forwarding the multicast requests to the router port of VLAN 1.

The following example shows how to enable IGMP Passthrough:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping tunnel
```

8.2.14 Configuring IGMP Snooping Querier

8.2.14.1 Globally Enabling Querier

In global configuration mode, execute the following steps to enable global querier:

Command	Function
DES-7200(config)# **ip igmp snooping querier**	Globally enable IGMP querier.
DES-7200(config)# **no ip igmp snooping querier**	Globally disable IGMP querier.

The following example shows how to globally enable IGMP querier:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping querier
```

8.2.14.2 Globally Configuring Querier Source IP

In global configuration mode, execute the following steps to globally configure the source IP address of queries:

Command	Function
DES-7200(config)# **ip igmp snooping querier address a.b.c.d**	Globally configure querier source IP.
DES-7200(config)# **no ip igmp snooping querier address**	Globally disable querier source IP.

The following example shows how to globally configure the source IP address of IGMP querier:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping querier address 192.168.2.2
```

8.2.14.3 Globally Configuring the Maximum Response Time to Queries

In global configuration mode, execute the following steps to configure the maximum response time to queries:

Command	Function
DES-7200(config)# **ip igmp snooping querier max-response-time** *num*	Globally configure the maximum response time to queries. The default value is 10 seconds.
DES-7200(config)# **no ip igmp snooping querier max-response-time**	Globally restore the maximum response time to queries to default value.

The following example shows how to configure the maximum response time to queries:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping querier 20
```

8.2.14.4 Globally Configuring the Query Interval

In global configuration mode, execute the following steps to configure the interval for periodically sending queries:

Command	Function
DES-7200(config)# **ip igmp snooping querier query-interval** *num*	Globally configure the interval for periodically sending IGMP queries. The default value is 60 seconds.
DES-7200(config)# **no ip igmp snooping querier query-interval**	Globally restore the interval for periodically sending IGMP queries to default value.

The following example shows how to globally configure the query interval:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping querier query-interval 300
```

8.2.14.5 Globally Configuring Querier Expiration Timer

In global configuration mode, execute the following steps to configure querier expiration timer:

Command	Function
DES-7200(config)# **ip igmp snooping querier timer expiry** *num*	Globally configure querier expiration timer.
DES-7200(config)# **no ip igmp snooping querier timer expiry**	Globally configure querier expiration timer to the default value.

The following example shows how to globally configure querier expiration timer:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping querier timer expiry 70
```

8.2.14.6 Globally Configuring IGMP Version Number

In global configuration mode, execute the following steps to globally configure IGMP version number:

Command	Function
DES-7200(config)# **ip igmp snooping querier version** *num*	Globally configure IGMP version number (1-2). Default value: 2.
DES-7200(config)# **no ip igmp snooping querier version**	Globally restore IGMP version number to the default value.

The following example shows how to globally configure IGMP version number:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping querier version 1
```

8.2.14.7 Globally Configuring Querier Function on VLAN

In global configuration mode, execute the following steps to enable querier funtion on VLAN:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *num* **querier**	Enable IGMP querier function on VLAN.
DES-7200(config)# **no ip igmp snooping vlan** *num* **querier**	Disable IGMP querier function on VLAN.

The following example shows how to enable IGMP querier on VLAN:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 2 querier
```

8.2.14.8 Globally Configuring Source IP for Querier on VLAN

In global configuration mode, execute the following steps to globally configure the source IP address of queries on VLAN:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *num* **querier address a.b.c.d**	Configure the source IP of querier on VLAN.
DES-7200(config)# **no ip igmp snooping vlan** *num* **querier address**	Remove the source IP of querier on VLAN.

The following example shows how to globally configure the source IP address of IGMP querier:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 2 querier address 192.168.2.2
```

8.2.14.9 Globally Configuring the Maximum Response Time to Queries on VLAN

In global configuration mode, execute the following steps to configure the maximum response time to queries:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *num* **querier max-response-time** *num*	Configure the maximum response time to queries on VLAN. The default value is 10 seconds.
DES-7200(config)# **no ip igmp snooping vlan** *num* **querier max-response-time**	Restore the maximum response time to queries on VLAN to default value.

The following example shows how to configure the maximum response time to queries:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 2 querier 20
```

8.2.14.10 Globally Configuring the Query Interval on VLAN

In global configuration mode, execute the following steps to configure the interval for periodically sending queries:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *num* **querier query-interval** *num*	Configure the interval for periodically sending IGMP queries on VLAN. The

	default value is 60 seconds.
DES-7200(config)# **no ip igmp snooping vlan** *num* **querier query-interval**	Restore the interval for periodically sending IGMP queries on VLAN to default value.

The following example shows how to configure the query interval on VLAN:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 2 querier query-interval 300
```

8.2.14.11 Globally Configuring Querier Expiration Timer on VLAN

In global configuration mode, execute the following steps to configure querier expiration timer:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *num* **querier timer expiry** *num*	Configure querier expiration timer on VLAN.
DES-7200(config)# **no ip igmp snooping vlan** *num* **querier timer expiry**	Configure querier expiration timer on VLAN to default value.

The following example shows how to configure querier expiration timer on VLAN:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 2 querier timer expiry 70
```

8.2.14.12 Globally Configuring IGMP Version Number on VLAN

In global configuration mode, execute the following steps to configure IGMP version number on VLAN:

Command	Function
DES-7200(config)# **ip igmp snooping vlan** *num* **querier version** *num*	Configure IGMP version number (1-2) on VLAN. Default value: 2.
DES-7200(config)# **no ip igmp snooping vlan** *num* **querier version**	Restore IGMP version number to the default value on VLAN.

The following example shows how to configure IGMP version number on VLAN:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping vlan 2 querier version 1
```

8.2.15 Configuring Multicast VLAN

8.2.15.1 Enabling SVGL mode

In global configuration mode, execute the following steps to enable SVGL mode of IGMP Snooping:

Command	Function
DES-7200(config)# **ip igmp snooping svgl**	Enable SVGL mode of IGMP Snooping.
DES-7200(config)# **ip igmp snooping ivgl-svgl**	Enable IVGL-SVGL mode of IGMP Snooping.

DES-7200(config)# **no ip igmp snooping**	Disable IGMP Snooping.

The following example shows how to globally enable IGMP querier:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping svgl
```

8.2.15.2 Configuring the Master VLAN of Multicast VLAN

In global configuration mode, execute the following steps to configure the master VLAN of multicast VLAN:

Command	Function
DES-7200(config)# **ip igmp snooping svgl vlan** *num*	Configure the master VLAN of multicast VLAN.
DES-7200(config)# **no ip igmp snooping svgl vlan**	Configure the default VLAN of multicast VLAN.

The following example shows how to globally configure the master VLAN of multicast VLAN to VLAN 2:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping svgl vlan 2
```

Caution

By default, the master VLAN of multicast VLAN is VLAN 1. After enabling multicast VLAN, the multicast traffic falling into the group address range of multicast VLAN can only be received and processed if entering from multicast VLAN; traffic entering from other VLANs won't be received and processed.

8.2.15.3 Configuring the Sub-VLANs of Multicast VLAN

In global configuration mode, execute the following steps to configure the sub-VLANs of multicast VLAN:

Command	Function
DES-7200(config)# **ip igmp snooping svgl subvlan** *num*	Configure the sub-VLANs of multicast VLAN.
DES-7200(config)# **no ip igmp snooping svgl subvlan**	Remove the sub-VLANs of multicast VLAN.

The following example shows how to globally configure the sub-VLANs of multicast VLAN to VLAN 3 and VLAN 6:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping svgl subvlan 3,6
IGMP Snooping running mode: IVGL-SVGL
SVGL vlan: 1
SVGL profile number: 1
IGMP Snooping SVGL subvlan 3,6
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 300(Seconds)

vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

```
vlan 3
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 4
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 6
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

Caution

By default, no sub-VLAN of the multicast VLAN is configured on the device. By this time all other VLANs will be able to receive the multicast traffic from master VLAN.

If sub-VLANs are configured, only VLANs falling into the range of sub-VLANs can receive multicast traffic.

8.2.15.4 Configuring the Multicast Address range of Multicast VLAN

After configuring the operating mode of IGMP Snooping to SVGL mode or IVGL-SVGL mode, you need to associate SVGL to one profile in order to specify which group addresses can be applied with SVGL mode, namely the member ports of multicast forwarding table entries can forward traffic across VLAN, while the member ports of multicast forwarding table entries corresponding to other multicast address ranges must belong to the same VLAN. By default, no profile is associated, meaning that no multicast group can be applied with SVGL mode.

Command	Function
DES-7200(config)# **ip igmp snooping svgl profile** *profile_num*	Configure to associate one profile with SVGL.
DES-7200(config)# **no ip igmp snooping svgl profile**	Disable SVGL-profile association and restore to the default value of 0.

The following example shows how to configure the multicast address range applied with SVGL mode:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping ivgl-svgl
DES-7200(config)# ip igmp snooping svgl profile 1
DES-7200(config)# end
DES-7200# show ip igmp snooping
IGMP Snooping running mode: IVGL_SVGL
SVGL vlan: 1
SVGL profile number: 1
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 30000(Seconds)

vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
```

```
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

8.2.16 Configuring IP Multicast Policy on Ports

8.2.16.1 Configuring Source Port Check

To enable source port check, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip igmp snooping source-check port**	Enable source port check.
DES-7200(config)# **no ip igmp snooping source-check port**	Disable source port check.

The following example enables the IGMP Snooping source port check function:

```
DES-7200# configure terminal
DES-7200(config)# ip igmp snooping source-check port
DES-7200(config)# end
```

8.2.16.2 Configuring Source IP Check

There are two configuration commands for the source IP check: one command is for the configuration of default source IP addresses of the legal multicast flows in all multicast groups; and the other command is for the configuration of the default source IP address for the legal multicast flows in the specified VLAN group. Only with the default source IP check enabled in all groups, the source IP address of the legal multicast server in a specific group can be set.

To enable source IP check, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **ip igmp snooping source-check default-server** *address*	Enable source IP check and configure the default source IP address of the legal multicast flows in all multicast groups. By default, this function is disabled.
DES-7200(config)# **no ip igmp snooping source-check default-server**	Disable source IP check.
DES-7200(config)# **ip igmp snooping limit-ipmc vlan** *vid* **address** *address* **server** *address*	Add the source IP address of the legal multicast flow to a specified multicast group addresses. By default, the source IP address of the legal multicast flow is the IP address of the default-server.
DES-7200(config)# **no ip igmp snooping limit-ipmc vlan** *vid* **address** *address*	Cancel a limit-ipmc configuration.

The following example enables source IP check and set the default source IP address to 1.1.1.1. In the example, a multicast group address-source IP address entry is added, where vid is 1, group IP address is 233.3.3.3 and source ip address is 1.1.1.2.

```
DES-7200# configure Terminal
DES-7200(config)# ip igmp snooping source-check default-server 1.1.1.1
DES-7200(config)# ip igmp snooping limit-ipmc vlan 1 address 223.3.3.3 server
1.1.1.2
```

```
DES-7200(config)# end
```

8.2.16.3 Configuring IGMP Filtering

In some cases, you may need to limit a port to receive a specified set of multicast data flows, and control the maximum number of multicast groups that the port is allowed to join dynamically IGMP Filtering can address this requirement.

You can apply one IGMP Profile to a port. If the port receives the IGMP Report message, the switch will check if the IP address of the multicast group that the port wants to join is permitted by the IGMP Profile. If so, the switch allows it to join the multicast group.

You can also configure the maximum number of multicast groups that the port is allowed to join. If the number of the multicast groups that the port joins exceeds the threshold, the switch will no longer receive or handle the IGMP Report message.

To enable IGMP Filtering, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration interface.
DES-7200(config-if)# **ip igmp snooping filter** *profile-number*	(Optional) Apply a profile to the interface. The profile number ranges from 1 to 1024.
DES-7200(config-if)# **ip igmp snooping max-groups** *number*	(Optional) Specify the maximum number of multicast groups that the interface can join, in the range of 0 to 1024.
DES-7200(config-if)# **no ip igmp snooping max-groups**	(Optional) Restore the max-groups to the default value.

The example below shows how to configure IGMP Flitering:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ip igmp snooping filter 1
DES-7200(config-if)# ip igmp snooping max-groups 1000
DES-7200 (config-if)#end
DES-7200 #show ip igmp snooping interface fastEthernet 0/1
Interface            Filter profile number       max-group
---------------      ---------------------       ---------
FastEthernet 0/1            1                        1000
```

8.3 Showing IGMP Snooping Information

8.3.1 Showing Current Mode

To view the current operation mode and global configuration of IGMP Snooping, execute the following command in the privileged mode:

Command	Function
DES-7200# **show ip igmp snooping**	View the current operation mode and global configuration of IGMP Snooping.

The following example uses the **show ip igmp snooping** command to view the IGMP Snooping configuration information:

```
DES-7200# show ip igmp snooping
IGMP-snooping mode     : IVGL
SVGL vlan-id           : 1
SVGL profile number    : 0
```

```
Source port check      : Disabled
Source ip check        : Disabled
IGMP Fast-Leave        : Disabled
IGMP Report suppress    : Disable
```

8.3.2 Showing and Clearing IGMP Snooping Statistics

To view and clear the IGMP Snooping statistics, execute the following commands in the privileged mode:

Command	Function
DES-7200# **show ip igmp snooping statistics** [**vlan** *vlan-id*]	View the IGMP Snooping statistics
DES-7200# **clear ip igmp snooping statistics**	Clear the IGMP Snooping statistics

The following example uses the **show ip igmp snooping statistics** command to view the IGMP Snooping statistics:

```
DES-7200# show ip igmp snooping statistics
Current number of Gda-table entries: 1
Configured Statistics database limit: 1024
Current number of IGMP Query packet received : 1957
Current number of IGMPv1/v2 Report packet received: 5
Current number of IGMPv3 Report packet received: 4
Current number of IGMP Leave packet received: 1

GROUP  Interface  Last Last  Report  Leave report time reporter  pkts   pkts
------   -------- ---------- ----------- ---- -- -------- ----
233.3.3.3 gi1/1   00:02:40    1.1.1.1     3       1
```

8.3.3 Showing the Route Interface

To view the route interface information of IGMP Snooping, execute the following commands in the privileged mode:

Command	Function
DES-7200# **show ip igmp snooping mrouter**	Show the router interface information of IGMP Snooping

The following example uses the **show ip igmp snooping** command to view the router interface information of IGMP Snooping:

```
DES-7200# show ip igmp snooping mrouter
Vlan    Interface           State       IGMP profile number
----    --------             -------      -------------------
1   GigabitEthernet 0/7    static        1
1   GigabitEthernet 0/12   dynamic       0
```

8.3.4 Showing Dynamic Forwarding Table

To view the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged mode:

Command	Function
DES-7200# **show ip igmp snooping gda-table**	Show the forwarding rule of each port in the multicast group.

This example shows the information on various multicast groups of the GDA table and the information on all the member ports of one multicast group:

```
DES-7200# show ip igmp snooping gda-table
Abbr: M - mrouter
      D - dynamic
      S - static
```

```
VLAN  Address              Member ports
--------------------    ---------------------------------
1      233.3.3.3          GigabitEthernet 0/7(S)
```

8.3.5 Clearing Dynamic Forwarding Table

To clear the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged mode:

Command	Function
DES-7200#**clear ip igmp snooping gda-table**	Clear the forwarding rule of each port in the multicast group.

8.3.6 Clearing IGMP Snooping Statistics

To clear the forwarding rule of each port in the multicast group, that is, the GDA(Group Destination Address) table, execute the following commands in the privileged mode:

Command	Function
DES-7200#**clear ip igmp snooping statistics**	Clear the dynamic statistics of the entry node in the forwarding table.

8.3.7 Showing Source Port Check Status

To view the current source port check status of IGMP Snooping, execute the following command in the privileged mode:

Command	Function
DES-7200# **show ip igmp snooping**	View the current operation mode and global configuration of IGMP Snooping.

This example shows the source port check status of IGMP Snooping:

```
DES-7200(config)# show ip igmp snooping
IGMP-snooping mode        :IVGL
SVGL vlan-id             :1
SVGL profile number      :0
Source check port        :Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
```

8.3.8 Showing IGMP Profile

To view the IGMP Profile information, execute the following command in the privileged mode:

Command	Function
DES-7200# **show ip igmp profile** *profile-number*	View the IGMP Profile information.

This example shows the IGMP Profile information:

```
DES-7200# show ip igmp profile 1
Profile    1
       Permit
```

```
range 224.0.1.0,   239.255.255.255
```

8.3.9 Showing IGMP Filtering

To view the IGMP Filtering information, execute the following command in the privileged mode:

Command	Function
DES-7200# **show ip igmp snooping interface** *interface-id*	View IGMP Filtering information.

The following example views the IGMP Filtering information.

```
DES-7200# show ip igmp snooping interface GigabitEthernet 0/7
Interface        Filter Profile number     max-groups
```

8.3.10 Showing IGMP Snooping Querier

To view the IGMP Snooping Querier information, execute the following command in the privileged mode:

Command	Function
DES-7200# **show ip igmp snooping querier**	View IGMP Querier information.
DES-7200# **show ip igmp snooping querier detail**	View the details of IGMP Querier.

The following example views the IGMP Querier information.

```
DES-7200# show ip igmp snooping querier detail
Vlan     IP Address         IGMP Version         Port
-----------------------------------------------------------

Global IGMP switch querier status
-----------------------------------------------------
admin state                : Enable
admin version              : 2
source IP address           : 1.1.1.1
query-interval (sec)         : 125
max-response-time (sec)       : 10
querier-timeout (sec)        : 60

Vlan 1:  IGMP switch querier status
-----------------------------------------------------
admin state                : Enable
admin version              : 2
source IP address           : 1.1.2.2
query-interval (sec)         : 125
max-response-time (sec)       : 10
querier-timeout (sec)        : 60
operational state           : Disable
operational version          : 2

Vlan 2:  IGMP switch querier status
-----------------------------------------------------
admin state                : Disable
admin version              : 2
source IP address           : 1.1.1.1
query-interval (sec)         : 125
max-response-time (sec)       : 10
querier-timeout (sec)        : 60
operational state           : Disable
operational version          : 2
```

8.4 Typical IGMP Snooping Configuraiton Example

8.4.1 Example of IVGL mode Configuration

- **Topological Diagram**

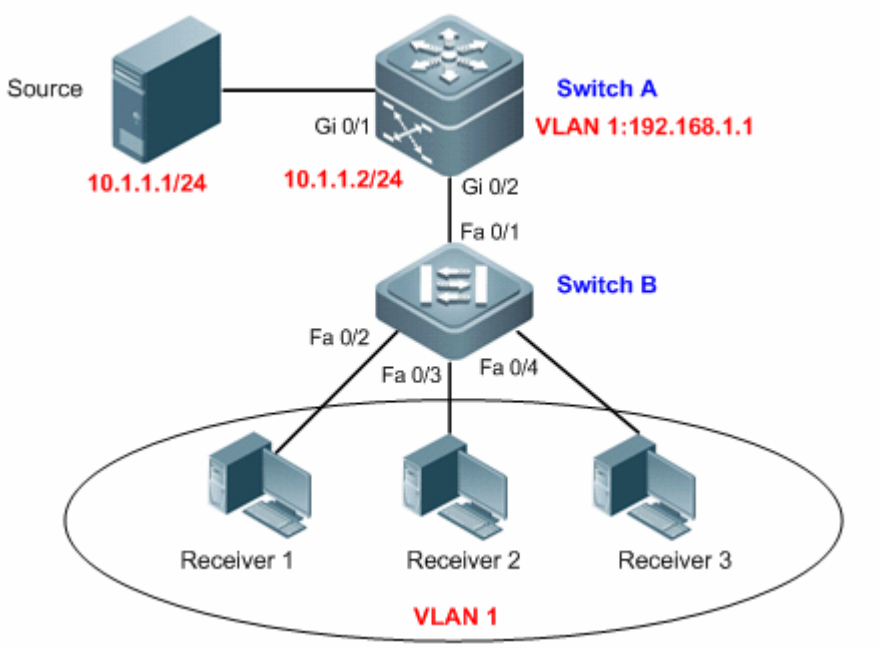


Figure4 Diagram for IVGL mode

- **Application Requirements**

As shown above, Switch A is a multicast routing device directly connected with a multicast source, and Switch B is a layer-2 access device connected with multiple multicast receivers which belong to the same VLAN. The primary requirements are shown below: ：

Achieve layer-3 multicast routing on Switch A, and on Switch B, multicast traffic won't be broadcasted on VLAN but sent to the specified receiver.

Receiver 1 can receive IP multicast traffic with group address being 224.1.1.1; Receiver 2 can only receive IP multicast traffic with group address falling within 225.1.1.1-226.1.1.1; Receiver 3 can only join 100 IP multicast groups.

On Switch B, all access ports can quickly leave a specific IP multicast group.

On Switch B, IGMP members are prohibited from forwarding response messages to Switch A, so as to lessen the burden of Switch A.

- **Configuration Tips**

On the multicast routing device (Switch A), enable multicast routing and forwarding and configure multicast routing protocol on the corresponding layer-3 interface (Gi 0/1 and VLAN 1); on the layer-2 multicast device (Switch B), configure IGMP Snooping to operate in IVGL mode; the router port can be generated dynamically or configured statically (configure port Fa 0/1 as the static router port).

Configure the port directly connected with Receiver 1 (Fa 0/2) as the static member port of corresponding group; configure IGMP Filtering on the port directly connected with Receiver 2 (Fa 0/3); Configure the maximum number of multicast

groups that can be joined on the port directly connected with Receiver 3 (Fa 0/4).

Enable fast leave on the device running IGMP Snooping (Switch B).

Configure IGMP Snooping report suppression on the device running IGMP Snooping (Switch B).

- **Configuration Steps**

Step 1: Configure multicast routing on the multicast routing device.

! Globally enable multicast routing and forwarding on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ip multicast-routing
```

! Configure port Gi 0/1 of Switch A as a router port for connecting multicast source and configure the multicast routing protocol

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#ip pim dense-mode
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

! Configure the SVI and VLAN 1 and configure multicast routing protocol on SVI.

```
SwitchA(config)#interface vlan 1
SwitchA(config-if-VLAN 1)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 1)#ip pim dense-mode
SwitchA(config-if-VLAN 1)#exit
```

! Configure port Gi 0/2 as a trunk port for connecting layer-2 multicast device.

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

Step 2: Enable IGMP Snooping on layer-2 multicast device and configure router port.

! On Switch B, globally configure IGMP Snooping to operate in IVGL mode and configure Fa 0/1 as the router port of VLAN 1.

```
SwitchB(config)#ip igmp snooping ivgl
SwitchB(config)#ip igmp snooping vlan 1 mrouter interface fastEthernet 0/1
```

Step 3: Configure the ports connecting with Receiver 1, Receiver 2 and Receiver 3.

! Configure port Fa 0/2 as the static member port of VLAN 1 with group address being 224.1.1.1.

```
SwitchB(config)#ip igmp snooping vlan 1 static 224.1.1.1 interface fastEthernet 0/2
```

! Configure IGMP Profile1 to receive only the IP multicast traffic with group address falling within 225.1.1.1-226.1.1.1 and apply to port Fa 0/3.

```
SwitchB(config)#ip igmp profile 1
SwitchB<config-profile>#permit
SwitchB<config-profile>#range 225.1.1.1 226.1.1.1
SwitchB<config-profile>#exit
SwitchB(config)#interface fastEthernet 0/3
SwitchB(config-if-FastEthernet 0/3)#ip igmp snooping filter 1
SwitchB(config-if-FastEthernet 0/3)#exit
```

! Configure that port Fa 0/4 can be joined by up to 100 multicast groups.

```
SwitchB(config)#interface fastEthernet 0/4
SwitchB(config-if-FastEthernet 0/4)#ip igmp snooping max-groups 100
SwitchB(config-if-FastEthernet 0/4)#exit
```

Step 4: On layer-2 device, configure that all access sports can quickly leave a certain IP multicast group and enable IGMP report suppression.

! Enable fast leave on Switch B.

```
SwitchB(config)#ip igmp snooping fast-leave enable
```

! Enable IGMP Snooping report suppression on Switch B.

```
SwitchB(config)#ip igmp snooping suppression enable
```

- **Verification**

Step 1: Display device configurations

! Configurations of Switch A

```
SwitchA#show running-config
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
 ip pim dense-mode
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface VLAN 1
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
```

! Configurations of Switch B

```
SwitchB#show running-config
!
interface FastEthernet 0/3
 ip igmp snooping filter 1
!
interface FastEthernet 0/4
 ip igmp snooping max-group 100
!
ip igmp profile 1
permit
range 225.1.1.1 226.1.1.1
ip igmp snooping ivgl
ip igmp snooping vlan 1 static 224.1.1.1 interface FastEthernet 0/2
ip igmp snooping vlan 1 mrouter interface FastEthernet 0/1
ip igmp snooping fast-leave enable
ip igmp snooping suppression enable
```

Step 2: Display the IGMP Snooping configurations of Switch B

```
SwitchB#show ip igmp snooping
IGMP Snooping running mode: IVGL
Source port check: Disable
Source ip check: Disable
IGMP Fast-Leave: Enable
IGMP Report suppress: Enable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 300(Seconds)
Tunnel IGMP Packet：Disable

vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 fast leave: Disabled
IGMP VLAN querier: Disable
```

Step 3: Display router port configuration of Switch B

```
SwitchB#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 1):
  VLAN(1)  1 MROUTES:
    FastEthernet 0/1 (S)
```

Step 4: Display interface configurations of IGMP Snooping

```
SwitchB#show ip igmp snooping interfaces
Interface         Filter profile number   max-group
```

```
----------------- -------------------- ---------
FastEthernet 0/3   1                    4294967294
FastEthernet 0/4   0                    100
```

Step 5: Send IP multcast traffic with group address being 224.2.2.2 through the Source, and reqeust multicast traffic on port Fa 0/2 of Switch B. Display the group members of Switch A and CDA table of Switch B.

! Switch A

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
224.2.2.2       VLAN 1  00:00:51  00:03:55  0.0.0.0
```

! Switch B

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,224.1.1.1, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(S)
(*,224.2.2.2, 1):
  VLAN(1) 2 OPORTS:
    FastEthernet 0/1(M)
    FastEthernet 0/2(D)
```

8.4.2 Example of IVGL-SVGL mode Configuration

- **Topological Diagram**

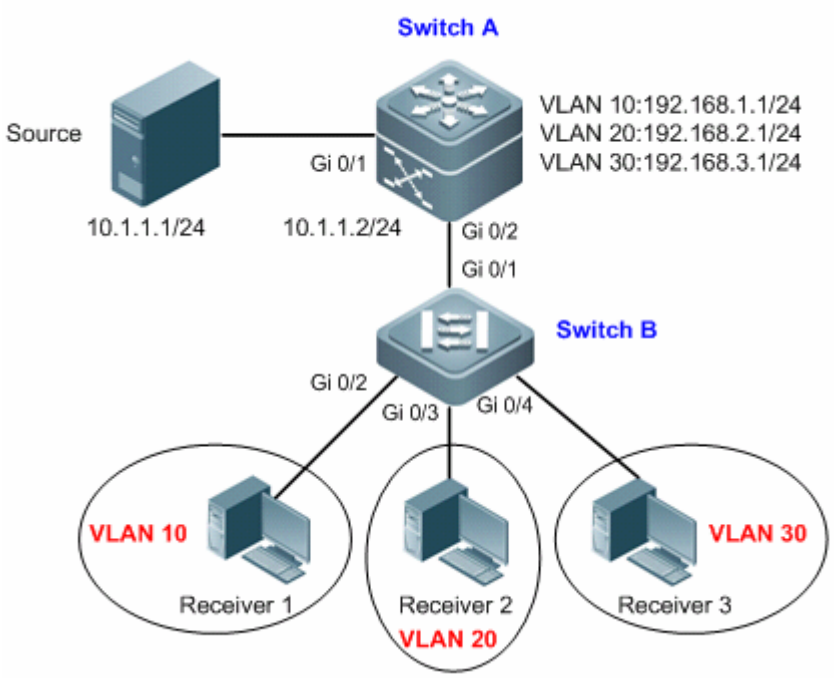


Figure5 Diagram for IVGL mode

- **Application Requirements**

As shown above, Switch A is a multicast routing device directly connected with a multicast source, and Switch B is a layer-2 access device connected with multiple multicast receivers which belong to different VLANs. The primary requirements are shown below:

Achieve layer-3 multicast routing on Switch A, and on Switch B, multicast traffic won't be broadcasted on VLAN but sent to the specified receiver.

On Switch B, specify that IP multicast traffic with multicast address falling within 224.1.1.1-226.1.1.1 can be forwarded across VLAN, while other IP multicast traffic can only be forwarded to the member ports belonging to the same VLAN.

On Switch B, only IP multicast traffic received by the router port will be forwarded, and IP multicast traffic received by non-router port will be blocked.

- **Configuration Tips**

On the multicast routing device (Switch A), enable multicast routing and forwarding and configure multicast routing protocol on the corresponding layer-3 interface (Gi 0/1 and VLAN 10, VLAN 20 and VLAN 30); on the layer-2 multicast device (Switch B), configure IGMP Snooping to operate in IVGL-SVGL mode; the router port can be generated dynamically or configured statically (configure port Gi 0/1 as the static router port).

On the layer-2 multicast device (Switch B) running IGMP Snooping, specify a VLAN as Share VLAN (VLAN 10) and configure the multicast address range (224.1.1.1-226.1.1.1) of Share VLAN, so that IP multicast traffic falling within this multicast address range can be forwarded across VLAN. By default, IP multicast traffic related to other address ranges can only be forwarded within the same VLAN.

Enable source port check on the layer-2 multicast device running IGMP Snooping (Switch B).

- **Configuration Steps**

Step 1: Configure multicast routing on the multicast routing device.

! Globally enable multicast routing and forwarding on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#ip multicast-routing
```

! Configure port Gi 0/1 of Switch A as a router port for connecting multicast source and configure the multicast routing protocol

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if-GigabitEthernet 0/1)#no switchport
SwitchA(config-if-GigabitEthernet 0/1)#ip address 10.1.1.2 255.255.255.0
SwitchA(config-if-GigabitEthernet 0/1)#ip pim dense-mode
SwitchA(config-if-GigabitEthernet 0/1)#exit
```

! On Switch A, configure the SVI of VLAN 10, VLAN 20 and VLAN 30, and configure multicast routing protocol on SVI.

```
SwitchA(config)#vlan 10
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 10
SwitchA(config-if-VLAN 10)#ip address 192.168.1.1 255.255.255.0
SwitchA(config-if-VLAN 10)#ip pim dense-mode
SwitchA(config-if-VLAN 10)#exit
SwitchA(config)#vlan 20
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 20
SwitchA(config-if-VLAN 20)#ip address 192.168.2.1 255.255.255.0
SwitchA(config-if-VLAN 20)#ip pim dense-mode
SwitchA(config-if-VLAN 20)#exit
SwitchA(config)#vlan 30
SwitchA(config-vlan)#exit
SwitchA(config)#interface vlan 30
SwitchA(config-if-VLAN 30)#ip address 192.168.3.1 255.255.255.0
SwitchA(config-if-VLAN 30)#ip pim dense-mode
SwitchA(config-if-VLAN 30)#exit
```

! On Switch A, configure port Gi 0/2 as a trunk port for connecting layer-2 multicast device.

```
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if-GigabitEthernet 0/2)#switchport mode trunk
SwitchA(config-if-GigabitEthernet 0/2)#exit
```

Step 2: Create VLAN on layer-2 multicast device and configure user ports of corresponding VLANs

! On Switch B, create VLAN 10, VLAN 20 and VLAN 30; configure port Gi 0/2 to belong to VLAN 10, Gi 0/3 to belong to VLAN 20, and Gi 0/4 to belong to VLAN 30.

```
SwitchB#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchB(config)#interface gigabitEthernet 0/2
SwitchB(config-if-GigabitEthernet 0/2)#switchport access vlan 10
SwitchB(config-if-GigabitEthernet 0/2)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if-GigabitEthernet 0/3)#switchport access vlan 20
SwitchB(config-if-GigabitEthernet 0/3)#exit
SwitchB(config)#interface gigabitEthernet 0/4
SwitchB(config-if-GigabitEthernet 0/4)#switchport access vlan 30
SwitchB(config-if-GigabitEthernet 0/4)#exit
```

! Configure port Gi 0/1 as a trunk port.

```
SwitchB(config)#interface gigabitEthernet 0/1
SwitchB(config-if-GigabitEthernet 0/1)#switchport mode trunk
SwitchB(config-if-GigabitEthernet 0/1)#exit
```

Step 3: Enable IGMP Snooping on layer-2 multicast device and configure router port.

! On Switch B, globally configure IGMP Snooping to operate in IVGL-SVGL mode and configure Gi 0/1 as the router port of VLAN 10, VLAN 20 and VLAN 30.

```
SwitchB(config)#ip igmp snooping ivgl-svgl
SwitchB(config)#ip igmp snooping vlan 10 mrouter interface gigabitEthernet 0/1
SwitchB(config)#ip igmp snooping vlan 20 mrouter interface gigabitEthernet 0/1
SwitchB(config)#ip igmp snooping vlan 30 mrouter interface gigabitEthernet 0/1
```

Step 4: Configure Share VLAN on layer-2 multicast device and specify the multicast address range.

! On Switch B, specify VLAN 10 as the Share VLAN.

```
SwitchB(config)#ip igmp snooping svgl vlan 10
```

! On Switch B, configure IGMP Profile 1 to permit the IP multicast address range of 224.1.1.1-226.1.1.1 and associate SVGL mode.

```
SwitchB(config)#ip igmp profile 1
SwitchB<config-profile>#permit
SwitchB<config-profile>#range 224.1.1.1 226.1.1.1
SwitchB<config-profile>#exit
SwitchB(config)#ip igmp snooping svgl profile 1
Step 5: Configure source port check on layer-2 multicast device.
SwitchB(config)#ip igmp snooping source-check port
```

- **Verification**

Step 1: Display device configurations

! Configurations of Switch A

```
SwitchA#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
ip multicast-routing
!
interface GigabitEthernet 0/1
 no switchport
```

```
 ip pim dense-mode
 no ip proxy-arp
 ip address 10.1.1.2 255.255.255.0
!
interface GigabitEthernet 0/2
 switchport mode trunk
!
interface VLAN 10
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.1.1 255.255.255.0
!
interface VLAN 20
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.2.1 255.255.255.0
!
interface VLAN 30
 ip pim dense-mode
 no ip proxy-arp
 ip address 192.168.3.1 255.255.255.0
```

! Configurations of Switch B

```
SwitchB#show running-config
!
vlan 10
!
vlan 20
!
vlan 30
!
interface GigabitEthernet 0/1
 switchport mode trunk
!
interface GigabitEthernet 0/2
 switchport access vlan 10
!
interface GigabitEthernet 0/3
 switchport access vlan 20
!
interface GigabitEthernet 0/4
 switchport access vlan 30
!
ip igmp profile 1
permit
range 224.1.1.1 226.1.1.1
ip igmp snooping ivgl-svgl
ip igmp snooping svgl vlan 10
ip igmp snooping svgl profile 1
ip igmp snooping source-check port
ip igmp snooping vlan 10 mrouter interface GigabitEthernet 0/1
ip igmp snooping vlan 20 mrouter interface GigabitEthernet 0/1
ip igmp snooping vlan 30 mrouter interface GigabitEthernet 0/1
```

Step 2: Display the IGMP Snooping configurations of Switch B

```
SwitchB#show ip igmp snooping
IGMP Snooping running mode: IVGL_SVGL
SVGL vlan: 10
SVGL profile number: 1
Source port check: Enable
Source ip check: Disable
IGMP Fast-Leave: Disable
IGMP Report suppress: Disable
IGMP Globle Querier: Disable
Dynamic Mroute Aging Time : 30000(Seconds)

vlan 1
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 10
-------------
IGMP Snooping state: Enabled
```

```
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 20
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable

vlan 30
-------------
IGMP Snooping state: Enabled
Multicast router learning mode: pim-dvmrp
IGMPv2 immediate leave: Disabled
IGMP VLAN querier: Disable
```

Step 3: Display router port configuration of Switch B

```
SwitchB#show ip igmp snooping mrouter
Multicast Switching Mroute Port
  D: DYNAMIC
  S: STATIC
(*, *, 10):
  VLAN(10)  1 MROUTES:
    GigabitEthernet 0/1(S)

(*, *, 20):
  VLAN(20)  1 MROUTES:
    GigabitEthernet 0/1(S)

(*, *, 30):
  VLAN(30)  1 MROUTES:
    GigabitEthernet 0/1(S)
```

Step 4: Send IP multicast traffic with group address being 224.1.1.1 through the Source, and request multicast traffic on port Gi 0/3 of Switch B (belonging to VLAN 20 and IP address being 192.168.2.3). Display the group members of Switch A and CDA table of Switch B:

! Switch A

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address  Interface Uptime  Expires   Last Reporter
224.1.1.1       VLAN 10 00:00:16  00:04:04  192.168.2.3
```

! Switch B

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,224.1.1.1, 20):
  VLAN(1) 2 OPORTS:
    GigabitEthernet 0/3(D)
    GigabitEthernet 0/1(M)
```

! From the above information, we can learn that the group address range of IP multicast traffic requested by port Gi 0/3 is 224.1.1.1-226.1.1.1, and the traffic is forwarded through Share VLAN 10.

Step 5: Send IP multicast traffic with group address being 228.1.1.1 through the Source, and request multicast traffic on port Gi 0/3 of Switch B (belonging to VLAN 20 and IP address being 192.168.2.3). Display the group members of Switch A and CDA table of Switch B:

! Switch A

```
SwitchA#show ip igmp groups
IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
228.1.1.1       VLAN 20  00:00:14 00:04:06  192.168.2.3
```

! Switch B

```
SwitchB#show ip igmp snooping gda-table
Multicast Switching Cache Table
  D: DYNAMIC
  S: STATIC
  M: MROUTE
(*,228.1.1.1, 20):
  VLAN(1) 2 OPORTS:
    GigabitEthernet 0/3(D)
    GigabitEthernet 0/1(M)
```

! From the above information, we can learn that the group address range of IP multicast traffic requested by port Gi 0/3 is outside 224.1.1.1-226.1.1.1, and the traffic is forwarded on VLAN 20.

9 MLD Snooping Configuration

9.1 Understanding MLD Snooping

9.1.1 MLD Snooping Overview

MLD Snooping is the short form of Multicast Listener Discovery Snooping. It is designed to manage and control the transmission of IPv6 multicast stream on layer 2.

By running the MLD Snooping equipment and analyzing the MLD message received, mapping relationship is established for port and MAC multicasting address, and such relationship provides a basis for the transmission of IPv6 multicast data on layer 2. When the MLD Snooping is not running, IPv6 multicast data message is broadcast on layer 2; while after the switch places MLD Snooping into operation, the known multicast data message of IPv6 multicast group will not be broadcast on layer 2, but be exchanged to specified receiver(s) on layer 2.

9.1.2 Basic Concepts of MLD Snooping

9.1.2.1 Understanding two types of MLD Snooping ports

As shown in Figure 1, Router is connected with multicast source and with the switch to run MLD Snooping, host A and host C become the hosts (or multicast listener) of receiver.

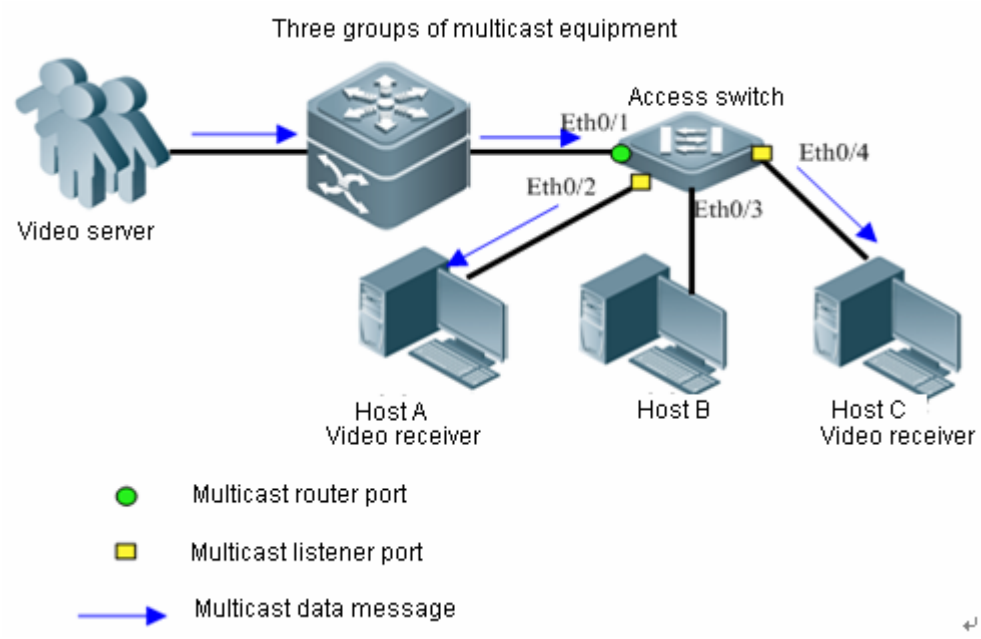


Figure 1 Two types of MLD Snooping ports

Multicast Router Port: a multicast device of the switch to connect layer 3, e.g., Eth 0 / 1 port;

Member Port: the short form of the IPv6 multicast group member port, also called Listener Port. For example, the Access Switch Eth0/2、Eth0/3 and Eth0/4 port.

9.1.2.2 Understanding MLD Profiles

MLD Profiles are actually some group filters, which can define a series of multicast address ranges, and permit or deny the access of those multicast addresses, providing usage for different functions of the following "multicast address ranges for SVGL mode application", "multicast data area to be filtered by router port", "MLD Filtering range", etc.

9.1.2.3 Understanding different kinds of working modes of MLD Snooping

DISABLE mode: Under this mode, MLD Snooping is out of function, i.e., layer 2 multicast equipment does not "snoop" the MLD message between hosts and router, and multicast frames are broadcast in VLAN.

IVGL (Independent VLAN Group Learn) working mode: Under this mode, multicast stream among all VLANs is inter-independent. A host can only request multicast stream from the router port in the same VLAN where the host is located; switch can only transmit the multicast data flow being received from any VLAN to listener ports in the same VLAN.

SVGL (Shared VLAN Group Learn) working mode: Under this mode, hosts of each VLAN share a multicast stream and may request for multicast stream across the VLAN. When specifying a shared VLAN, only the multicast data flow of the VLAN may transmit to other hosts across the VLAN. So long as multicast data flow belongs to Shared VLAN, they can be transmitted to the listener ports of this multicast address, even if some listener ports do not belong to Shared VLAN. Under SVGL mode, it is necessary to use MLD Profile to allocate a number of multicast address ranges to SVGL, within such ranges the listener ports of the multicast forwarding-table may transmit across VLAN. Under default condition, all

class ranges are not within the application area of SVGL, and all multicast stream will be discarded.

The two modes of IVGL and SVGL may coexist, you may allocate with MLD Profile a number of multicast addresses ranges to SVGL, within such ranges the listener ports of the multicast forwarding-table may transmit across VLAN. However, the listener ports of the multicast forwarding-tables within other multicast address ranges must belong to the same VLAN.

9.1.2.4 Understanding source port check

Some of the layer 2 multicast equipments newly launched by DES-7200 provide support to check MLD Snooping source port, thus enhancing network security.

MLD Snooping source port check means strict limitation of porting of MLD multicast stream. When MLD Snooping source port check is disabled, multicast stream incoming from any port is legal and can be transmitted to registered listener port(s) according to MLD Snooping forwarding-table by layer 2 multicast equipment. When MLD Snooping source port check is enabled, only multicast stream incoming from router port is legal and can be transmitted to registered port(s) by layer 2 multicast equipment; while multicast stream incoming from non-router port is considered illegal and will be discarded.

9.1.3 Working Principle of MLD Snooping

The switch that runs MLD Snooping processes different MLD messages in the following ways:

1. MLD QUERY

Layer 3 multicast equipments regularly send group-general query message to all hosts and routers (address: FF 02::1) within local network segment to find out which listeners of IPv 6 multicast group exist in this local network segment. A switch transmits MLD group-general query message being received to all other ports except receive port within VLAN and process the receive port in the following ways:

If the port is already included in the list of router ports, its aging timer should be reset.

If the port is not included in the list of router ports, it should be added to the list of router ports and its aging timer should be enabled.

Whenever receiving MLD group-general query message, layer 2 multicast equipment will update respective aging timers of all listener ports and demote the timer to configured MLD query-max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. Layer 2 multicast equipment will delete the port from MLD Snooping forwarding-table.

Whenever receiving MLD group-specific query message, layer 2 multicast equipment will update aging timers of all listener ports in the specific group, and demote the timer to configured MLD query-max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. Layer 2 multicast equipment will delete the port from MLD Snooping forwarding-table.

When receiving MLD group-specific source query message, the aforesaid two kinds of timers will not be updated.

2. MLD REPORT

A host will send MLD membership report to MLD queriers under following conditions:

When receiving MLD (group-general or group-specific) query message, the listener hosts of IPv6 multicast group will respond with MLD membership report message.

When joining certain IPv6 multicast group, a host will actively send MLD membership report message to MLD queriers to announce its joining in this IPv 6 multicast group.

A switch transmits through all routers in VLAN the MLD membership report message being received, resolve the IPv6 multicast group addresses which hosts will join, and process the receive port in the following ways:

If the forwarding-table corresponding to this IPv6 multicast group does not exist, a forwarding-table should be created. And the port should be added as a dynamic listener port to the list of outgoing ports and its aging timer should be enabled.

If the forwarding-table corresponding to this IPv6 multicast group already exists, but the list of its outgoing ports does not include this port, the port should be added as a dynamic listener port to the list of outgoing ports and its aging timer should be enabled.

If the forwarding-table corresponding to this IPv6 multicast group already exists, and the list of its outgoing ports includes this dynamic listener port, then its aging timer should be reset.

3. MLD LEAVE

When leaving IPv6 multicast group, a host will send MLD leave message to notify the multicast router that it has left certain IPv6 multicast group. A switch will directly forward to router port the MLD leave message it receives from certain dynamic listener port. When the fast–leave function is enabled, the equipment will directly remove relevant ports from the list of ports that transmit corresponding group records.

9.1.4 Protocol Specification

Relevant Protocol specification:

RFC4541

9.2 MLD Snooping Configuration Task

9.2.1 Default Configuration

The following table is used to describe the default configuration of MLD Snooping.

Function characteristics	Default value
Global MLD Snooping switch	Disabled
VLAN-based MLD Snooping switch	Enabled
Aging interval of router ports	300s
Max-response-time for MLD query	10s
Function as a dynamic learn router port	Disabled
The function of fast–leave from multicast listener ports	Disabled

The function of restraining MLD report	Disabled
The function of source port check	Disabled
Port-based filtration of unicast group of specific multicast	Disabled
Number of port-based max-restriction multicast group	1024

9.2.2 Enable Global MLD Snooping

It is necessary to specify the working mode of MLD Snooping when enabled MLD Snooping is set as default. You may assign one of the three modes of IVGL, SVGL and IVGL-SVGL (coexist).

Caution

After enabling the layer2 multicasting on the Private VLAN and Super VLAN, if the multicast source exists in the Sub-VLAN, one more route entry is needed to be duplicated and the ingress is the Sub-VLAN in which the multicast streams enter as the ingress validity check is required when multicast forwarding, resulting in occupying one more multicast hardware entry with 1 less multicast capacity.

9.2.2.1 Configuring IVGL Mode

To enable the MLD Snooping and configure the IVGL mode, run the following commands:

Command	Function
DES-7200(config)# **ipv6 mld snooping ivgl**	Enable the MLD Snooping and configure the IVGL mode. By default, the MLD Snooping is disabled.
DES-7200(config)# **exit**	Return to the privilege mode.
DES-7200# **show ipv6 mld snooping**	Verify the configurations.

The following example shows how to enable the MLD Snooping and configure the IVGL mode:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping ivgl
DES-7200(config)# exit
DES-7200# show ipv6 mld snooping
MLD-snooping mode        :IVGL
SVGL VLAN-ID             :1
SVGL profile number      :0
Source check port        :Disable
Query Max Response Time   :10 (Seconds)
```

9.2.2.2 Configuring SVGL Mode

To enable the MLD Snooping and configure the SVGL mode, run the following commands:

Command	Function
DES-7200(config)# **ipv6 mld snooping svgl**	Enable the MLD Snooping and configure the SVGL mode. By default, the MLD Snooping is disabled.

DES-7200(config)# **exit**	Return to the privilege mode.
DES-7200# **show ipv6 mld snooping**	Verify the configurations.

The following example shows how to enable the MLD Snooping and configure the SVGL mode:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping svgl
DES-7200(config)# exit
DES-7200# show ipv6 mld snooping
MLD-snooping mode        :SVGL
SVGL VLAN-ID             :1
SVGL profile number      :0
Source check port        :Disable
Query Max Response Time   :10 (Seconds)
```

Caution

When configuring the mode as SVGL mode, a profile must be related to assign multicast address range for SVGL mode application, otherwise, the default application of SVGL will not take effect. For the detailed configuration, please refer to the section of *Configuring the multicast address range for SVGL mode application*.

MLD SNOPING SVGL mode and IPV4/V6 layer 3 multicast cannot coexist.

9.2.2.3 Configuring IVGL-SVGL Mode

To enable the MLD Snooping and configure the IVGL-SVGL mode, run the following commands:

Command	Function
DES-7200(config)# **ipv6 mld snooping ivgl-svgl**	Enable the MLD Snooping and configure the IVGL-SVGL mode. By default, the MLD Snooping is disabled.
DES-7200(config)# **exit**	Return to the privilege mode.
DES-7200# **show ipv6 mld snooping**	Verify the configurations.

The following example shows how to enable the MLD Snooping and configure the IVGL-SVGL mode:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping ivgl-svgl
DES-7200(config)# exit
DES-7200# show ipv6 mld snooping
MLD-snooping mode        :IVGL-SVGL
SVGL VLAN-ID             :1
SVGL profile number      :0
Source check port        :Disable
Query Max Response Time   :10 (Seconds)
```

Caution

When configuring the mode as IVGL-SVGL mode, a profile must be related to assign multicast address range for SVGL mode application, otherwise, the default application of SVGL will not take effect. During configuring, please refer to the following section of "multicast address range applied in configuring SVGL mode".

MLD SNOPING IVGL-SVGL mode and IPV4/V6 layer 3 multicast cannot coexist.

9.2.3 Disable Global MLD Snooping

To disable the MLD Snooping function, run the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **no ipv6 mld snooping**	Disable the MLD Snooping function. By default, the MLD Snooping is disabled.
DES-7200(config)# **exit**	Return to the privilege mode.
DES-7200# **show ipv6 mld snooping**	Verify the configurations.

The following example shows how to disable the MLD Snooping function:

```
DES-7200# configure terminal
DES-7200(config)# no ipv6 mld snooping
DES-7200(config)# exit
DES-7200# show ipv6 mld snooping
MLD-snooping mode        :DISABLE
SVGL VLAN-ID             :1
SVGL profile number      :0
Source check port        :Disable
Query Max Response Time   :10 (Seconds)
```

9.2.4 Disable VLAN-based MLD Snooping

To disable the VLAN-based MLD Snooping function, run the following commands in the vlan configuration mode:

Command	Function
DES-7200(config-vlan)# **no ipv6 mld snooping**	Disable the VLAN-based MLD Snooping function. By default, with the global MLD Snooping enabled, the MLD Snooping function in all VLANs are enabled.
DES-7200(config-vlan)# **end**	Return to the privilege mode.
DES-7200# **show ipv6 mld snooping**	Verify the configurations.

The following example shows how to disable the MLD Snooping in vlan 2:

```
DES-7200# configure terminal
DES-7200(config)# vlan 2
DES-7200(config-vlan)# no ipv6 mld snooping
DES-7200(config-vlan)# end
DES-7200# show ipv6 mld snooping
MLD-snooping mode        :IVGL
SVGL VLAN-ID             :1
SVGL profile number      :0
Source check port        :Disable
Query Max Response Time   :10 (Seconds)
DISABLE VLAN             :2
```

Note

After enabling MLD Snooping within VLAN, users must also enable IGMP Snooping within this VLAN if they make application of IPv 4 multicast within this VLAN.

9.2.5 Configuring the Aging Timer for the Dynamic Route Port

If the dynamic route port has not received MLD group-general query message or IPv6 PIM Hello message before its aging time is out, the switch will delete the port from the list of router ports.

To configure the aging timer for the dynamic route port, run the following command:

Command	Function
DES-7200(config)# **ipv6 mld snooping dyn-mr-aging-time** *time*	Configure the aging timer for dynamic route port *time*: the valid range is 1-3600, and the default value is 300s.

Use the **no IPv6 MLD Snooping dyn-mr-aging-time** command to restore the aging time for the dynamic route port to the default value.

The following example shows how to set the aging time for the dynamic route port as 100s:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping dyn-mr-aging-time 100
```

9.2.6 Configuring Max-response-time for MLD Query Message

After receiving MLD group-general query message, layer-2 multicast equipment will enable respective aging timers of all listener ports and timer is set at max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. And layer-2 multicast equipment will delete the port from MLD Snooping forwarding-table.

After receiving MLD group-specific query message, layer-2 multicast equipment will enable respective aging timers of all listener ports in the specific group and timer is set at max-response-time. When the timer value is reduced to "0", it is considered that there is no longer any listener of the port receiving multicast stream. And layer-2 multicast equipment will delete the port from MLD Snooping forwarding-table.

As for MLD group-specific source query message, timers will not be updated.

Command	Function
DES-7200(config)# **ipv6 mld snooping query-max-response-time** *time*	Configure MLD group-general and group-specific query max-response-time within the range of 1-65535, and the default value is 10s.

The following example shows how to set the max-response-time for the MLD query message as 15s:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping query-max-response-time 15
```

9.2.7 Configuring Router port

By default, you may enable the dynamic router port learning in a VLAN for the layer-2 multicast device. Use the **no** form of this command to disable dynamic learning and clear all dynamically-learned router port.

You may also configure the switch port as a static router port so that all IPv6 multicast data received by the switch may be transmitted through this port.

To configure the router port, run the following command:

Command	Function
DES-7200(config)# **ipv6 mld snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn** }	Set the interface as static router port, by default, the port is not a static router port; set the dynamically-learned router port on the layer 2 multicast device, by default, the dynamic learning is allowed.

The following example shows how to set the Ethernet interface 0/1 as the router port and configure the auto-learning for the router port:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitEthernet
0/1
DES-7200(config)# ipv6 mld snooping vlan 1 mrouter learn
DES-7200(config)# end
DES-7200# show ipv6 mld snooping mrouter
VLAN    Interface        State       MLD profile
----    ---------        ------      -------------
1   GigabitEthernet 0/1   static          0
1   GigabitEthernet 0/2   dynamic         0
DES-7200# show ipv6 mld snooping mrouter learn
VLAN   learn method
----   ------------------
1      pim
```

9.2.8 Configuring Static Listener Port

Use this command to set a port joins to the IPv6 multicast group statically to become a static listener port, if the host that connects to the port needs to receive the IPv6 multicast data sent to an IPv6 multicast group in a fixed manner.

To configure the MLD Snooping static listener port, run the following commands:

Command	Function
DES-7200(config)# **ipv6 mld snooping ivgl**	Enable and set MLD Snooping to IVGL mode.
DES-7200(config)# **ipv6 mld snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id*	Statically configure a port to receive certain multicast stream. • *vlan-id*: VID of multicast stream • *ip-addr*: Multicast address • interface-id:Port number

Use the **no ipv6 mld snooping vlan** *vlan-id* **static** *ip-addr* **interface** *interface-id* command to delete the static configuration of the multicast listeners.

The following example shows how to set the MLD Snooping static listener port:

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping vlan 1 static FF88::1234 interface
GigabitEthernet 0/7
DES-7200(config)# end
DES-7200# show ipv6 mld snooping gda
Abbr: M - mrouter
      D - dynamic
      S - static
VLAN  Address              Listener ports
---- --------------   ----------------------------
1    FF88::1234       GigabitEthernet 0/7(S)
```

9.2.9 Configuring Port Fast–leave

Port Fast–leave means that when receiving from a port the MLD leave message

sent from a host for leaving certain IPv 6 multicast group, a switch will directly delete the port from the list of outgoing ports in the corresponding forwarding-table. If there is only one receiver connecting underneath the port on the switch, you may enable Port Fast–leave to save band width and resource.

To configure the port fast–leave of MLD Snooping, run the following commands:

Command	Function
DES-7200(config)# **ipv6 mld snooping fast-leave enable**	Enable the fast-leave function for the layer 2 multicast device, by default, this function is disabled.

Use the **no ipv6 mld snooping fast–leave enable** command to disable the port fast-leave function.

9.2.10 Configuring the Response Suppression for MLD Snooping Membership Report Message

When receiving MLD membership report message from one IPv multicast listener, layer-2 equipment will forward the message to directly connected layer 3 equipment. Thus, when there exist in layer-2 equipment a number of listeners that belong to one IPv 6 multicast group, directly connected layer-3 equipment will receive the same MLD membership report message sent by these listeners.

After enabling MLD membership report message suppression function, layer-2 equipment will only forward to layer-3 equipment the first MLD membership report message of one IPv 6 multicast group it receives within one query interval, instead of keeping on forwarding to layer-3 equipment other MLD membership report message from the same multicast group. In this way, message quantity will be reduced in the network.

Run the following command to enable the response suppression for the layer-2 multicast device:

Command	Function
DES-7200(config)# **ipv6 mld snooping suppression enable**	Enable he response suppression for the layer-2 multicast device, by default, this function is disabled.

Use the **no ipv6 mld snooping suppression enable** command to disable the suppression function.

9.2.11 Configuring Source Port Check

To configure the source port check function, run the following command:

Command	Function
DES-7200(config)# **ipv6 mld snooping source-check port**	Enable the source port check.

Use the **no ipv6 mld snooping source-check port** command to disable the source port check function.

9.2.12 Configuring MLD Profiles

MLD Profiles are actually a number of group filters to provide support for following functions of "multicast address range for SVGL mode application", "multicast data area to be filtered by router port", "MLD Filtering range", etc.

To configure the MLD profile, run the following command:

Command	Function
DES-7200(config)# **ipv6 mld profile** *profile-number*	Enter the MLD Profile mode and assign for identification a number from 1 to 1024. By default, no profile is configured.
DES-7200 (config-profile)# **permit** | **deny**	(Optional) Permit or deny the range of the multicast address, deny by default. It indicates that the range of multicast address and other multicast address will be permitted or denied. By default, all groups are denied.
DES-7200(config-profile)# **range** *low-address high_address*	Add the multicast address range, which can be both a single IPv6 group address(low IPv6 group address) and a group address zone(high IPv6 group address). Meanwhile, multiple ranges may be configured.
DES-7200(config)# **end**	Return to the privilege mode.

Use the **no ipv6 mld profile** *profile_number* command to delete an MLD profile. Use the **no range** *low-address high_address* command to delete the profile range.

The following example shows how to configure the profile:

```
DES-7200(config)# ipv6 mld profile 1
DES-7200(config-profile)# permit
DES-7200(config-profile)# range ff77::1 ff77::100
DES-7200(config-profile)# range ff88::123
DES-7200(config-profile)# end
DES-7200# show ipv6 mld profile 1
MLD Profile 1
permit
range ff77::1 ff77::100
range ff88::123
```

According to this configuration, the rule for this MLD profile is to permit the multicast addresses from ff77::1 to ff77::100 as well as ff88::123, while other multicast addresses are all denied.

9.2.13 Configuring the Multicast Address Range for SVGL Mode Application

A profile shall be associated with the SVGL with the MLD Snooping working mode(SVGL mode or IVGL-SVGL mode) configured, to specify which ranges of group addresses may use SVGL mode, i.e., the listener ports of the multicast forwarding-table may transmit across VLAN. However, the listener ports of the multicast forwarding-tables within other multicast address ranges must belong to the same VLAN. By default, no profile associated is considered that no multicast group can apply the SVGL mode.

Command	Function
DES-7200(config)# **ipv6 mld profile** *1*	Enter the MLD Profile mode and assign for identification a number from 1 to 1024. By default, no profile is configured.
DES-7200(config)# **ipv6 mld snooping ivgl-svgl**	Configure the IVGL-SVGL mode

DES-7200(config)# **ipv6 mld snooping svgl profile** *1*	Associate the profile 1with the SVGL mode.
DES-7200(config)# **end**	Return to the privilege mode.

The following example shows how to configure the multicast address range for SVGL Mode application

```
DES-7200# configure terminal
DES-7200(config)# ipv6 mld snooping ivgl-svgl
DES-7200(config)# ipv6 mld snooping svgl profile 1
DES-7200(config)# end
DES-7200# show ipv6 mld snooping
MLD-snooping mode        :IVGL
SVGL VLAN-ID             : 1
SVGL profile number      : 1
Source check port        :Disable
Query Max Response Time   : 10 (Seconds)
```

9.2.14 Configuring MLD Filtering

Under certain circumstances, you may need to control certain port so that it can only transmit multicast data flow within a number of specific ranges and what max groups are allowed to join under the port. MLD Filtering can meet this demand.

You may apply certain MLD Profile under a port. When the port receives MLD Report message, layer 2 multicast equipment will find out whether the multicast address for this port to join is permitted by MLD Profile. If so, joining is permitted before later processing.

You may also configure the max group number that are permitted to join one port. When the max group number is exceeded, layer 2 multicast equipment will no longer receive and process MLD report message.

To configure the MLD Filtering, run the following commands:

Command	Function
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **ipv6 mld snooping filter** *profile-number*	(Optional) Apply the profile to this port. *profile-number:* the valid range is 1-1024. By default, no profile is associated with a port.
DES-7200(config-if)# **ipv6 mld snooping max-groups** *number*	(Optional) Permit a max number of groups to join this port dynamically. *number:* the valid range is 0-1024 By default, the value is 1024.

The following example shows how to configure the MLD Filtering:

```
DES-7200# configure terminal
DES-7200(config)# interface fastEthernet 0/1
DES-7200(config-if)# ipv6 mld snooping filter 1
DES-7200(config-if)# ipv6 mld snooping max-groups 1000
DES-7200 (config-if)#end
DES-7200 #show ipv6 mld snooping interface fastEthernet 0/1
Interface            Filter profile number       max-group
---------------      ---------------------       ---------
FastEthernet 0/1            1                        1000
```

9.3 Monitor and Maintain MLD Snooping State and Listener Information

9.3.1 Viewing Current Mode of MLD Snooping

To view the current working mode and global configuration of MLD Snooping, run the following command:

Command	Function
DES-7200# **show ipv6 mld snooping**	View the current working mode and global configuration of MLD Snooping

The following example shows the MLD Snooping configurations:

```
DES-7200# show ipv6 mld snooping
MLD-snooping mode      : IVGL
SVGL VLAN-ID           : 1
SVGL profile number    : 0
Source check port      : Disabled
Query max Response time : 10(Seconds)
```

9.3.2 Viewing and Clearing MLD Snooping Statistics

To view and clear the MLD Snooping statistics, run the following commands:

Command	Function
DES-7200# **show ipv6 mld snooping statistics** [VLAN *VLAN-ID*]	View the MLD Snooping statistics.
DES-7200# **clear ipv6 mld snooping statistics**	Clear the MLD Snooping statistics.

The following example shows the MLD Snooping statistics:

```
DES-7200# show ipv6 mld snooping statistics
GROUP    Interface    Last report       Last leave     Last
                         time          time         reporter
--------------- ------------ -------------  -------------   -
FF88::1 VL1:Gi4/2   0d:0h:0m:7s     ----    2003::1111
                        Report pkts: 1          Leave pkts: 0
```

9.3.3 Viewing Router port Information

To view and clear the MLD Snooping router port information, run the following command:

Command	Function
DES-7200# **show ipv6 mld snooping mrouter**	View the MLD Snooping router port information.

The following example shows the MLD Snooping router port information:

```
DES-7200# show ipv6 mld snooping mrouter
VLAN    Interface       State     MLD profile number
----     --------         -------     -------------------
1   GigabitEthernet 0/7   static       1
1   GigabitEthernet 0/12   dynamic       0
```

9.3.4 Viewing the Forwarding-table

To view the forwarding rule of each port in a multicast group, i.e., to view GDA (Group Destination Address) table, run the following command:

Command	Function
DES-7200# **show ipv6 mld snooping gda-table**	View the forwarding rule of each port in a multicast group.

The following example shows each multicast group information in the GDA table and the information of all listener ports of a multicast group:

```
DES-7200# show ipv6 mld snooping gda-table
Abbr: M - mrouter
     D - dynamic
     S - static
VLAN  Address            Listener ports
-------------------------------------------------------------
1      FF88::1         GigabitEthernet 0/7(S)
```

9.3.5 Clearing Dynamic Forwarding-table Information

To clear GDA(Group Destination Address) information from dynamic forwarding-table, run the following command:

Command	Function
DES-7200# **clear ipv6 mld snooping gda-table**	Clear the group information learned in a dynamic way from forwarding-table.

9.3.6 Viewing Source Port Check Status

To view current status of MLD Snooping source port check, run the following command:

Command	Function
DES-7200# **show ipv6 mld snooping**	View the current working mode and global configuration of MLD Snooping.

The following example shows the source port check status:

```
DES-7200# show ipv6 mld snooping
MLD-snooping mode        :IVGL
SVGL VLAN-ID             :1
SVGL profile number      :0
Source check port        :Disable
Query Max Response Time   :10 (Seconds)
```

9.3.7 Viewing MLD Profile

To view view MLD Snooping Profile information, run the following command:

Command	Function
DES-7200# **show ipv6 mld profile** *profile-number*	View the MLD Snooping Profile information.

The following example shows the MLD Snooping Profile information:

```
DES-7200# show ipv6 mld profile 1
MLD Profile 1
permit
range FF77::1 FF77::100
```

```
range FF88::123
```

9.4 Configuring Other Restrictions for MLD Snooping

MLD Snooping source port should be checked with Masks, definition of which can be seen the section "Configuring access control list". Address binding , source port check and ACL are applied by sharing Masks, total number of which is decided by different products. Due to limited number of Masks, the three functions may influence each other. Two masks are occupied when enabling Address binding function. It is the same with enabling source port check. Masks available for ACL depend on whether these two functions have been enabled. Suppose 8 masks should be available for ACL under default condition, when enabling Address binding function or source port check, masks available for ACL will decrease by two. If Address binding and source port check are both enabled, the masks available for ACL will be reduced by four and only four remains. On the other way, when ACL is using a number of masks and the remaining masks cannot meet the need of the two applications, the system will display the information of masks resource exhausted when enabling Address binding or source port check. When one of the three functions is not in normal state due to masks limitation, masks occupied for the other two functions may be reduced to return the function to normal. When three functions are all enabled and masks exhausted information is shown after enabling source port check, you may disable Address binding function (delete all address binding) or delete the ACE of ACL that occupies a number of masks, and thus source port check can be normally enabled.

When enabling MLD Snooping or setting router port and source port check has been enabled, source port check may fail because of insufficient masks. Then, the system will show "Source port check applying failed for hardware out of resources". You should release other masks, disable again before enabling source port check.

9.5 Typical Configuration Example of MLD Snooping

- **Networking Requirements**

  A multicast source server, a layer 3 multicast equipment, an access switch, three multicast requesters;

  Layer 3 multicast equipment supports PIM-SMv6 function;

  The access switch supports MLD Snooping functions.

- **Networking Topology**

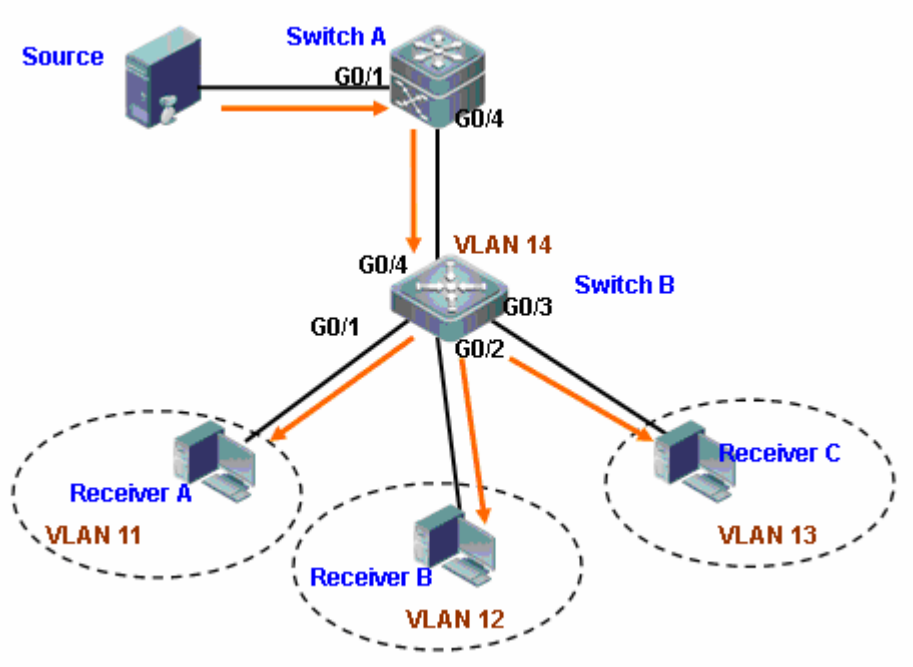


Figure 1 MLD Snooping networking topology

Configuring Steps

Configuring Switch A (layer 3 switch)

Enable layer 3 multicast

```
DES-7200#configure terminal
DES-7200(config)# ipv6 multicast-routing
DES-7200(config)# int vlan 14
DES-7200(config-if)# ipv6 pim sparse-mode
DES-7200(config-if)# ipv6 add 1111:1111::1111/64
DES-7200(config)# int gigabitEthernet 0/1
DES-7200(config-if)# no switch
DES-7200(config-if)# ipv6 pim sparse -mode
DES-7200(config-if)# ipv6 add 1111:2222::1111/64
```

Configuring G0/4 as trunk port and its native vlan as SVGL vlan

```
DES-7200#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/4
DES-7200(config-if)#sw trunk native vlan 14
```

Configuring Switch B (layer 2 switch)

Configuring VLAN

Configuring VLAN11

```
DES-7200#configure terminal
DES-7200(config)# vlan 11
DES-7200(config-vlan)#exit
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if)#switchport access vlan 11
```

Configuring VLAN12

```
DES-7200(config-if)#exit
DES-7200(config)# vlan 12
DES-7200(config-vlan)#exit
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if)#switchport access vlan 12
```

Configuring VLAN13

```
DES-7200(config-if)#exit
DES-7200(config)# vlan 13
DES-7200(config-vlan)#exit
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-if)#switchport access VLAN 13
```

Configuring VLAN14

```
DES-7200(config-if)#exit
DES-7200(config)#VLAN 14
DES-7200(config-VLAN)#exit
DES-7200(config)#interface gigabitEthernet 0/4
DES-7200(config-if)#switchport access VLAN 14
```

Configuring MLD profile

```
DES-7200# configure terminal
DES-7200(config)#IPv6 MLD profile 1
DES-7200<config-profile>#permit
DES-7200<config-profile>#range ff13::  ff13:1111::
DES-7200<config-profile>#end
DES-7200#show IPv6 MLD profile 1
Profile    1
       Permit
       range ff13::,   ff13:1111::
```

Configuring router port

```
DES-7200(config)#IPv6 MLD Snooping VLAN 14 mrouter interface gigabitEthernet
0/4
```

Configuring SVGL working mode

Enabling and setting MLD Snooping to SVGL mode

```
DES-7200#configure terminal
DES-7200(config)#IPv6 MLD Snooping SVGL
```

Configuring SVGL VLAN

```
DES-7200(config)#IPv6 MLD Snooping SVGL VLAN 14
```

Configuring SVGL profile

```
DES-7200(config)#IPv6 MLD Snooping SVGL profile 1
```

Viewing MLD Snooping configuration

```
DES-7200#show IPv6 MLD Snooping
mld-snooping mode       :SVGL
SVGL VLAN-ID            :14
SVGL profile number      :1
Source check port        :Disable
Query Max Response Time   :10 (Seconds)
DES-7200#show run
…
IPv6 MLD profile 1
permit
range ff13:: ff13:1111::
IPv6 MLD Snooping SVGL VLAN 14
IPv6 MLD Snooping SVGL profile 1
IPv6 MLD Snooping SVGL
IPv6 MLD Snooping VLAN 14 mrouter interface GigabitEthernet 0/4
!
```

10 PIM-Snooping Configuration

10.1 PIM Snooping Overview

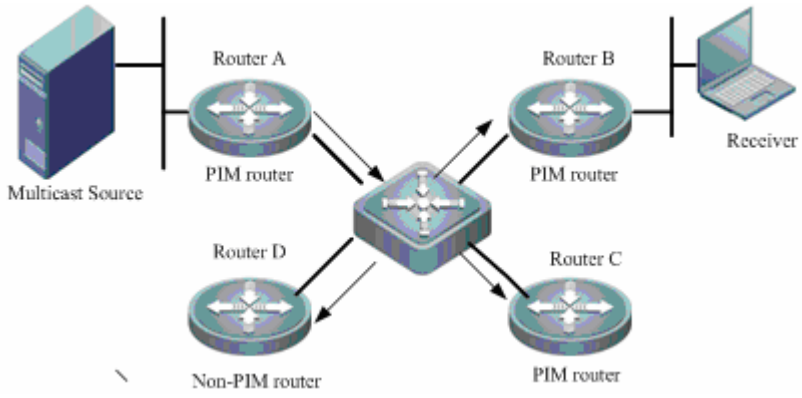
Within the network that the L2 switches connect with several routers, the multicast frames are forwarded in the broadcast form, which easily leads to the multicast flow storm and a waste of network bandwidth.

IGMP Snooping deals with the problem occurs when the connected receiving devices in the VLAN are all hosts and enables the multicast flow to be forwarded only to the port where the registered users are, not influencing other users. However, when the receiving devices in the VLAN in the downstream direction are the routers with PIM protocol enabled, IGMP Snooping fails to regulate the Layer 2 forwarding of the multicast flow. And PIM Snooping deals with the problem of Layer 2 forwarding of the multicast flow for the connected routers in the VLAN with PIM protocol enabled. PIM Snooping must be combined with IGMP Snooping to manage the Layer 2 forwarding of the multicast flow in the VLAN.

The figure below shows the flooding of multicast frames before the PIM snooping is enabled and the restriciton of multicast frames after the PIM snooping is enabled.

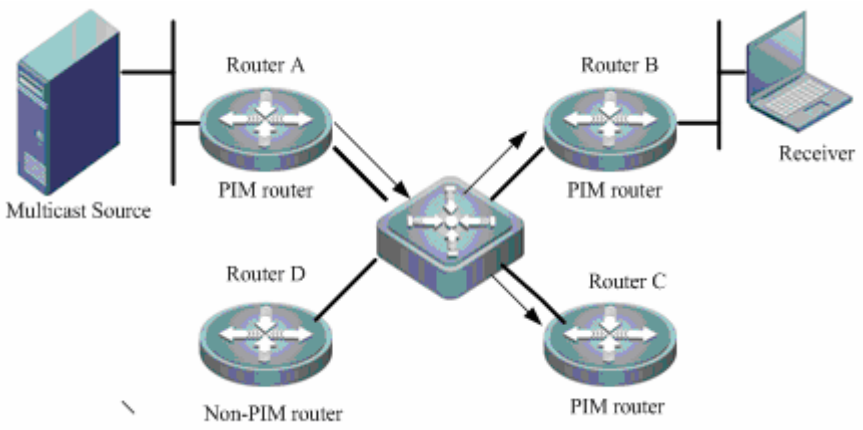
As shown in Figure-1, multicast frames is flooded to all the ports of the switch when the PIM snooping is not enabled.

Figure-1 Multicast flow When the PIM Snooping is not enabled



As shown in the Figure-2, multicst frames flow only to the ports that connect with the multicast routers B and C, but not to the router D.

Figure-2 Multicast flow after the PIM Snooping is enabled



Snooping means “eavesdrop”, from which we can understand the working process easily. When the L2 multicast device “eavesdrops” Hello message from router, it will add the interface to the multicast forwarding table. In a certain time, if the L2 multicast device does not receive Hello message, the interface will be removed from the forwarding table.

10.2 Default PIM Snooping Confiugration

By default, the PIM Snooping is disabled.

10.3 PIM Snooping Configuration Guide and Limit

PIM Snooping applies to PIM-DM and PIM-SM.

PIM Snooping can be enabled or disabled separately on SVI.

The timeout of neighbor information of PIM Snooping is processed based on the hold time of the hello message.

10.4 PIM Snooping Cofiguration Tasks

10.4.1 Enabling the PIM Snooping globally

The PIM Snooping can be enabled in the VLAN after the it is enabled globally.

To enable the PIM snooping globally, execute the following commands:

Command	Function
DES-7200(config)# **ip pim snooping**	Enable the IGMP Snooping IVGL mode.

The following example will show how to enable the PIM Snooping globally and verify the configurations.

```
DES-7200(config)# ip pim snooping
DES-7200(config)# end
DES-7200# show ip pim snooping
Global runtime mode         : Enabled
Global admin mode       : Enabled
DR Flooding status      : Enabled
Number of user enabled VLANs: 0
User enabled VLANs:
```

Caution

The IGMP Snooping must be enabled before enabling PIM Snooping.

The PIM Snooping only deals with the Layer 2 multicast flow management for PIM-SM. If the Layer 3 multicast is enabled with PIM-DM protocol, it is possible that the multicast flow cannot be forwarded normally.

10.4.2 Enabling the PIM Snooping on the interface

The PIM Snooping must be enabled on the SVI interfaces respectively. With the PIM Snooping enabled on the interface, you can snoop the PIM messages, maintain and update the Layer 2 multicast forwarding table on the interface.

To enable the PIM snooping on the interface, execute the following commands:

Command	Function
DES-7200(config)# **interface vlan** *vlan_ID*	Enter the SVI interface configuration mode.
DES-7200(config-if)# **ip pim snooping**	Enable the PIM Snooping on the interface.

The following example will show how to enable the PIM Snooping on the interface and verify the configurations.

```
DES-7200(config)# interface vlan 199
DES-7200(config-if)# ip pim snooping
DES-7200(config-if)# end
DES-7200# show ip pim snooping
Global runtime mode: Enabled
Global admin mode  : Enabled
DR Flooding status: Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 199
```

Caution

When the VLAN and the multicast source are connected, PIM Snooping floods the multicast flow to the interface connected to DR only. If another device in this VLAN becomes the forwarder for the STP creation, PIM Snooping fails to forward the multicast flow.

It is not recommended to enable the PIM Snooping in the VLAN with multicast source.

10.5 Monitoring and Maintaining PIM-Snooping

PIM Snooping offers command **show** to monitor and maintain PIM Snooping. You can view PIM Snooping information such as global configuration, neighboring list and Layer 2 forwarding table by executing command **show.**

Use the following command to view PIM Snooping running status information:

Command	Function
show ip pim snooping	Show global configuration information of PIM Snooping.
show ip pim snooping neighbor	Show PIM Snooping neighbor information.
show ip pim snooping vlan	Show PIM Snooping in a VLAN.

For the detailed usage of the above command, please refer to *PIM-Snooping Command Reference.*

10.6 PIM-Snooping Configuration Examples

- **Configuration requirement**

  As the following figure shows, multicast flow arrives on the interface of L3 switch in VLAN 2. In VLAN 3, only router B configures PIM protocol while router A does not.

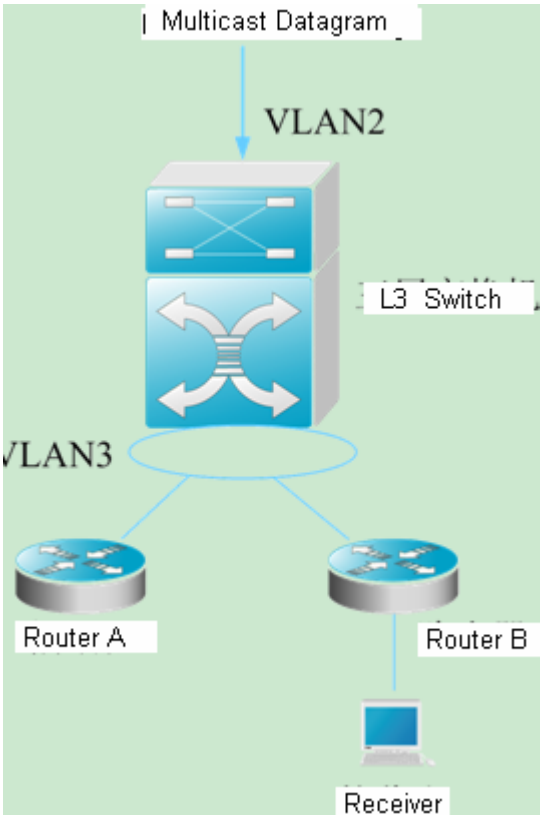


Figure-3 Topology Structure of PIM-Snooping Configuration Example

- **Device configuration**

  The following example explains how to configure PIM Snooping on the switch:

```
DES-7200(config)# ip pim snooping
DES-7200(config)# interface vlan 3
DES-7200(config-if)# ip pim snooping
DES-7200(config-if)# end
```

  You can configure PIM Snooping for L2 multicast device in VLAN 3 according to above steps and view the running status of PIM Snooping by command **show.**

DES-7200

MPLS Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)
Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 MPLS Configuration

Note

The router icon in this chapter refers to the routers and the layer-3 switches with the routing protocol enabled.

1.1 Introduction to MPLS

In the Multiprotocol Label Switching (MPLS), the multiprotocol refers to various network layer protocols supported by an MPLS network, such as IP, IPv6, and IPX, and label switching indicates the addition of labels to packets and the forwarding of packets based on the labels. The MPLS is compatible with multiple link layer technologies including ATM, frame relay, Ethernet, and PPP. The MPLS works at both the connectionless control plane and the connection-oriented data plane and provides connection-oriented attributes to connectionless IP networks. The MPLS technology was first introduced to enhance the forwarding rate of routing devices. With the development of hardware technologies and network processors, this competitive edge has gradually lost its appeal. Due to the innate advantage of combining Layer 2 switching and Layer 3 routing technologies, however, the MPLS still has unprecedented edges over other technologies in terms of virtual private networks (VPNs) and traffic engineering (TE). The MPLS VPN is increasingly favored by carriers to address interconnection problems between companies and to provide various new services. It has already become an important means to provide value-added services on IP networks. At the same time, the MPLS TE technology also turns into a major method to reduce congestion and guarantee QoS on IP networks by managing network traffic. Therefore, the MPLS technology receives more and more attention and the MPLS applications gradually shift to MPLS VPN and TE applications.

Basic Concepts

Label

LDP

MPLS Network

MPLS Forwarding Actions

LSP Setup and Loop Detection

MPLS Applications

1.1.1 Basic Concepts

MPLS node

The nodes enabled with MPLS can identify the MPLS signaling protocol (control protocol), support one or more Layer 3 routing protocols (including static routes), and forward packets based on MPLS labels. Generally speaking, an MPLS node is also capable of forwarding original Layer 3 packets (such as IP packets).

Forwarding Equivalence Class (FEC)

FEC indicates one type of data packets that are handled in equal cost mode during the forwarding, such as data packets that have the same prefix in their destination addresses. The FEC supports different classification methods for different applications. For example, the FEC classifies IP unicast routes based on the address prefixes. That is, one route corresponds to one FEC. All the packets in the same FEC are equally handled on the MPLS network.

Label Switching Router (LSR)

As a core device on an MPLS network, the LSR provides label switching and distribution functions. As specified by RFC 3031 for MPLS system files, the LSR is also an MPLS node that is capable of forwarding original Layer 3 packets (such as IP packets or IPv6 packets). For the MPLS on an IP network, this means that the LSR can also forward normal IP packets.

Label Switching Edge Router (LER)

Located on the edge of an MPLS network, the LER identifies different EFCs for incoming traffic, requests labels for these FECs, and restores the original packets for outgoing traffic by popping out the labels. The LER thus provides traffic classification, label mapping, and label removal functions.

Label Switched Path (LSP)

One FEC data stream is assigned with specific labels on different nodes and transmitted along the nodes according to the switching of assigned labels. The path that the data stream travels is an LSP. It is a collection of several LSRs. In this manner, you can consider the LSP as a tunnel that traverses the MPLS core network.

Next Hop Label Forwarding Entry (NHLFE)

The NHLFE table is used to store the next-hop information about MPLS packets. The NHLFE entries generally cover the following information:

1. Next hop of data packets
2. Link layer encapsulation of data packets to be forwarded
3. Encoding method in the label stack of data packets to be forwarded

4. Operations to the label stack of data packets, including:

   a) Replacing the label of the label stack top with a new label

   b) Popping out the label of the stack top

   c) Adding one or more labels

   d) Replacing the label of the label stack top with a new label and adding one or more new labels

Incoming Label Map (ILM)

The ILM table is a label forwarding table that maps each incoming label to a series of NHLFEs (multiple NHLFEs indicate multiple paths). The ILM is applied when an LSR receives and forwards MPLS packets with labels.

FEC-to-NHLFE (FTN)

Different from ILM, the FTN maps each FEC to a series of NHLFEs (multiple NHLFEs indicate multiple paths). The FTN table is used when an LER receives and forwards packets without labels and is required to encapsulate labels to the packets before forwarding them.

1.1.2 Label

A label is a short identifier with fixed length and of local significance. The label is distributed and transmitted only between two adjacent LSRs. As a result, it is valid only between the two LSRs. One label identifies one FEC. When arriving at the MPLS ingress, packets are classified into different FECs according to certain rules. Based on the FECs, the packets are encapsulated with different labels and then forwarded on the MPLS network based on the labels.

1.1.2.1 Label Structure

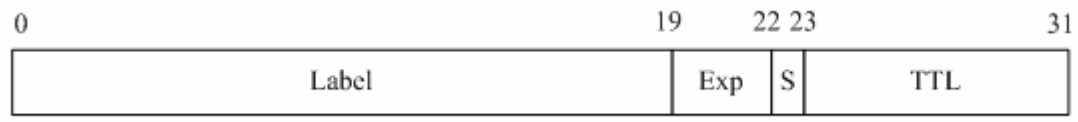


Figure 1 Encoding structure of an MPLS label

As shown in the preceding figure, a label consists of four fields. The following introduces the four fields separately:

- Label field

The label field is used to save the label that is 20 bits long. The label value is an index to the forwarding table of labels. The IETF defines 0 to 15 as reserved labels and predefines the meanings of these label values:

Reserved Label Value	Meaning
0	Indicates the IPv4 explicit null label. According to RFC 3032, the 0 label must be at the stack bottom. This means that the label should be popped out and the packets should then be forwarded according to destination IP addresses. RFC 4182 modifies the description of 0 label in RFC 3032. For the received packets with 0 label, the router directly pops out the label and determines the forwarding action based on the contents after 0 label. If another label follows, the router forwards the packets according to the label; if the packets are IPv4 packets, the router forwards them according to their destination IP addresses.
1	Indicates the router alert label. This label is not allowed at the bottom of the label stack. When receiving packets with the router alert label, the router must send the packets to the local software module for processing. The actual forwarding of the packets must be based on the labels that follow the router alert label. Before the forwarding, however, the router alert label must be added to the label stack again. This option is similar to the Router Alert Option of IP packets. You can use this option to configure the LSRs on each hop to check MPLS packets.
2	Indicates the IPv6 explicit null label. According to RFC 3032, the 2 label must be at the stack bottom. This means that the label should be popped out and the packets should then be forwarded according to destination IP addresses. RFC 4182 modifies the description of 2 label in RFC 3032. For the received packets with 2 label, the router directly pops out the label and determines the forwarding action based on the contents after 2 label. If another label follows, the router forwards the packets according to the label; if the packets are IPv4 packets, the router forwards them according to their destination IP addresses.
3	Indicates the implicit null label. This label can be distributed by the label distribution protocol (LDP) but can never be transmitted in the label stacks of MPLS packets. When an LSR exchanges MPLS packets, the router pops out the label of the stack top rather than replaces the label if the label to be replaced at the stack top is 3. The implicit null label is used in the Penultimate Hop Popping (PHP) function.

4 to 15	These values are reserved by the IETF for future usage.

- Exp field

The Exp field is currently used to store the QoS information about MPLS. This field is 3 bits.

- S mark

The S mark field indicates the stack bottom. It is one bit long. If multiple labels exist, the S bit at the stack bottom is set to 1 and the S bits of other labels are 0. If only one label exists, the S bit is directly set to 1.

- TTL

Short for Time To Live, the TTL field is 8 bits long. It is similar to the TTL value in IP packet headers. When a label is first added to an IP packet, the TTL value can be copied from the TTL field (or HopLimit of IPv6) of the IP packet header. The TTL value of the outer (stack top) label then decreases by one at every label switching. When MPLS runs on ATM links, the label encoding methods are different and no TTL field exists. For the corresponding methods and solutions, refer to RFC 3032.

1.1.2.2 Label Stack

One MPLS packet can have several labels, that is, a label stack. The label that is close to the link layer header is the top label and the label that is next to the IP header is the bottom label. The LSR always exchanges labels based on the top label. When multiple labels exist, each label must be complete and have 32 bits. With the label stack, one MPLS packet can carry multiple layers of labels. In this manner, the MPLS technology can support hierarchical network systems and at the same time, support LSPs.

1.1.2.3 Operation Methods of Labels

There are the following basic label operations on MPLS nodes:

- Push

Insert a label to the link header and network layer header on an ingress LER or add a new label to the stack top of an MPLS packet on an intermediate LSR.

- Pop

Remove the label of packets on the egress LER to restore the IP packets or remove the top label on an intermediate LSR to reduce the layers of a label stack.

- Swap

Replace the top label in the label stack of packets based on the ILM during forwarding.

1.1.3 LDP

As a new network system, MPLS also has its own signaling protocols or "routing protocols". One of the basic concepts in the MPLS system is that two LSRs must reach consensus on the meaning of labels used for traffic transmission. This consensus is realized through a series of processes, that is, the LDP. Through the LDP, one LSR can notify the other LSR of the label binding. The MPLS system architecture does not assume the existence of a single LDP. Some MPLS systems use independent distribution protocols, such as the LDP defined in RFC 3036 by the IETF; other MPLS systems support the distribution of labels by extending existing protocols in piggybacking mode, such as MP-BGP and RSVP. You can choose different LDPs for MPLS networks based on the different application scenarios.

1.1.4 MPLS Network

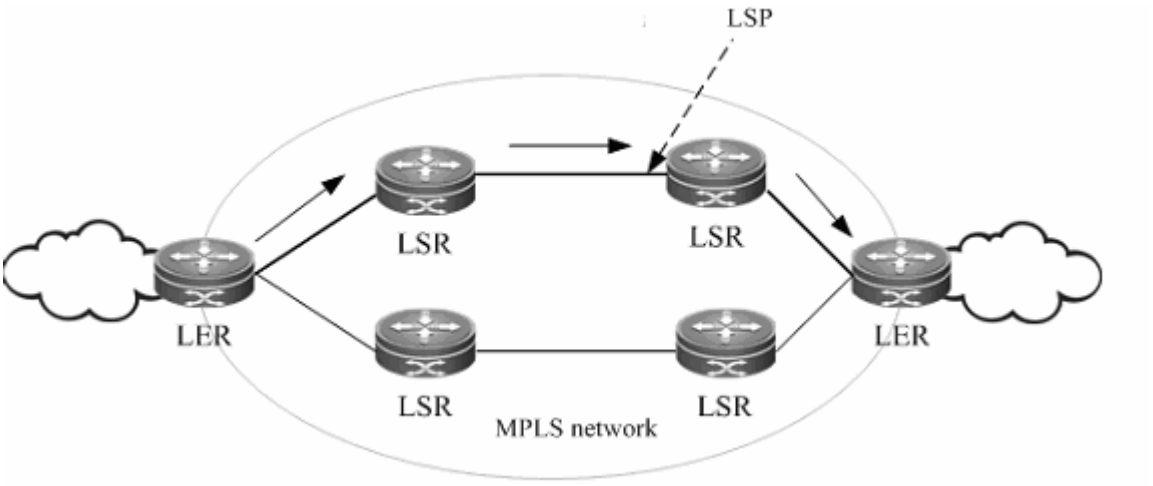


Figure 2

An MPLS network has two basic components: LSR and LER. The LSR, which is located at the core MPLS network, runs the LDP and forwards packets based on labels. The LER classifies incoming packets into FECs, adds labels, and encapsulates the labels as MPLS packets for forwarding. The LER also removes the labels from outgoing MPLS packets and restores the original packets. On the MPLS network, packets with labels are forwarded along the LSP set up through the LDP.

The MPLS system architecture can be divided into the forwarding unit (data plane) and control unit (control plane). The former forwards packets by searching the label forwarding database based on the labels carried in packets whereas the latter is responsible for creating and maintaining label forwarding information database between the connected MPLS nodes. Each

MPLS node must run one or more routing protocols (including static routes) to exchange routing information with other MPLS nodes on the MPLS network. Judged from the control plane, each MPLS node is in nature an IP router. Similar to a traditional IP router, unicast routing protocols (including static routes) are also enabled to create and maintain a routing table on an MPLS node. The traditional router uses the routing table to create a forwarding table. The MPLS node, however, uses the routing table to exchange label binding information between each destination subnet and adjacent MPLS nodes. The protocol that is responsible for exchanging label binding information is the LDP.

1.1.5 MPLS Forwarding Actions

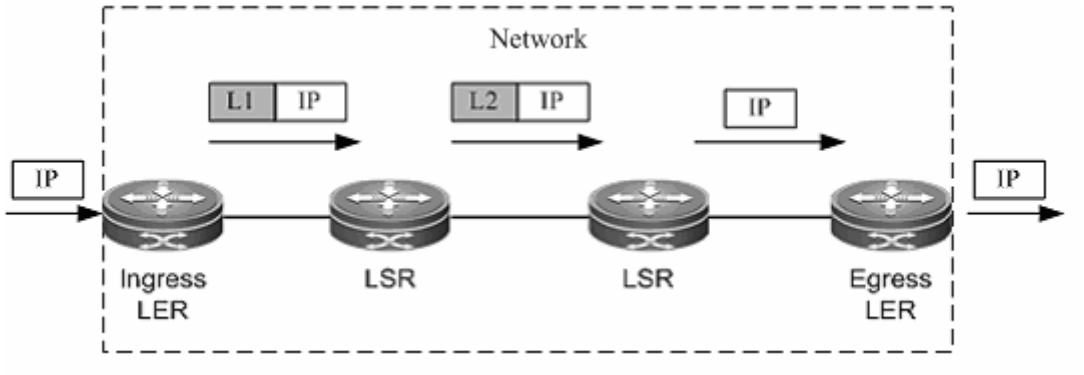


Figure 3 Forwarding process of MPLS packets that support PHP

The following takes traditional IP routing services as an example to show the MPLS forwarding process:

1. Enable traditional routing protocols (OSPF or IS-IS) on all LSRs (including LERs) and create IP routing tables on the LSRs and LERs.
2. Set up an LDP LSP based on the IP routing table.
3. Upon receipt of an IP packet, the ingress LER analyzes the IP packet header and maps it to an FEC. The ingress LER then adds the label L1, to which the FEC corresponds, to the packet and sends the labeled packet to the next hop LSR along the LSP.
4. The next-hop LSR receives the labeled packet, searches the LSP based on the label of the stack top, and then forwards the packet to the next-hop LSR on the LSP after replacing the label.
5. The intermediate LSRs perform the same actions as 4.
6. Upon receipt of the labeled packet, the PHP LSR searches the label forwarding table and pops out the label after learning that the outgoing label is the implicit null label 3. The PHP LSR then forwards the original IP packet to the last-hop LSR. If the outgoing label is the explicit null label, the PHP LSR pops out the label and directly sends the original packet based on the routes of the IP header in the IP forwarding table.

7. If the label is popped out on the PHP LSR, the last-hop egress LER receives the original IP packet and forwards it according to the IP routing table.

1.1.6 LSP Setup and Loop Detection

The pseudo MPLS wire is an LSP. One FEC data stream is assigned with different labels on different MPLS nodes and forwarded according to the labels. The path that the data stream travels is an LSP that consists of a series of LSRs. The data streams of the same FEC pass through the same LSP.

LSP Setup

LSP Loop Control

1.1.6.1 LSP Setup

The LSP setup is in fact the process of binding the FEC to a label and notifying adjacent LSRs of the binding. This process is completed by the LDP. RFC 3036 stipulates the protocol specifications of LDP, the interactive process of LSRs, and the message formats.

The LDP detects adjacent LSRs by periodically sending Hello packets. The LDP Hello packets adopt UDP encapsulation and use the well-known port 646 as the destination port. The destination address of these packets is the multicast address of all routers in the subnet (the corresponding IP address is 224.0.0.2). Upon the discovery of a neighboring LSR, the LDP session is triggered. Setting up an LDP session involves two steps:

1) Set up a transmission connection. This is in fact the completion of TCP three-way handshakes that do not require any interaction of LDP messages.

2) Initialize the session. The LDP session parameters are negotiated and determined by exchanging the initialization information of both parties, such as the label distribution mode, Keepalive duration, and the maximum length of Protocol Data Unit (PDU).

After the LDP session is created and both parties enter the Operational status, the two parties can exchange label messages to distribute and manage labels, and create an LSP for each FEC.

During the LSP setup process, there are two label distribution modes: Downstream on Demand (DOD) and Downstream Unsolicited (DU). In DOD mode, one LSR responds to a label binding message only after the receipt of a label request from an adjacent LSR. In DU mode, one LSR voluntarily sends label binding messages to its adjacent LSRs without receiving any request.

During the LSP setup process, there are two label control methods: independent and ordered control. In independent control mode, each LSR announces to its adjacent devices the binding of labels and FECs at any required time. In independent DOD mode, one LSR can immediately answer an upstream label mapping request without waiting for the label mapping from the next

hop device. In independent DU mode, one LSR can announce the label mapping of an FEC at any time deemed as proper.

In ordered control mode, one LSR binds an FEC to a label and sends the binding upstream only when the FEC has the next-hop label mapping or the LSR is the egress of the FEC. Otherwise, the LSR does not bind the FEC to a label, or send the binding to an upstream LSR until receiving the label mapping of the FEC from a downstream LSR. In ordered control and DU mode, one LSR announces the label to an upstream LSR only when the LSR is the egress of the FEC or the LSR receives the label distributed by a downstream LSR. If the label distribution mode of the downstream LSR is DOD, the LSR, either in DOD or DU mode, passes on the label request from an upstream LSR to downstream devices.

1.1.6.2 LSP Loop Control

During the LSP setup process, the loop detection mechanism must be provided to ensure timely detection of any loops formed by the LSP. There are two methods to avoid LSP loops: the maximum number of hops and path vector.

In the former mode, the messages that transmit label binding information record the number of bypassing LSRs. The number increases by one after every LSR. If the number exceeds the specified maximum value, the system considers that a loop occurs and terminates the LSP.

In the latter mode, the messages that transmit label binding information record the IDs of bypassing LSRs. The ID of an LSR is recorded to the vector table of the message after each LSR. Upon receipt of a label binding message, an LSR checks whether its own ID is included in the vector table. If not, the LSR adds its own ID to the record when distributing the message; if yes, the LSR considers that a loop occurs and terminates the LSP.

1.1.7 MPLS Applications

Thanks to the combination of Layer 2 switching and Layer 3 routing technologies, the MPLS technology improves the forwarding rate of packets. With the development of the Application-Specific Integrated Circuit (ASIC) technologies, the forwarding rate is no longer a bottleneck in network development. As a result, the edges of MPLS in enhancing forwarding rates are not remarkable. Due to the innate advantage of combining Layer 2 switching and Layer 3 routing technologies, however, MPLS still has unprecedented edges over other technologies in terms of virtual private networks (VPNs) and traffic engineering (TE). In this context, MPLS receives more and more attention. The MPLS applications also gradually shift to the application areas of MPLS VPN and MPLS TE.

1.2 Configuring MPLS

1.2.1 Procedures for Configuring Basic MPLS

To configure basic MPLS forwarding functions, perform the following configuration procedures:

Enabling MPLS Globally (Mandatory)

Enabling LDP Globally (Mandatory)

Enabling Label Switching on an Interface (Mandatory)

Caution	For the router products, the **ip ref** command must be used in the interface configuration mode to enable the router MPLS express forwarding function and improve the forwarding performance.

Enabling LDP on an Interface (Mandatory)

Configuring MPLS mtu on an Interface (Optional)

Fragmenting MPLS Packets (Optional)

Handling ICMP Error Messages (Optional)

Configuring the MPLS TTL Replication Function (Optional)

Verifying the MPLS Information (Optional)

Caution	1. The LDP is a topology-driven protocol. To ensure the normal working of the LDP, you should enable IPv4 routing protocols and ensure their normal operations. 2. For the router products, the **ip ref** command must be used in the interface configuration mode to enable the router MPLS express forwarding function and improve the forwarding performance.

1.2.1.1 Enabling MPLS Globally

In the configuration mode, you can run the **mpls ip** command to enable a device to support MPLS forwarding. By default, MPLS is disabled on a device. After MPLS is enabled, the device first forwards packets according to their labels rather than IP addresses. When the label forwarding fails, the device then attempts to forward packets based on their IP addresses.

Run the **no mpls ip** command to disable MPLS forwarding.

Command	Function
DES-7200(config)# **mpls ip**	Enable MPLS globally.

DES-7200(config)# **no mpls ip**	Disable MPLS globally.

Caution

This command is not applicable for controlling switch chip forwarding.

1.2.1.2 Enabling LDP Globally

In the global configuration mode, you can first use the **mpls router ldp** [*vrf-name*] command to enable LDP for a VRF instance and enter the LDP configuration mode.

Run the **no mpls router ldp** [*vrf-name*] command to disable LDP for a VRF instance.

Command	Function
DES-7200(config)# **mpls router ldp** [*vrf-name*]	Enable LDP for a VRF instance and enter the LDP configuration mode.
DES-7200(config-mpls-router)# **ldp router-id interface loopback** *id* **force**	Configure the LDP router ID. The loopback address is generally used as the router ID.
DES-7200(config)# **no mpls router ldp** [*vrf-name*]	Disable LDP for a VRF instance.

Caution

1. After LDP is enabled globally, you still need to run the **mpls ip** command in the interface mode to enable LDP for an interface.
2. If no *vrf-name* is entered, LDP is globally enabled for all VRF instances.
3. You are generally required to specify the router ID for an LDP when you enable LDP.

1.2.1.3 Enabling Label Switching on an Interface

By default, interfaces do not forward MPLS packets. In the global configuration mode, you can use the **mpls ip** command to enable MPLS on a device. You should also use the **label-switching** command to explicitly enable MPLS on a specified interface.

Command	Function

DES-7200(config-if-*type ID*)# **label-switching**	Enable MPLS on an interface.
DES-7200(config-if-*type ID*)# **no label-switching**	Disable MPLS on an interface.

Caution

For the router products, the **ip ref** command must be used in the interface configuration mode to enable the router MPLS express forwarding function and improve the forwarding performance.

1.2.1.4 Enabling LDP on an Interface

After LDP is globally enabled, you should run the **mpls ip** command in the interface mode to enable LDP on an interface.

Command	Function
DES-7200(config-if-*type ID*)# **mpls ip**	Enable LDP on an interface.
DES-7200(config-if-*type ID*)# **no mpls ip**	Disable LDP on an interface.

Caution

After LDP is enabled in the interface mode, the LDP does not take effect on an interface if the **mpls router ldp** command is not used in the global configuration mode to enable LDP. To enable LDP on the interface, you must also use the **label-switching** command to enable MPLS on the interface.

1.2.1.5 Configuring MPLS mtu on an Interface (Optional)

By default, the mtu of MPLS packets that can be transmitted by an interface is the same as the mtu of the interface. The MPLS mtu determines whether MPLS packets should be fragmented during the forwarding. The MPLS mtu indicates the overall length of MPLS encapsulation and encapsulated (such as IP) layers.

Run the **no mpls mtu** command to restore the default value of the MPLS mtu on an interface.

Command	Function
DES-7200(config-if-*type ID*)# **mpls mtu** *bytes*	Configure the MPLS mtu on an interface.

DES-7200(config-if-*type ID*)# **no mpls mtu**	Restore the default value of the MPLS mtu on an interface.

Caution

The MPLS mtu on an interface cannot exceed the actual size of packets transmitted on the interface. For the switches, this configuration is invalid. The switches forward packets based on the mtu configured on actual interfaces and directly discard the packets that exceed the mtu rather than performing fragmentations. To adjust the mtu of an interface, you can use the **mtu** command in the interface mode. Fragmentations are supported by only process and router forwarding. In actual applications, you should adjust the mtu value to avoid performance degradation due to fragmentations.

1.2.1.6 Fragmenting MPLS Packets (Optional)

By default, MPLS packets that exceed the MPLS mtu on an interface are fragmented as IP fragmentations. The fragmented IP packets are still encapsulated with the original labels and transmitted along the original LSP.

Run the **no mpls ip fragment** command to directly discard packets that should be fragmented.

Command	Function
DES-7200(config)# **no mpls ip fragment**	Directly discard MPLS packets that exceed the MPLS mtu on an interface.
DES-7200(config)# **mpls ip fragment**	Restore the default value to fragment packets that exceed the MPLS mtu on an interface.

Caution

This command is valid only for the encapsulated IP packets. It is invalid for non-IP packets. This configuration is also invalid for the switches. The switches directly discard packets that exceed the mtu on an interface. Fragmentations are supported only in process forwarding.

1.2.1.7 Handling ICMP Error Messages (Optional)

To handle ICMP error messages (such as typical MPLS TTL timeout messages) generated during the forwarding of MPLS packets, you can use the **mpls ip icmp-error pop** *labels* command to provide different processing methods for MPLS packets with different numbers of labels. The default value of *labels* is 1. This indicates that the ICMP error messages generated

by MPLS packets with a single layer of labels are forwarded through the global routing table. The ICMP error messages generated by MPLS packets with multiple layers of labels are forwarded along the LSP of the original label stack.

Command	Function
DES-7200(config)# **mpls ip icmp-error pop** *labels*	Control ICMP error messages generated by labeled MPLS packets.
DES-7200(config)# **no mpls ip icmp-error pop**	Restore the default value.

1.2.1.8 Configuring the MPLS TTL Replication Function (Optional)

There are two modes for handling the TTL of encapsulated and decapsulated IP (or MPLS) packets on an MPLS network:

TTL replication mode: This is the default working mode. The procedure is as follows: When a label is pushed, the label TTL copies the TTL of the existing IP or MPLS header to the TTL field of the label. When a label is popped out, the TTL is copied back from the external label to the inner IP packet or MPLS packet.

TTL non-replication mode: In this mode, the TTL is not copied. The procedure is as follows: When a label is pushed, the TTL value of the label is directly set as 255. When a label is popped out, the original TTL value of the inner IP packet or MPLS packet is exposed and retained.

Run the **mpls ip ttl propagate** { **public | VPN** } command to configure the TTL replication function for packets sent and forwarded by a device.

Command	Function
DES-7200(config)# [**no**] **mpls ip ttl propagate public**	Enable or disable the TTL replication function for MPLS packets sent by the device.
DES-7200(config)# [**no**] **mpls ip ttl propagate VPN**	Enable or disable the TTL replication function for MPLS service packets forwarded by the device.

After the TTL replication function is enabled on an MPLS network, you can use the Tracert tool on a CE to track all the LSRs that the packets pass through in the MPLS domain. If the TTL non-replication mode is configured on PEs, the entire LSP of the packets is considered as only one hop.

Caution

1. After TTL replication is enabled, the TTL of the inner header is not copied but retained if it is smaller than the TTL of the outer header.
2. For the switches, the TTL of the inner header is directly copied from the outer header during the PHP Pop operation, if TTL replication is enabled. The TTL of the packets forwarded, however, does not decrease by one. If TTL non-replication is enabled, the TTL of the inner header does not copy that from the outer header. Instead, the TTL of the inner header is retained. The TTL of packets forwarded also does not decrease by one.

1.2.1.9 Verifying the MPLS Information

You can use the **show** commands in the privilege mode to view MPLS information and verify the configuration results.

1. Display MPLS information.

Display the utilization information about the label space and the interfaces enabled with MPLS. You can verify whether the configurations are accurate based on the information.

Command	Function
DES-7200# **show mpls summary**	Display basic MPLS information.

2. Display the MPLS forwarding table.

Display the contents of MPLS forwarding entries and the contents of MPLS forwarding entries added to an MPLS application protocol (such as LDP and MP-BGP).

Command	Function
DES-7200# **show mpls forwarding-table** [*ip-address/mask*] [**label** *label*] [**interface** *interface-name*] [**next-hop** *ip-address*] [**ftn** [**ip	vc**]] [**ilm** [**ip	vc**]] [**vrf** *vrf-name* [**ftn	ilm**]] [**detail**] [**sumary**]	Display the information about the MPLS forwarding table.

3. Display the utilization of the label pool.

Command	Function
DES-7200# **show mpls label-pool**	Display information about the utilization of the MPLS label pool.

4. Check the LSP connectivity.

Command	Function
DES-7200# **ping mpls ipv4** *ip-address/mask* [**repeat** *repeat*] [**ttl** *time-to-live*] [**timeout** *timeout*] [**size** *size*] [**interval** *mseconds*] [**source** *ip-address*] [**destination** *ip-address*] [**force-explicit-null**] [**pad** *pattern*] [**reply mode** {**ipv4** | **router-alert**}] [**dsmap**] [**flags fec**] [**verbose**]	Check the LSP connectivity.
DES-7200# **traceroute mpls ipv4** *ip-address/mask* [**timeout** *timeout*] [**ttl** *ttl*] [**source** *ip-address*] [**destination** *ip-address*] [**force-explicit-null**] [**reply mode** {**ipv4 | router-alert**}] [**flags fec**] [**verbose**]	Check the LSR nodes that the LSP passes through.

1.2.2 Configuring Optional LDP Parameters (Optional)

You can modify the default LDP parameters as required. To modify LDP parameters, you should run the commands in the LDP or the interface configuration mode.

1.2.2.1 Configuring Parameters for an LDP Session

Configuring the LDP Router ID

The LDP Router ID, expressed in the format of IP addresses, uniquely identifies one LSR in a domain. By default, the LDP uses the system Router ID as the LDP Router ID, that is, the LSR ID. The value of an LDP Router ID must be globally unique. In addition, the LDP Router ID must be reachable to other LSRs. This is because the LDP defaults the LDP Router ID as the transport address. You can run the **ldp router-id** command to modify the LSR ID.

Command	Function
DES-7200(config-mpls-router)# **ldp router-id interface** *interface-name* [**force**]	Specify the address of an interface as the LDP Router ID of the LSR. **force** indicates that the current configurations immediately take effect.

DES-7200(config-mpls-router)# **no ldp router-id**	Restore the default value. The system Router ID is used as the LDP Router ID.

Configuring transport-address

By default, the LSR ID is used as the global transport address. As an option, you can choose the main address of an interface or specify an IP address as the transport address to set up an LDP session on the interface. There are the following two configuration methods.

Use commands to configure the transport address of an interface.

Command	Function
DES-7200(config-if-*type ID*)# **mpls ldp transport-address** { **interface** | *ip-address*}	Configure the transport address for LDP sessions on an interface.
DES-7200(config-if-*type ID*)# **no mpls ldp transport-address**	Delete the configuration on the interface. By default, the global transport address is adopted. If no global transport address is configured, the LSR ID is used as the transport address.

Use commands in the LDP configuration mode to globally configure a transport address for all LDP sessions.

Command	Function
DES-7200(config-mpls-router)# **transport-address {interface** | *ip-address* | *interface-name* **}**	Configure a global transport address for LDP sessions.
DES-7200(config-mpls-router)# **no transport-address**	Remove the global setting and restore the LSR ID as the transport address.

Caution

1. When you specify an IP address as the transport address, make sure that the address is reachable to other directly connected LSRs; otherwise, the LDP session cannot be set up.
2. If transport addresses are configured on an interface and globally, the basic LDP session set up on the interface prefers the transport address configured for the interface.
3. The configured transport address is valid only for the basic LDP session. The LDP session set up through extended mechanisms always use the LSR ID as the transport address.

Configuring the Time Interval for Hello Packets

The LDP periodically sends Hello packets to detect LDP peers. By default, the interval for sending Hello packets in the basic LDP discovery mechanism is 5s. You can freely set the interval that ranges from 1 to 65535 seconds in the interface mode.

Command	Function
DES-7200(config-if-*type ID*)# **mpls ldp hello-interval** *seconds*	Set the interval for sending Hello packets in the basic LDP discovery mechanism.
DES-7200(config-if-*type ID*)# **no mpls ldp hello–interval**	Restore the default interval for sending Hello packets in the basic LDP discovery mechanism.

The default interval for sending Hello packets in the extended LDP discovery mechanism is 10s. You can run the **discovery target-hello** *interval* command to modify the interval.

Command	Function
DES-7200(config-mpls-router)# **discovery target-hello interval** *seconds*	Set the interval for sending Hello packets in the extended LDP discovery mechanism.
DES-7200(config-mpls-router)# **no discovery target-hello interval**	Restore the default interval for sending Hello packets in the extended LDP discovery mechanism.

Configuring the Hold Time of Hello Packets

After an LDP peer is detected by periodically sending Hello packets, the local LDP device retains the peer for a period of time although no Hello packet is received from the peer, and considers that the peer expires after this period. This period of time is called the hold time of Hello packets.

The default hold time of Hello packets is 15s. You can freely set the interval that ranges from 1 to 65535 seconds in the interface mode. The value 65535 indicates an indefinite hold time.

Command	Function
DES-7200(config-if-*type ID*)# **mpls ldp hello-holdtime** *seconds*	Set the hold time of Hello packets.
DES-7200(config-if-*type ID*)# **no mpls ldp hello-holdtime**	Restore the default hold time of Hello packets.

The default hold time of Hello packets in the extended LDP discovery mechanism is 45s. You can run the **discovery target-hello** *holdtime* command to modify this value.

Command	Function
DES-7200(config-mpls-router)# **discovery target-hello holdtime** *seconds*	Set the hold time of Hello packets in the extended LDP discovery mechanism.
DES-7200(config-mpls-router)# **no discovery target-hello holdtime**	Restore the default hold time of Hello packets in the extended LDP discovery mechanism.

Configuring the Hold Time of Keepalive Packets

After an LDP peer is detected by periodically sending Hello packets and an LDP session is set up in TCP mode, the local LDP device retains the peer for a period of time although no Keepalive packet is received from the peer. The local LDP device considers that the peer expires and voluntarily terminate the LDP session after this period. This period of time is called the hold time of Keepalive packets. The default hold time of Keepalive packets for the session set up in the basic discovery mechanism is 45s and that for the session set up in the extended discovery mechanism is 180s. You can freely set the value at the range of 15 to 65535. The interval for sending Keepalive packets is one third of the hold time of Keepalive packets.

Command	Function
DES-7200(config-if-*type ID*)# **mpls ldp keepalive–holdtime** *seconds*	In the interface mode, set the hold time of Keepalive packets for the session set up in the basic discovery mechanism.
DES-7200(config-if-*type ID*)# **no mpls ldp keepalive–holdtime**	Restore the default hold time of Keepalive packets for the session set up in the basic discovery mechanism.

DES-7200(config-mpls-router)# **targeted-session holdtime** *seconds*	In the LDP mode, set the hold time of Keepalive packets for the session set up in the extended discovery mechanism.
DES-7200(config-mpls-router)# **no targeted-session holdtime**	Restore the default hold time of Keepalive packets for the session set up in the extended discovery mechanism.

Configuring the Maximum Number of Repeated Label Requests

When an LDP device requests labels, it waits for a period of time to start another attempt if no label is detected due to various reasons. The default number of repeated requests is indefinite. You can freely set the value that ranges from 0 to 255 in the interface mode.

Command	Function
DES-7200(config-mpls-router)# **mpls ldp max-label-requests** *times*	Set the maximum number of repeated LDP label requests.
DES-7200(config-mpls-router)# **no mpls ldp max-label-requests**	Restore the default number of repeated LDP label requests.

Configuring the Maximum PDU

The messages exchanged between LDP devices are all contained in PDUs. You can freely set the value of the PDU that ranges from 256 to 4096 in the interface mode. The default PDU value is 4096.

Command	Function
DES-7200(config-mpls-router)# **mpls ldp max-pdu** *max-pdu*	Set the maximum PDU.
DES-7200(config-mpls-router)# **no mpls ldp max-pdu**	Restore the default PDU (4096).

Configuring the Extended LDP Discovery Mechanism

The basic discovery mechanism is used to detect the local LDP peers. That is, set up a local LDP session with the directly connected LSR. The extended discovery mechanism is used to detect the remote LDP peers. That is, set up a remote LDP session with the non-directly connected LSR.

Command	Function
DES-7200(config-mpls-router)# **neighbor** *ip-address*	Create an extended LDP peer.
DES-7200(config-mpls-router)# **no neighbor** *ip-address*	Delete an extended LDP peer.

1.2.2.2 Configuring LDP Loop Detection

Configuring the Loop Detection Mode

The LDP provides two methods to detect loops: maximum number of hops and path vector. By default, loop detection is disabled for the LDP.

In the loop detection based on the maximum number of hops, in addition to label information, a packet also carries the number of hops and the number increases by one every time the packet passes an LSR. When the number exceeds a preconfigured maximum value, the device considers that a loop occurs on the LSP.

In the loop detection mode of path vector, the packet also carries the LSR ID apart from the label information. At each hop, an LSR first checks whether the number of LSRs in the path vector list already exceeds the preset maximum number in the path vector list.If yes, it means that a loop occurs. If not, the LSR continues to check whether its LSR ID already exists in the path vector list of the LDP message. If yes, it means that a loop occurs; if not, the LSR adds its own LSR ID to the path vector list.

Command	Function
DES-7200(config-mpls-router)# **loop-detection**	Enable loop detection.
DES-7200(config-mpls-router)# **no loop-detection**	Disable loop detection.

Configuring the Maximum Number of Hops

In the interface mode, you can set the maximum number of hops allowed in the loop detection mode. By default, the number is 254. You can set the value at the range of 1 to 255. If loop detection is enabled and the number of hops in an LDP message is detected to exceed the set value, the LSR considers that a loop occurs.

Command	Function

DES-7200(config-if-*type ID*)# **mpls ldp max-hop-count** *number*	Set the maximum number of hops in loop detection.
DES-7200(config-if-*type ID*)# **no mpls ldp max-hop-count**	Restore the default value of the maximum number of hops in loop detection.

Configuring the Maximum Number in the Path Vector List

In the interface mode, you can set the maximum number of LSRs included in the path list of the loop detection based on path vector. By default, the number is 254. You can set the number at the range of 0 to 254. The number means the maximum number of LSRs that can be carried in the path vector list. After loop detection is enabled, an LSR considers that a loop occurs if the LSR detects its own LSR ID in the path vector list or the number of LSR IDs in the path vector list exceeds the preset value.

Command	Function
DES-7200(config-mpls-router)# **mpls ldp max-path-vector** *number*	Set the maximum number in the path vector list of loop detection.
DES-7200(config-mpls-router)# **no mpls ldp max-path-vector**	Restore the default value of the maximum number in the path vector list of loop detection.

1.2.2.3 Configuring the LDP Working Mode

Configuring the LDP Label Distribution Control Mode

The LDP label distribution control mode specifies when an LSR notifies its neighbors of the binding between labels and FECs. There are two control modes: independent control and ordered control.

In independent control mode, the LSR announces to its adjacent devices the binding of labels and FECs at any required time. In ordered control mode, an LSR binds an FEC to a label and sends the binding upstream only when the FEC has the next-hop label mapping or the LSR is the egress LSR of the FEC.

By default, the LDP uses the independent control mode. You can run the **lsp-control-mode** command to set the LDP control mode.

Command	Function

DES-7200(config-mpls-router)# **lsp-control-mode** {**independent** | **orderd**}	Set the label distribution control mode.
DES-7200(config-mpls-router)# **no lsp-control-mode**	Restore the default label distribution control mode.

Configuring the LDP Label Distribution Mode

The LDP label distribution mode specifies how an LSR notifies its neighbors of the binding between labels and FECs. There are two modes: DOD and DU.

In DOD mode, a downstream LSR responds to a label binding message only after the receipt of a label request from an upstream LSR neighbor. In DU mode, one LSR voluntarily sends label binding messages to its upstream LSRs according to certain triggering policies. If the upstream and downstream LSRs use different label distribution modes, use the DU mode if the LSRs are connected to each other through Ethernet.

By default, the LDP works in DU mode. You can use the **distribution-mode** command in the interface mode to set the label distribution mode on an interface.

Command	Function
DES-7200(config-if-*type ID*)# **mpls ldp distribution-mode {du | dod}**	Set the label distribution mode.
DES-7200(config-if-*type ID*)# **no mpls ldp distribution-mode**	Restore the default label distribution mode (DU).

Configuring the LDP Label Retention Mode

The label retention mode specifies whether an LSR should retain the label binding learnt from a label mapping message if the message is not sent from the next hop of the corresponding FEC or the message does not match any existing IP route. There are two label retention modes: conservative and liberal modes.

When the preceding situation occurs, the liberal mode retains the binding of the FEC and label from the neighbor whereas the conservative mode does not retain the binding information.

The conservative label retention mode uses and maintains a small number of labels. The LSR should reobtain the label values in the case of route changes, prolonging responses. The liberal label retention mode, however, responds rapidly to route changes but unnecessary label mappings are also distributed and maintained.

By default, the LDP uses the liberal label retention mode.

You can run the **label-retention-mode** command to set the label retention mode.

Command	Function
DES-7200(config-mpls-router)# **label-retention-mode** {**liberal** | **conservation**}	Set the label retention mode.
DES-7200(config-mpls-router)# **no label-retention-mode**	Restore the default label retention mode.

Configuring Label Merging

If an LSR binds several incoming labels for a certain FEC but uses the same outgoing label for all packets in the FEC, it means that the LSR is capable of label merging. You can enable or disable label merging through LDP configurations.

By default, label merging is enabled for the LDP.

You can run the command to enable or disable label merging.

Command	Function
DES-7200(config-mpls-router)# **label-merge**	Enable label merging.
DES-7200(config-mpls-router)# **no label-merge**	Disable label merging.

Configuring the Transmission Mode of Label Release Messages

When an FEC becomes invalid, the LDP sends label release messages to downstream devices to cancel the label bound to the FEC. Each LDP device on the LSR determines whether to transmit the messages to downstream devices based on the setting on the transmission mode of label release messages.

By default, an LDP device does not send label release messages received from an upstream device to downstream devices.

You can run the **propagate-release** command to set the transmission mode of label release messages.

Command	Function
DES-7200(config-mpls-router)# **propagate-release**	Configure a device to send label release messages to downstream devices.
DES-7200(config-mpls-router)# **no propagate-release**	Configure a device not to send label release messages to downstream devices.

1.2.2.4 Configuring Label Control Policies

Configuring Label Distribution Policies

By default, the LDP assigns labels to all valid IGP routes (excluding BGP routes). In some special situations, you may only want to assign labels to some routes or to only certain LDP peers. In this manner, you can reduce the number of labels and the number of LSPs to lessen device and network burdens.

Command	Function
DES-7200(config-mpls-router)# **advertise-labels for host-routes**	Configure the device to assign labels to only host routes that satisfy the mask length of 32 bits in the route forwarding table. By default, the mask length of routes is not restricted.
DES-7200(config-mpls-router)# **advertise-labels for bgp-routes** [**acl** *acl-name*]	Configure the device to assign labels to BGP routes. By default, the LDP does not assign labels to BGP routes.
DES-7200(config-mpls-router)# **advertise-labels for default-route**	Configure the device to assign labels to default routes. By default, the LDP assigns implicit null label 3 to default routes.
DES-7200(config-mpls-router)# **advertise-labels for acl** *prefix-access-list* [**to** *peer-access-list*]	Configure the device to assign labels to FECs that match ACL rules and specify the device to assign labels only to LDP peers that match the rules.

Caution

1. By default, the LDP assigns labels to only IGP routes. To assign labels to BGP routes, you can run the **advertise-labels for bgp-routes** command.
2. By default, the LDP does not set up an LSP for default routes.

Configuring Label Reception Policies

By default, the LDP receives all label binding information sent from all neighbors. In certain situations, you may need to control the device to receive only some binding information about FECs and labels from certain neighbors. In this case, you can run the **neighbor** *ip-address* **labels accept** command.

Command	Function
DES-7200(config-mpls-router)# **neighbor** *ip-address* **labels accept** *acl- name*	Configure a label reception policy.

Configuring Policies for Distributing Explicit Null Labels

By default, the LDP assigns implicit null labels to the FEC (such as direct routes) with the local device as the egress. You can use the **explicit-null** command to assign explicit null labels to all direct routes or routes that match certain ACL rules. You can also use the **no explicit-null** command to restore the default setting.

Command	Function
DES-7200(config-mpls-router)# **explicit-null** [**for** *prefix_acl* **| to** *peer_acl*]	Configure a device to assign explicit null labels to all direct routes or routes that match certain ACL rules.
DES-7200(config-mpls-router)# **no explicit-null**	Restore the default setting.

Caution

1. For an FEC with the local device as the egress, the device cannot assign explicit null labels to the FEC if the corresponding LSP is a tunnel that carries L2VPN or L3VPN services.
2. Configure this function only for the global LDP instance. This function is not supported by the VRF instance.

1.2.2.5 Configuring the LDP MD5 Authentication

To enhance the reliability of LDP sessions, you can configure the MD5 authentication for the TCP connections used by the LDP sessions. You can run the **neighbor** *ip-address* **password** [**0 | 7**] *pwd-string* command to configure the MD5 authentication for TCP connections between a

device and its peer and run the **no neighbor** *ip-address* **password** [**0 | 7**] *pwd-string* command to restore the default setting.

Command	Function
DES-7200(config-mpls-router)# **neighbor** *ip-address* **password** [**0	7**] *pwd-string*	Configure a device to adopt the MD5 authentication for the TCP connections with its peer.
DES-7200(config-mpls-router)# **no neighbor** *ip-address* **password**	Restore the default setting.

1.2.2.6 Verifying the LDP Information

Display LDP attributes.

You can run the **show mpls ldp parameters** [**all | vrf** *vrf-name*] command to view information about LDP attributes, including the LSR ID, transport address, loop detection mechanism, label distribution control mode, label retention mode, the interval and hold time of Hello packets with extended peers, and the interval and hold time of Keepalive packets with extended peers. You can verify the information to confirm whether the configurations are correct. By default, the LDP attributes of the default VRF are displayed. If **all** is chosen, the LDP attributes of all VRFs are displayed; if *vrf-name* is specified, the LDP attributes of a specified VRF are displayed.

Command	Function
DES-7200# **show mpls ldp parameters** [**all	vrf** *vrf-name*]	Display information about LDP attributes.

Display the information about an interface enabled with LDP.

You can use the **show mpls ldp interface** [**all | vrf** *vrf-name* **|** *interface-name*] command to display the LDP status information about interfaces in all or a specified VRF. You can also display the LDP status information about specific interfaces. By default, the LDP status information about the interfaces of the default VRF is displayed. If **all** is chosen, the LDP status of interfaces in all VRFs is displayed; if *vrf-name* is specified, the LDP status of interfaces in a specified VRF is displayed; if *interface-name* is specified, the LDP status of the specified interface is displayed.

Command	Function
DES-7200# **show mpls ldp interface** [**all	vrf** *vrf-name* **|** *interface-name*]	Display information about the interface enabled with LDP.

Display the binding between FECs and labels.

You can use the **show mpls ldp binding** [**all|vrf** *vrf-name*] | [*ip-address/mask* | **label** *label*] **|** [**remote | local**] command to display the binding information between FECs and labels. You can also use this command to view the LDP working status, whether an FEC is properly bound to a label, or the specific label value bound to an FEC. When using this command, you can filter the display information based on the VRF, address prefix, label value, remote binding, or local binding.

Command	Function
DES-7200# **show mpls ldp bindings** [**all | vrf** *vrf-name*] | [*ip-address/mask* | **label** *label* **|** [**remote | local**]	Display the binding between FECs and labels.

Display LDP neighbors.

You can use the **show mpls ldp neighbor** [**all | vrf** *vrf-name*] | [**detail**] command to view the LDP neighbors of all or a specified VRF, including the TCP connection port, LDP status, statistics about packets received and transmitted, the voluntary LDP discovery party of the local and remote LDP devices. The parameter **detail** displays the detailed information about LDP neighbors.

Command	Function
DES-7200# **show mpls ldp neighbor** [**all | vrf** *vrf-name*] | [**detail**]	Display information about LDP neighbors.

Display information about discovered LDP neighbors.

You can use the **show mpls ldp discovery** [**all | vrf** *vrf-name*] | [**detail**] command to display the information about the ports where LDP neighbors are discovered and about the neighbors. The parameter **detail** displays the detailed information about LDP neighbors.

Command	Function
DES-7200# **show mpls ldp discovery** [**all | vrf** *vrf-name*] **|** [**detail**]	Display information about discovered LDP neighbors.

Reset the LDP session.

You can use the **clear mpls ldp neighbor** command to reset an LDP session and set up a new session.

Command	Function
DES-7200# **clear mpls ldp neighbor** [**all** | **vrf** *vrf-name*] [*|*ip-address*]	Reset an LDP session and set up a new session.

1.2.3 Configuring Static MPLS Forwarding

To support basic MPLS forwarding functions, you can also use static configurations rather than the LDP. To configure basic MPLS forwarding functions in static mode, perform the following configuration procedures:

(Mandatory) Enabling MPLS Globally

(Mandatory) Enabling MPLS on an Interface

(Mandatory) Configuring a Static LSP

Caution

The configuration of a static LSP is independent of LDP. As a result, IPv4 routes are not required. Even if no IPv4 routes exist on the network, the static LSP takes effect, as long as the physical network is reachable.

For the configuration procedures to enable MPLS globally and enable MPLS on an interface, refer to**Procedures for Configuring Basic MPLS**.

1.2.3.1 Configuring a Static LSP

The configuration of an MPLS network in static mode centers around the static LSP. The other configurations are the same as those of the LDP. To configure a static LSP, perform the following three procedures:

Configuring a Static FTN on the Ingress LSR

Configuring a Static ILM on the Intermediate LSR.

Configuring a Static ILM on the PHP LSR

Caution

The label values 16 to 1024 are reserved for static LSPs. When you configure static LSPs, you can choose only these reserved values.

Configuring a Static FTN on the Ingress LSR

On the ingress LSP, set up an FTN entry for the FEC, that is, bind the FEC to a label.

You can run the **mpls static ftn** command in the global configuration mode to configure a static FTN. The syntax of the command is as follows:

Command	Function

DES-7200(config)# **mpls static ftn** *ip-address/M* **out-label** *label* **nexthop** *interface nexthop-ip*	Add a global FTN.
DES-7200(config)# **no mpls static ftn** *ip-address/mask*	Delete a global FTN.

For example, to configure a global FTN that binds label 16 to FEC 192.168.1.0/24, supports the next hop of the LSP as 192.168.10.10, and the outgoing interface as GigabitEthernet 2/1, run the following command:

DES-7200(config)# **mpls static ftn** *192.168.1.0/24* **out-label** *16* **GigabitEthernet** *2/1 192.168.10.10*

To delete the TFN, run the following command. In this case, you are required to only enter the FEC. Other parameters are not required.

DES-7200(config)# **no mpls static ftn** *192.168.1.0/24*

Configuring a Static ILM on the Intermediate LSR.

An intermediate LSR should forward labels for incoming labeled packets. In this case, you are required to configure ILM forwarding entries to map incoming labels to outgoing ones. You can run the **mpls static ilm in-label** command in the global configuration mode to configure a static ILM. The syntax of the command is as follows:

Command	Function
DES-7200(config)# **mpls static ilm in-label** *in_label* **forward-action swap-label** *swap_label* **nexthop** *interface nexthop-ip* **fec** *ip-address/mask*	Add a global ILM.
DES-7200(config)# **no mpls static ilm in-label** *in_label*	Delete a global ILM.

For example, to configure a global ILM that maps the incoming label 16 to the outgoing label 17, supports the next hop of the LSP as 192.168.11.11, the outgoing interface as GigabitEthernet 2/2, and the FEC of the LSP as 192.168.1.0/24, run the following command:

DES-7200(config)# **mpls static ilm in-label** *16* **forward-action swap-label** *17* **nexthop GigabitEthernet** *2/2 192.168.11.11* **fec** *192.168.1.0/24*

To delete the ILM, run the following command:

DES-7200(config)# **no mpls static ilm in-label** *16*

Configuring a Static ILM on the PHP LSR

Since the second but last hop should perform PHP, its ILM entries are different from those on other intermediate LSRs. That is, the outgoing label in the ILM of the PHP LSR on the LSP should be an implicit null label (3).

Caution

For information about the PHP, refer to related materials.

For example, you are required to configure a global ILM on the PHP LSR of the LSP. The LSR pops out the incoming label 17 and sends the packets from GigabitEthernet 2/2. The next hop address is 192.168.12.12 and the corresponding FEC is 192.168.1.0/24. Run the following command:

DES-7200(config)# **mpls static ilm in-label** *17* **forward-action swap-label** *3* **nexthop GigabitEthernet** *2/2 192.168.11.11* **fec** *192.168.1.0/24*

To delete the ILM, run the following command:

DES-7200(config)# **no mpls static ilm in-label** *17*

1.2.4 Example for Configuring Basic MPLS Functions

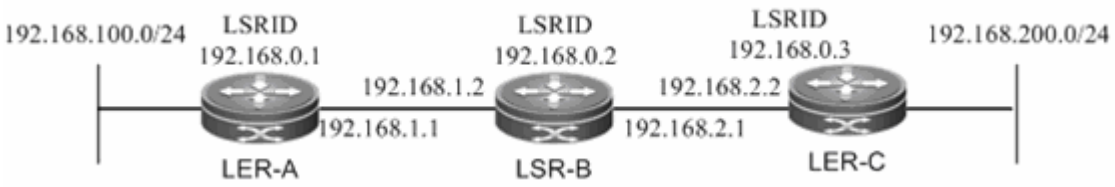


Figure 4

As shown in the preceding figure, three MPLS devices are deployed to construct an MPLS network. The following introduces the setup of an LSP through the LDP and the setup of a static LSP to show the MPLS configuration procedures.

1.2.4.1 Setting Up an LSP Through LDP

The LDP works only with IPv4 routes. Here, OSPF is enabled to set up IPv4 routes. Before the following configurations, make sure that you have created a loopback interface (Loopback 0) and

assigned an IP address, which also serves as the router ID, to the loopback interface on each device.

Configurations on LER_A:

Command	Function
DES-7200(config)# **mpls ip**	Enable MPLS globally.
DES-7200(config)# **mpls router ldp**	Enable LDP and enter the LDP mode.
DES-7200(config-mpls-router)# **ldp router-id interface loopback** 0 **force**	Configure the LDP router ID. The loopback address is generally used as the router ID.
DES-7200 (config-mpls-router)# **exit**	Quit the LDP mode and enter the global configuration mode.
DES-7200(config)# **interface gigabitEthernet** *2/2*	Enter the interface mode of GigabitEthernet 2/2.
DES-7200(config-if-GigabitEthernet 2/2)# **mpls ip**	Enable LDP on the interface.
DES-7200(config-if-GigabitEthernet 2/2)# **label-switching**	Enable MPLS on the interface.
DES-7200(config-if-GigabitEthernet 2/2)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **router ospf** *10*	Enable OSPF and enter the OSPF mode.
DES-7200 (config-router)# **network** *192.168.100.0 0.0.0.255* **area** *0* DES-7200 (config-router)# **network** *192.168.0.1 0.0.0.0* **area** *0* DES-7200 (config-router)# **network** *192.168.1.0 0.0.0.255* **area** *0*	Add routing information to OSPF.
DES-7200(config-router)# **end**	End

Configurations on LER_B:

Command	Function
DES-7200 (config)# **mpls ip**	Enable MPLS globally.
DES-7200 (config)# **mpls router ldp**	Enable LDP and enter the LDP mode.

DES-7200(config-mpls-router)# **ldp router-id interface loopback** *0* **force**	Configure the LDP router ID. The loopback address is generally used as the router ID.
DES-7200 (config-mpls-router)# **exit**	Quit the LDP mode and enter the global configuration mode.
DES-7200 (config)# **interface gigabitEthernet** *2/1*	Enter the interface mode of GigabitEthernet 2/1.
DES-7200(config-if-GigabitEthernet 2/1)# **mpls ip**	Enable LDP on the interface.
DES-7200(config-if-GigabitEthernet 2/1)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-GigabitEthernet 2/1)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **interface gigabitEthernet** *2/2*	Enter the interface mode of GigabitEthernet 2/2.
DES-7200(config-if-GigabitEthernet 2/2)# **mpls ip**	Enable LDP on the interface.
DES-7200(config-if-GigabitEthernet 2/2)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-GigabitEthernet 2/2)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **router ospf** *10*	Enable OSPF and enter the OSPF mode.
DES-7200 (config-router)# **network** *192.168.1.0 0.0.0.255* **area** *0* DES-7200 (config-router)# **network** *192.168.2 .0 0.0.0.255* **area** *0* DES-7200 (config-router)# **network** *192.168.0.2 0.0.0.0* **area** *0*	Add routing information to OSPF.
DES-7200 (config-router)# **end**	End

Configurations on LER_C:

Command	**Function**
DES-7200 (config)# **mpls ip**	Enable MPLS globally.
DES-7200 (config)# **mpls router ldp**	Enable LDP and enter the LDP mode.

DES-7200(config-mpls-router)# **ldp router-id interface loopback** *0* **force**	Configure the LDP router ID. The loopback address is generally used as the router ID.
DES-7200 (config-mpls-router)# **exit**	Quit the LDP mode and enter the global configuration mode.
DES-7200 (config)# **interface gigabitEthernet** *2/1*	Enter the interface mode of GigabitEthernet 2/1.
DES-7200(config-if-GigabitEthernet 2/1)# **mpls ip**	Enable LDP on the interface.
DES-7200(config-if-GigabitEthernet 2/1)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-GigabitEthernet 2/1)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **router ospf** *10*	Enable OSPF and enter the OSPF mode.
DES-7200 (config-router)# **network** *192.168.200.0 0.0.0.255* **area** *0* DES-7200 (config-router)# **network** *192.168.0.3 0.0.0.0* **area** *0* DES-7200 (config-router)# **network** *192.168.2.0 0.0.0.255* **area** *0*	Add routing information to OSPF.
DES-7200 (config-router)# **end**	End

1.2.4.2 Configuring a Static LSP

You can configure a static LSP without IPv4 routes.

Consider an example. Set up two LSPs between No.1 interface at the 192.168.100.0/24 network segment on LER_A and No.2 interface at the 192.168.200.0/24 network segment on LER_C to connect the two network segments. You need to configure one LSP from LER_A to LER_C and the other LSP from LER_C to LER_A. This is because the LSP is uni-directional.

Configurations on LER_A:

Command	Function
DES-7200 (config)# **mpls ip**	Enable MPLS globally.
DES-7200 (config)# **interface gigabitEthernet** *2/2*	Enter the interface mode of GigabitEthernet 2/2.

DES-7200(config-if-GigabitEthernet 2/2)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-GigabitEthernet 2/2)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **mpls static ftn** *192.168.200.0/24* **out-label** *16* **nexthop gigabitEthernet** *2/2 192.168.1.2*	Create an FTN that binds 192.168.200.0/24 to label 16, specify the next hop of the FTN as 192.168.1.2 and the outgoing interface as GigabitEthernet 2/2.
DES-7200(config-router)# **end**	End

Configurations on LER_B:

Command	Function
DES-7200 (config)# **mpls ip**	Enable MPLS globally.
DES-7200 (config)# **interface gigabitEthernet** *2/1*	Enter the interface mode of GigabitEthernet 2/1.
DES-7200(config-if-GigabitEthernet 2/1)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-GigabitEthernet 2/1)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **interface gigabitEthernet** *2/2*	Enter the interface mode of GigabitEthernet 2/2.
DES-7200(config-if-GigabitEthernet 2/2)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-GigabitEthernet 2/2)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **mpls static ilm in-label** *16* **forward-action swap-label** *3* **nexthop gigabitEthernet** *2/2 192.168.2.2* **fec** *192.168.200.0/24*	Create an ILM that maps the incoming label 16 to the outgoing label 3 (implicit null label) on GigabitEthernet 2/2. Specify the next hop address as 192.168.2.2 and the FEC as 192.168.200.0/24.
DES-7200 (config)# **mpls static ilm in-label** *17* **forward-action swap-label** *3* **nexthop gigabitEthernet** *2/1 192.168.1.1* **fec** *192.168.100.0/24*	Create an ILM that maps the incoming label 17 to the outgoing label 3 (implicit null label) on GigabitEthernet 2/1. Specify the next hop address as 192.168.1.1 and the FEC as 192.168.100.0/24.
DES-7200 (config-router)# **end**	End

Since LER_B is the PHP LSR for the FEC 192.168.100.0/24, the incoming label 17 is mapped to the outgoing label 3 (implicit null label). The outgoing interface is GigabitEthernet 2/1.

Similarly, since LER_B is the PHP LSR for the FEC 192.168.200.0/24, the incoming label 16 is also mapped to the outgoing label 3 (implicit null label). The outgoing interface is GigabitEthernet 2/2.

Configurations on LER_C:

Command	Function
DES-7200 (config)# **interface gigabitEthernet** *2/1*	Enter the interface mode of GigabitEthernet 2/1.
DES-7200(config-if-GigabitEthernet 2/1)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-GigabitEthernet 2/1)# **exit**	Quit the interface mode and enter the global configuration mode.
DES-7200 (config)# **mpls static ftn** *192.168.100.0/24* **out-label** *17* **nexthop gigabitEthernet** *2/1 192.168.2.1*	Create an FTN that binds 192.168.200.0/24 to label 16, specify the next hop of the FTN as 192.168.1.2 and the outgoing interface as GigabitEthernet 2/2.
DES-7200 (config-router)# **end**	End

After the preceding configurations, the packets destined for the 192.168.200.0/24 network segment on LER_A are sent out by GigabitEthernet 2/2 on LER_A and pushed with label 16. After arrival at the GigabitEthernet 2/1 interface on LER_B, the packets with label 16 are then transformed to IP packets and sent out by GigabitEthernet 2/2 on LER_B. After the IP packets destined for the 192.168.200.0/24 network segment arrives at LER_C, LER_C selects routes based on the destination IP addresses and sends out the packets from GigabitEthernet 2/1.

2 Configuring BGP IP VPN

2.1 Introduction to BGP/MPLS VPN

In traditional VPNs, private network data streams are generally transmitted over public networks through GRE, L2TP, and PPTE tunnel protocols. As another implementation of VPN, BGP/MPLS IP VPN can be considered as a VPN between Layer 2 and Layer 3. An LSP is a tunnel on the public network that is set up through the MPLS LDP. In an MPLS VPN, the different branches of private networks at different locations are connected together to form one network through LSPs. The MPLS VPN also supports interworking between different VPNs. The implementation of VPN through MPLS has natural edges. For VPN users, the work amount is largely reduced since no special VPN devices are required to construct the VPN. Instead, the VPN users can directly use traditional routers. For carriers, the MPLS VPN can be easily expanded.

As a highly effective technical platform for IP backbone networks, MPLS provides VPNs with flexible and scalable technical foundations.

The L3VPN based on BGP/MPLS VPN has the following features:

1) The VPN tunnels are set up on the provider edge (PE) devices of network service providers rather than the customer edge (CE) devices. The VPN routes are also transmitted between PEs. In this manner, users are not required to maintain VPN information.

2) Directly utilize existing routing protocols. The setup of VPN tunnels and route advertising are dynamically implemented, facilitating the expansion of VPNs.

3) Support address overlapping. Different VPN users can use the same address space.

4) On the network of service providers, VPN services are exchanged according to labels rather than traditional routes.

5) Support the same security as user dedicated lines.

The BGP/MPLS VPN provides the following functions:

1) Adopt the LDP to set up LSPs on the backbone network. This process is generally performed on the provider's network and completed when the topology becomes stable.

2) Forward data packets based on the pushed label and the local mapping table.

3) Support MP-BGP and extended BGP attributes to transmit VPN routes and carry VPN attributes and labels.

4) Manage VPN routes to set up multiple routing tables and maintain VPN routes.

2.1.1 Components of a BGP/MPLS VPN

A BGP/MPLS VPN model consists of three components, as shown in the following figure.

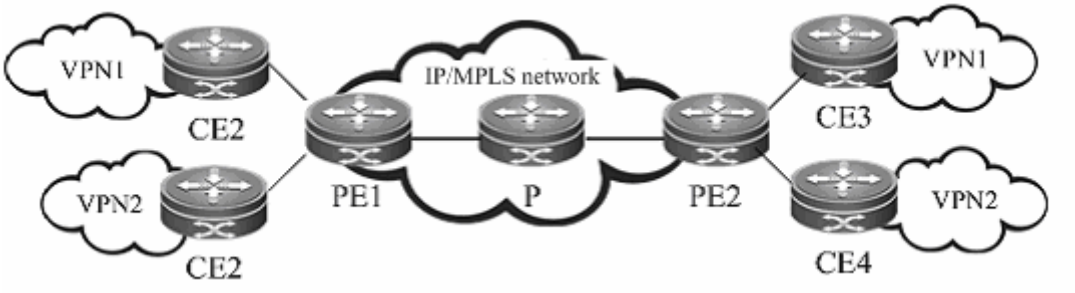


Figure 5 Basic components of a VPN

- CE

Located at customer edge, a CE logically belongs to a user VPN. One interface on the CE is directly connected to the PE device. The CE can be a host, router, or switch that may not support MPLS. As shown in the figure, CE1, CE2, CE3, and CE4 are CE devices.

- PE

A PE is an edge device on the SP backbone network. It can be a router, an ATM switch or an FR switch, as shown in PE1 and PE2 in the figure. A PE logically belongs to the service provider and is directly connected to a CE. You can connect one PE to multiple CEs. The PE is mainly responsible for receiving the VPN information from CEs and transmitting the information to other PEs, or receiving the VPN information from other PEs and sending it to the CEs. The PEs should support MPLS.

- P

The Provider Router (P) is a core device on the SP backbone network, as shown in P1, P2, and P3 in the figure. The P is not connected to CEs. It is responsible for routing and rapid forwarding. As a device on the core MPLS backbone network, the P should support MPLS. The P knows the routes to any destination on the backbone network but does not know the routes to a VPN.

2.1.2 VRF

- VRF

The VPN Routing and Forwarding table (VRF) is used to address the conflicts of local routes. Each connection between a PE and CE is associated with a VRF. One PE can have several VRFs to exchange route information with CEs. You can consider a VRF as a virtual router. Each virtual router should be connected to a CE to receive route information from the CE or notify the CE of the VPN route information. The VRF addresses the conflicts of local routes due to the adoption of the same address space by different VPNs. One VRF includes the following:

1) An independent routing table

2) A group of interfaces that belong to the VRF

3) A group of routing protocols that are used in the VRF

The VRF has two important attributes: Route Distinguisher (RD) and Route-Target (RT) attributes.

- RD

The RD is introduced to address the conflict of routes during the transmission.

You can consider the RD as a distinguisher. If different VPNs use the same network address and advertise their route information on the backbone network through BGP, the BGP module chooses and advertises only the best route from the overlapped addresses. As a result, some VPNs cannot obtain their route information. If the RD values are added to the overlapped addresses, the BGP module identifies the same network addresses based on the different RDs carried in the VPN information. In this manner, each VPN can obtain its own route information. The RD only serves as a distinguisher to identify the same network addresses. If address overlapping does not exist for different VPNs, you can configure no RD values.

Generally speaking, one VPN is specified with a unique RD value. In this manner, different VPNs have different RDs, facilitating the transmission of routing information on the backbone network. The RD value is generally defined as xx: xx, such as RD 1: 100, among which 1 stands for the AS number of the backbone network and 100 is a number specified by the user. One VPN route can carry only one RD value.

The RD consists of three fields: type, administrator, and assigned number. Based on the value of the type field, the encoding formats are classified into the following three types:

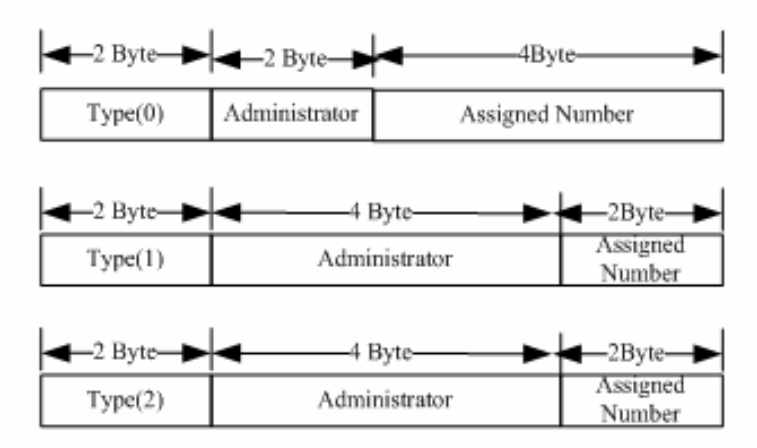


Figure 6 RD structure

1) When Type = 0, the administrator field has two bytes and is marked by the AS number that must be of a public AS. The assigned number has four bytes that are managed by the service provider.
2) When Type = 1, the administrator field has four bytes and uses an IPv4 address that must be a global IP address. The assigned number has two bytes that are managed by the service provider.
3) When Type = 2, the administrator field has four bytes and is marked by the four-byte AS number. The assigned number has two bytes that are managed by the service provider.

- Route-Target

The introduction of the RT attribute is to let the VRF choose its route selection mode. The RT attributes are classified into export Route-Target and import Route-Target. A PE receives routes from a CE and adds Export Route-Target to the VPN routes and then notifies other PEs of the VPN routes. The PE determines whether to import the routes received from other PEs to the VRF based on the Import Route-Target. One principle is that when a PE receives a VPN route, the PE imports the route to the VRF only when at least one RT attribute carried in the route is the same as the Import RT in the VRF of the PE. In this manner, you can flexibly control the advertising of VPN routes. One VPN route can carry multiple RT values.

The BGP extended community attribute defines the RT encoding structure, as shown in the following figure.

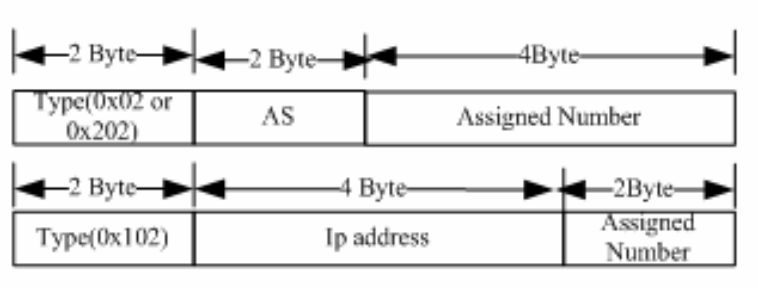


Figure 6 RT structure

The definition of RT is similar to that of RD. For 0x02 and 0x202, the AS number must be a public one. For 0x102, the IPv4 address must be a global one rather than a private address.

2.1.3 MP-BGP

The VPN route information is transmitted on the backbone network through BGP. The export RT attribute is carried in the BGP extended community attribute. The traditional BGP4, however, transmits only IPv4 routes and cannot carry the VPN route that includes RDs. Therefore, the BGP is extended to introduce new attributes. One of the biggest advantages of BGP is its scalability. The Multi-Protocol (MP-BGP) is a new attribute introduced to the original BGP to support multiple protocols. The MP-BGP can carry VPN information. In this manner, the VPN route takes up the form of RD + IP address prefix. By adding RDs to VPN routes exchanged between PEs, the MP-BGP allows VPN users to change the IPv4 routes to VPN-IPv4 routes and transmit them on the backbone network.

2.1.4 Protocol Specifications

IETF RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)

2.2 Default Configurations

By default, BGP/MPLS L3 VPN is disabled.

Functions	Default Setting
Basic BGP/MPLS L3 VPN functions	Disabled
VPN label distribution mode	Assigning labels to each VRF
Inter-AS VPN	Disabled
CSC VPN	Disabled
MPLS VPN Over GRE	Disabled

2.3 Configuring BGP/MPLS VPN

2.3.1 Configuring Basic BGP/MPLS VPN Functions

To configure basic BGP/MPLS VPN fucntions, perform the following configurations:

Configuring an MPLS Network (Mandatory)

Configuring a VPN Routing Instance (Mandatory)

Configuring PEs to Transmit VPN Routes (Mandatory)

Configuring Route Exchanging Between PEs and CEs (Mandatory)

Configuring the VPN Label Distribution Mode (Optional)

Configuring Import and Export Policies for VPN Routes (Optional)

Configuring a Static L3VPN FTN and ILM (Optional)

2.3.1.1 Configuring an MPLS Network

To use MPLS on the backbone network, you must configure the MPLS LDP on the P and PE to set up public tunnels. This means that you have to configure LDP on MPLS devices and enable MPLS on each interface. The configuration procedure is as follows:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **mpls ip**	Enable MPLS globally.
DES-7200(config)# **mpls router ldp**	Enable LDP and enter the LDP configuration mode.
DES-7200(config-mpls-router)# **ldp router-id interface loopback** *id* **force**	Configure the LDP router ID. The IP address of the loopback interface is generally used as the router ID.
DES-7200(config-mpls-router)# **exit**	Quit the LDP configuration mode.
Ruiije(config)# **interface** *type ID*	Enter the interface configuration mode.
DES-7200(config-if-*type ID*)# **ip address** *ip-address mask*	Assign an IP address to the interface.
DES-7200(config-if-*type ID*)# **label-switching**	Enable MPLS on the interface at the public network side.
DES-7200(config-if-*type ID*)# **mpls ip**	Enable LDP on the interface.

DES-7200(config-if-*type ID*)# **show running-config**	View all configuration information.

Configure an MPLS network.

```
DES-7200# configure terminal
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)#interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-gigabitethernet 1/1)# no switchport
DES-7200(config-if-gigabitethernet 1/1)# ip address 192.168.10.1 255.255.255.0
DES-7200(config-if-gigabitethernet 1/1)# label-switching
DES-7200(config-if-gigabitethernet 1/1)# mpls ip
```

2.3.1.2 Configuring a VPN Routing Instance

A VPN routing instance is the VRF that is configured on PEs. The CE and P devices do not have VRFs.

The configuration of a VRF includes defining the VRF, assigning RD and RT values to the VRF, and associating the VRF with an interface. The configuration procedure is as follows:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip vrf** *vrf-name*	Create a VRF and enter the VRF configuration mode.
DES-7200(config-vrf)# **rd** *rd-value*	Set the RD value.
Ruiije(config-vrf)# **route-target** {**both | export | import**} *rt-value*	Set the RT value.
DES-7200(config-vrf)# **exit**	Quit the VRF configuration mode.
DES-7200(config-if-*type ID*)# **interface** *type ID*	Enter the interface configuration mode.
DES-7200(config-if-*type ID*)# **ip vrf forwarding** *vrf-name*	Associate the interface with the VRF.
DES-7200(config-if-*type ID*)# **ip address** *address mask*	Assign an IP address to the interface.

DES-7200(config-if-*type ID*)# **show running-config**	View all configuration information.

Configure a VRF and bind it to Gigabitethernet 1/1.

```
DES-7200(config)# ip vrf vpn1
DES-7200(config-vrf)# rd 100: 1
DES-7200(config-vrf)# route-target both 100: 1
DES-7200(config-vrf)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-gigabitethernet 1/1)# no switchport
DES-7200(config-if-gigabitethernet 1/1)# ip vrf forwarding vpn1
DES-7200(config-if-gigabitethernet 1/1)# ip address 192.168.10.1
255.255.255.0
```

Caution

1. If the VRF on a PE is defined with an RD value or the PE is enabled with BGP VRF, the RD value cannot be modified or deleted. In this case, you can only delete the VRF and create the VRF again to set the RD value.
2. Two different VRFs on the same PE cannot be assigned with the same RD.
3. If you enter the **ip vrf forwarding** *vrf-name* command, the IP address assigned to the interface earlier is deleted. In this case, you need to redefine the IP address in the interface mode.

2.3.1.3 Configuring PEs to Transmit VPN Routes

PEs transmit routing information through BGP. Since a PE needs to transmit VPN routing information rather than common IPv4 routing information with another PE, you need to enter the VPN address family mode to configure the PE to transmit VPN routes with the peer PE. The configuration procedure is as follows:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-num*	Create a BGP domain and enter the BGP configuration mode.

DES-7200(config-router)# **neighbor** *ip-address* **remote-as** *asn-number*	Configure a BGP session.
Ruiije(config-router)# **neighbor** *ip-address* **update-source** *interface-name*	Set the interface address used to set up the MP-IBGP session as the source address. The address of the loopback interface is generally used as the source address.
Ruiije(config-router)# **address-family vpnv4**	Enter the VPN address family.
DES-7200(config-router-af)# **neighbor** *ip-address* **activate**	Activate the BGP session to exchange VPN routes.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Set up an MP-BGP session with the neighboring PE at 1.1.1.1.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 1
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
```

2.3.1.4 Configuring Route Exchanging Between PEs and CEs

Configuring BGP Between PEs and CEs to Transmit Routing Information

To configure a BGP session with a CE, you need to enter the VRF address family mode on the PE and then configure the routing protocol with the CE. The configuration procedure on the PE is as follows:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *pe-asn-num*	Create a BGP domain and enter the BGP configuration mode.
DES-7200(config-router)# **address-family ipv4 vrf** *vrf-name*	Configure and enter the BGP VRF address family configuration mode.

Ruiije(config-router-af)# **neighbor** *ip-address* **remote-as** *ce-asn-num*	Set up an EBGP session with a CE.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Set up an EBGP session with the neighboring CE at 192.168.10.2.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf vrf1
DES-7200(config-router)# neighbor 192.168.10.2 remote-as 2
```

Caution

Generally speaking, a VRF is assigned with an RD value after the VRF is defined. If no RD value is specified for the VRF, the preceding **address-family ipv4 vrf** *vrf-name* command enters the address family of the specified VRF and the system creates a default RD value 0:0 for the VRF. After this value is created, the RD value cannot be modified or deleted.

The configuration procedure for a PE peer on the CE is as follows:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *ce-asn-num*	Create a BGP domain and enter the BGP configuration mode.
Ruiije(config-router)# **neighbor** *ip-address pe-asn*	Set up an EBGP session with a PE.
DES-7200(config-router)# **show running-config**	View all configuration information.

Set up an EBGP session with the PE at 192.168.10.1.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 2
DES-7200(config-router)# neighbor 192.168.10.1 remote-as 1
```

Configuring OSPF Between PEs and CEs to Transmit Routing Information

To run OSPF between a PE and CE, you must configure an OSPF instance for the VRF on the PE. The VRF then uses the OSPF instance to exchange routing information between the PE and CE. By redistributing BGP routes, the OSPF module sends the VPN routes received from other

PEs to the CE. At the same time, by redistributing OSPF routes, the BGP module sends the VPN routing information that is sent to the PE by the CE to other PE peers.

The configuration procedure on the PE is as follows:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router ospf** *ospf-id vrf-name*	Create an OSPF instance and enter the OSPF configuration mode.
DES-7200(config-router)# **network** *prefix mask* **area** *area-id*	Configure an OSPF link.
Ruiije(config-router)# **redistribute bgp subnets**	Configure the OSPF module to redistribute BGP routes.
Ruiije(config-router)# **exit**	Quit the OSPF configuration mode.
DES-7200(config)# **router bgp** *asn*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **address-family ipv4 vrf** *vrf-name*	Enter the BGP VRF configuration mode.
DES-7200(config-router-af)# **redistribute ospf** *ospf-id*	Redistribute OSPF routes.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Run OSPF between a PE and CE to distribute VPN routes.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 vrf1
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config-router)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf vrf1
DES-7200(config-router-af)# redistribute ospf 10
```

Transmitting Routing Information Between a PE and CE Through Static Configurations

In simple network environments, you can generally configure static routes. The configuration procedure is as follows:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip route vrf** *vrf-name prefix mask interface-name nexthop*	Configure a static route.
DES-7200(config)# **router bgp** *asn*	Enter the BGP configuration mode.
DES-7200(config-router)# **address-family ipv4 vrf** *vrf-name*	Enter the BGP VRF address family configuration mode.
DES-7200(config-router-af)# **redistribute static**	Redistribute static routes.
DES-7200(config-router)# **show running-config**	View all configuration information.

Configure a static route on the PE to distribute VPN routes.

```
DES-7200# configure terminal
DES-7200(config)# ip router vrf vrf1 192.168.20.0 255.255.255.0 gigabitEthernet 2/3
192.168.10.2
DES-7200(config-router)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf vrf1
DES-7200(config-router-af)# redistribute static
```

2.3.1.5 Configuring the VPN Label Distribution Mode (Optional)

RFC 4364 describes two label distribution modes for L3VPN applications: route-based and VRF-based label distribution. The advantage of the former is rapid forwarding speed that allows a device to forward packets to the next hop by searching the ILM table. The disadvantage, however, is the large capacity of the ILM table. The advantage of the latter is the reduced capacity of the ILM table. This is because one label is assigned for each VRF and all routes in the VRF thus share the label. The disadvantage is the lower forwarding efficiency since it requires two times of table searching. The device should first locate the VRF of the packets based on the ILM table and then forward the packets by searching routes based on the destination IP address of the VRF.

By default, an L3VPN adopts the VRF-based label distribution mode. You can run the **alloc-label** command in the VRF configuration mode to modify the default label distribution mode. You can also choose different distribution modes for different VRFs.

To configure the label distribution mode, you should enter the privilege mode and perform the following configuration steps:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **ip vrf** *vrf-name*	Create a VRF and enter the VRF configuration mode.
DES-7200(config-vrf)# **alloc-label per-vrf**	Assign one label to all routes in the VRF. When advertising VPN routes, the MP-BGP uses the same label for all routes.
DES-7200(config-vrf)# **alloc-label per-route**	Assign one label to each route in the VRF. When advertising VPNv4 routes, the MP-BGP uses a different label for each route.
DES-7200(config-vrf)# **show running-config**	View all configuration information.

Caution

1. When you modify the label distribution mode, the MP-BGP cancels all routes advertised in the VPN and advertises the routes again.
2. By default, the VRF-based label distribution mode is adopted. In this case, a PE first pops out the received packets with labels and then chooses routes to forward the packets based on the IP routing table.

2.3.1.6 Configuring Import and Export Policies for VPN Routes (Optional)

In most situations, you can define the route-target import attribute in the VRF configuration mode to determine the routes to be imported into the VRF and define the route-target export attribute to determine the RTs to be carried in the routes. These configurations are valid to all routes. In certain application scenarios that require accurate control on the import and export of VPN routes, however, you need to adopt polices. Enter the privilege mode and perform the following configuration procedure:

Command	Function

DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **ip vrf** *vrf-name*	Create a VRF and enter the VRF configuration mode.
DES-7200(config-vrf)# **import map** *routemap-name*	Set the policy to import remote VPNv4 routes to the local VPN routes based on the rules defined in the route map.
DES-7200(config-vrf)# **export map** *routemap-name*	Set the extended community attribute to export remote VPNv4 routes based on the rules defined in the route map.
DES-7200(config-vrf)# **show running-config**	View all configuration information.

Caution

The rules defined by using the **import map** command take effect after the extended community attribute defined in the VRF is imported. That is, remote VPN routes can enter the rules defined by using the **import map** command for further filtering only after the routes match the extended community attribute defined by the **route-target import** command for the VRF.

Configure a route map that exports VPN routes with the RT of 100:1 to vrf1.

```
DES-7200# configure terminal
DES-7200(config)# ip extcommunity-list 1 permit rt 100: 1
DES-7200(config)# route-map IN-RT-FILTER
DES-7200(config-route-map)# match extcommunity 1
DES-7200(config-route-map)# exit
DES-7200(config)# ip vrf vrf1
DES-7200(config-vrf)# rd 100:2
DES-7200(config-vrf)# route-target export 100: 30
DES-7200(config-vrf)# import-map IN-RT-FILTER
DES-7200(config-route-map)# end
DES-7200# show ip vrf vrf1
VRF vrf1; default RD : 100:2
Interfaces:
Vlan 1 // the interface bound to the VRF
Export VPN route-target communities: //the configured list of export extended community
attributes
RT: 100:30
```

```
No import VPN route-target community //the configured list of import extended community
attributes (no configuration)import-map: IN-RT-FILTER //the configured import policies
```

2.3.1.7 Configuring a Static L3VPN FTN and ILM (Optional)

In most situations, the MP-BGP assigns labels to private routes and the public LSP is generated by running the LDP on a public network. You can also configure a static LSP to assign labels to private routes and set up private LSPs. To configure an FTN for the L3VPN on the PE, you should enter the privilege mode and perform the following configuration steps:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **mpls static l3vpn-ftn** *vrf-name ip-address/mask* **out-label** *out-label* **remote-pe** *ip-address*	Configure a static private FTN that specifies the egress of the FEC as another PE. In this case, you must specify the private label and the egress PE. The address of the egress PE is then used to configure the public LSP.
DES-7200(config)# **mpls static l3vpn-ftn** *vrf-name fec-prefix/fec-mask* **local-forward nexthop** *interface-name nexthop-ip*	Configure a static private FTN that specifies the egress of the FEC as the local PE. In this case, you must specify the outgoing interface on the local PE and the next-hop address (the outgoing interface and the next hop is generally in another VRF). You can use this command when the local PE has several VRFs that belong to the same VPN.
DES-7200# **show running-config**	View all configuration information.

To configure an ILM for the L3VPN on the PE, you should enter the privilege mode and perform the following configuration steps:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **mpls static ilm in-label** *in-label* **forward-action pop-l3vpn-nexthop** *vrf-name* **nexthop** *interface-name nexthop-ip-address* **fec** *ip-address/mask*	Configure an ILM entry for the L3VPN on the PE. You need to specify the incoming label, the outgoing interface, and the next-hop address.
DES-7200# **show running-config**	View all configuration information.

Caution

The configured static private FTN and ILM take effect only after the corresponding public LSP is set up. To set up the public LSP, refer to Procedures for Configuring Basic MPLS. You can set up a public LSP through LDP or static configurations.

2.3.2 Configuring an Inter-AS VPN

On an actual network, different sites of VPN users may be located on different ASs and mutual communication is required between these sites. In this case, the VPN routes should be exchanged between different ASs. This technology is called the inter-AS VPN.

RFC 4364 introduces three types of inter-AS VPN schemes:

OptionA: VRF-to-VRF mode

OptionB: single-hop MP-EBGP mode

OptionC: multi-hop MP-EBGP mode

2.3.2.1 OptionA: VRF-to-VRF Mode

Also referred to as the VRF back-to-back, the VRF-to-VRF mode features easy implementation. The ASBR of an AS sets up a VRF for each inter-AS VPN to bind the VRF to an interface. The VRFs on ASBRs then exchange VPN routes through the interface.

The purpose to create a VRF and bind it to an interface is as follows:

Receive VPN routes from the local AS.

Set up an EBGP connection between the VRF and the VRF of another AS to exchange IPv4 routes.

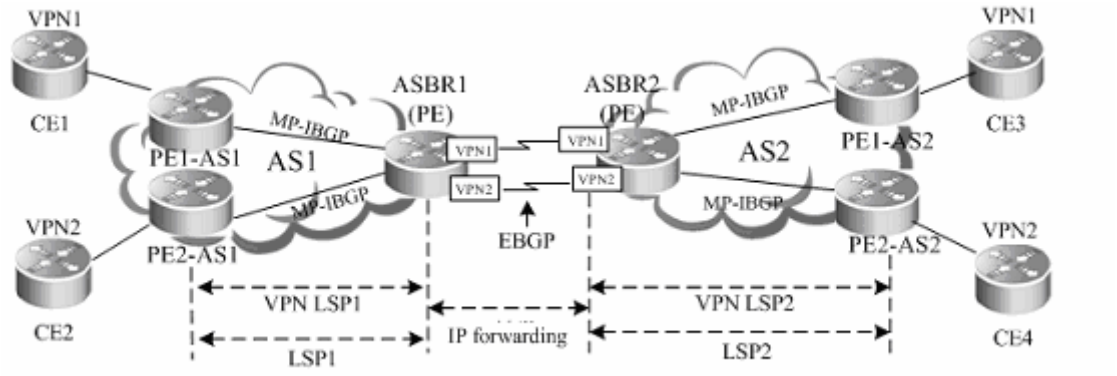


Figure 8 VRF-to-VRF inter-AS VPN

As shown in the preceding figure, the VRFs between the ASBRs set up common EBGP sessions to exchange IPv4 routes and the ASBRs and PEs set up MP-IBGP sessions to exchange VPN routes. For the VRF on an ASBR, the other VRF, with which the EBGP session is set up, is equivalent to a CE. This configuration scheme is similar to the common intra-domain scheme. The ASBRs and PEs set up MP-IBGP sessions to exchange VPN routes. The VRFs of ASBRs set up EBGP sessions in the BGP VRF address family mode to exchange IPv4 routes.

Characteristics and limitations

The VRF-to-VRF mode is easy to implement by directly using MP-IBGP. The service deployment is also simple. This scheme, however, requires an interface (generally a logical sub-interface) for each inter-AS VPN on an ASBR. The number of bound interfaces at least should be equal to the number of inter-AS VPNs. You should configure an interface for each VPN on the ASBR, complicating network expansion. In addition, the separate creation of sub-interfaces for each VPN poses high requirements on ASBRs. As a result, this scheme is generally applicable to networks with a small number of inter-AS VPNs.

The configuration of OptionA is similar to that of a BGP/MPLS VPN and is not described here.

2.3.2.2 OptionB: Single-Hop MP-EBGP Mode

In the OptionA scheme, you need to configure a VRF for each VPN on an ASBR and bind the VRF to an interface. This is because VPN routes cannot be directly transmitted between EBGPs and can only be carried through MP-IBGP. If the VPN routes can be directly transmitted between EBGPs, you are not required to configure VRFs on the ASBR. This is clearly a better implementation mode. In this case, the OptionB scheme extends MP-IBGP and allows the direct transmission of VPN routes between ASBRs. This is called the single-hop EBGP, as shown in the following topology.

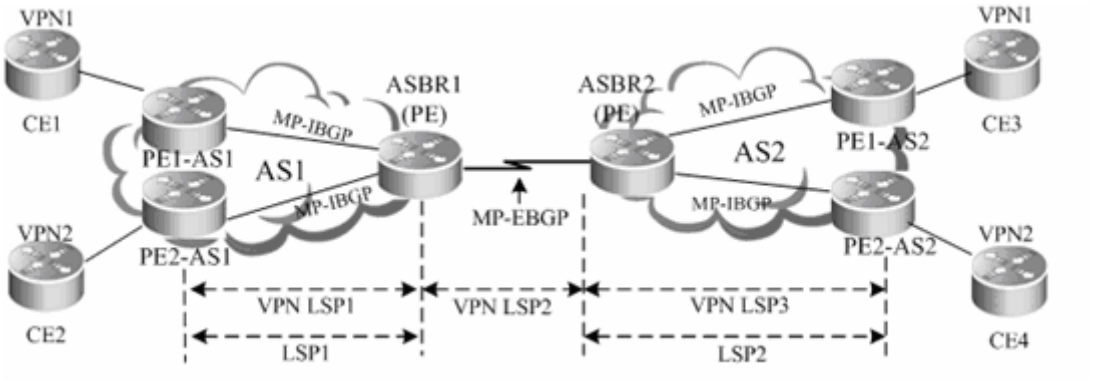


Figure 9 OptionB inter-AS VPN

Characteristics and limitations

The advantage of this MP-EBGP scheme is that you are not required to configure a sub-interface for each site of VPN users on an ASBR. You are also not required to set up the inter-AS LSP. The VPN routes are directly transmitted between single-hop MP-EBGP neighbors. The VPN routing information, however, is maintained and spread by the ASBRs between ASs. If a large number of VPN routes exist, the ASBRs are faced with heavy pressures. Since the ASBRs also generally assume forwarding tasks of IP packets on the public network, high requirements are imposed on these devices. In addition, the ASBRs cancel the RT filtering function for received VPN routes. The VPN routes on PEs may be spread to the ASBRs in another AS. This may lead to the leakage of VPN routes. As a result, the SPs, who exchange VPN routes, must reach trust agreements on route exchanging. The ASBRs should trust each other and perform corresponding route filtering policies. The OptionB scheme is applicable to networks with lots of inter-AS VPN services.

OptionB has two schemes:

The ASBR does not change the next hop of a VPN route.

The ASBR changes the next hop of a VPN route.

The following describes the configuration procedures of the two schemes.

Scheme 1: Next Hop Unchanged

When an ASBR receives VPN routes sent from the ASBR in another AS and sends the routes to the MP-IBGP neighbors in the local AS, the next hop of the routes is not changed. This mode is called the "OptionB Next Hop Unchanged Scheme". In this mode, the PEs and ASBRs in an AS still set up MP-IBGP sessions to exchange VPN routes and the two ASBRs set up MP-EBGP sessions to directly exchange VPN routes. When sending routes to an MP-IBGP neighbor, the ASBR does not change the next hop of the VPN routes received from the MP-EBGP neighbor. This requires that the PE in the AS should have a route to the next hop address (that is, the ASBR in another AS). For this purpose, you can configure the local ASBR to redistribute routes destined for the other ASBR to the IGP protocol in the local AS. In this manner, the address of the ASBR in another AS becomes reachable and you can set up an LSP through the LDP.

The configuration procedure is as follows:

- Configuring Route Exchanging Between PEs and CEs
- Configuring an IGP and MPLS Signaling Protocol in an AS
- Configuring an ASBR to Cancel the Default RT Filtering Function
- Configuring PEs and ASBRs in the Same AS to Exchange VPN Routing Information

- Setting Up an MP-EBGP Session Between ASBRs
- Configuring Route Map Rules to Filter VPN Routers (Optional)
- Configuring an IGP to Redistribute ASBR Routes of Another AS

Configuring Route Exchanging Between PEs and CEs

This procedure is similar to Configuring Route Exchanging Between PEs and CEs and is not described here.

Configuring an IGP and MPLS Signaling Protocol in an AS

This procedure is similar to Configuring an MPLS Network and is not described here.

Configuring an ASBR to Cancel the Default RT Filtering Function

By default, a PE rejects a VPN route sent by another PE (or ASBR), if the route is not imported by any VRF on the PE. Therefore, you should disable the default filtering on an ASBR so that the ASBR can receive all VPN routes from others PEs (or ASBRs), no matter whether these routes are imported into the local VRF or not.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-number*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **no bgp default route-target filter**	Disable RT filtering.
DES-7200(config-router)# **show running-config**	View all configuration information.

Disable RT filtering.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 2
DES-7200(config-router)# no bgp default route-target filter
```

Configuring PEs and ASBRs in the Same AS to Exchange VPN Routing Information

This procedure is similar to Configuring PEs to Transmit VPN Routes and is not described here.

Setting Up an MP-EBGP Session Between ASBRs

Set up directly-connected single-hop MP-EBGP sessions between inter-AS ASBRs to advertise VPN routes.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-number*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *asbr-address* **remote-as** *asbr-asn-number*	Configure an ASBR EBGP session.
DES-7200(config-router)# **address-family vpnv4**	Enter the BGP VPN address family.
DES-7200(config-router-af)# **neighbor** *asbr-address* **activate**	Enable the VPN route exchange with the peer.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Configure an EBGP neighbor at 20.20.20.2 and activate the VPN address family.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 2
DES-7200(config-router)# neighbor 20.20.20.2 remote-as 1
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 20.20.20.2 activate
```

Caution

1. You must run the **label-switching** command on the interface that connects two ASBRs to enable MPLS on the interface so that the links between the ASBRs can forward MPLS packets.
2. If the ASBRs do not use directly connected addresses to set up an MP-EBGP session and use the loopback address with 32-bit mask length as the source address to set up an MP-EBGP session, you must use the **neighbor ebgp-multihop** command to enable multi-hop EBGP. At the same time, you must configure static routes on the ASBR to the loopback address on the peer, enable LDP or configure a static FTN (with an outgoing label as 3, indicating that the ASBR is the second but last hop).

Configuring Route Map Rules to Filter VPN Routes (Optional)

In view of the AS security in actual applications, you can generally configure policies on ASBRs to send or receive only certain VPN routers. You can realize this purpose by filtering the RT extended community attributes of VPN routes. In addition, all VPN routes are saved since the default RF filtering function is disabled on the ASBR. In this case, you can configure VPN route policies to receive only inter-AS VPN routes sent from the local AS, lessening the capacity pressure of the ASBR.

To configure a filtering policy, you should enter the privilege mode and perform the following configuration steps:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip extcommunity-list standard** *extcommunity-name* | *extcommunity-number* {**permit|deny**} **rt** *rt-value*	Create a rule for the extended community attribute list.
DES-7200(config)# **show ip extcommunity-list** [*list-number*|*list-name*]	Verify the configured rule for the extended community attribute list.
DES-7200(config)# **route-map** *route-map-name* **permit** [*number*]	Create a route map rule and enter the route map configuration mode.
DES-7200(config-route-map)# **match extcommunity** *extcommunity-name*|*extcommunity-number*	Set the RT matching rule for a route map.
DES-7200(config-route-map)# **show route-map** *route-map-name*	Display the route map rule.
DES-7200(config-route-map)# **exit**	Quit the route map configuration mode.
DES-7200(config)# **router bgp** *as-num*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **address-family vpnv4**	Enter the VPN address family.

DES-7200(config-router-af)# **neighbor** *peer-address* **route-map** *route-map-name* **in**	Filter the VPN routes received from the ASBR in another AS.
DES-7200(config-router-af)# **neighbor** *peer-address* **route-map** *route-map-name* **out**	Filter the VPN routes sent to the ASBR in another AS.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Configure an ASBR to receive VPN routes with an RT value of 100:1 from the MP-IBGP peer at 1.1.1.1.

```
DES-7200# configure terminal
DES-7200(config)# ip extcommunity-list standard RT permit rt 100:1
DES-7200(config)# show ip extcommuniy-list RT
  Named extended community standard list RT
  permit rt 100:1
DES-7200(config)# route-map RT-IN permit
DES-7200(config-route-map)# match extcommunity RT
DES-7200(config-route-map)# show route-map RT-IN
  route-map map, permit, sequence 10
  Match clauses:
  extcommunity (extcommunity-list filter):RT
  Set clauses:
  Policy routing matches: 0 packets, 0 bytes
DES-7200(config-route-map)# exit
DES-7200(config)# router bgp 100
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 100
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
DES-7200(config-router-af)# neighbor 1.1.1.1 route-map RT-IN in
DES-7200(config-router-af)# end
```

Configuring an IGP to Redistribute ASBR Routes of Another AS

Since the ASBR does not change the next hop of VPN routes sent to the IBGP peer, the next hop address of VPN routes learnt by the PEs in the local AS is the ASBR address in another AS. Therefore, you must configure the PEs to learn the route to the next hop address. For the single-hop directly-connected MP-EBGP session where BGP is enabled to carry labels (through IPv4 routes or VPN routes), the MP-BGP module supports the automatic generation of a host route with 32-bit mask length and FTN entry (with the outgoing label 3) on the ASBR. In this

manner, the tunnel egress is not terminated on the local ASBR. Therefore, as long as the ASBR redistributes the host route to the IGP in the local AS, the PEs can learn routes to the ASBR in the other AS.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router** *igp*	Enable an IGP that can be OSPF, RIP, or IS-IS.
DES-7200(config-router)# **redistribute connected subnets**	Redistribute directly connected network segment routes.
DES-7200(config-router)# **show running-config**	View all configuration information.

Configure the OSPF module on an ASBR to redistribute the directly connected network routes.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# redistribute connected subnets
```

Scheme 2: Next Hop Changed

When an ASBR receives VPN routes sent from the ASBR in another AS and sends the routes to the PEs in the local AS, the next hop of the routes is changed. This mode is called the "OptionB Next Hop Changed Scheme." In this mode, the PEs and ASBRs in the same AS can set up MP-IBGP sessions to exchange VPN routes. Two ASBRs can set up MP-EBGP sessions to exchange VPN routes. Upon receipt of a VPN route from another ASBR neighbor, an ASBR changes the next hop as its own address when notifying the MP-IBGP peer in the AS of the route.

The configuration procedure is as follows:

- Configuring Route Exchanging Between PEs and CEs
- Configuring an IGP and MPLS Signaling Protocol in an AS
- Configuring an ASBR to Cancel the Default RT Filtering Function
- Setting Up an MP-IBGP Session Between an ASBR and PE and Modifying the Next Hop Address as its Own Address

- Setting Up an MP-EBGP Session Between ASBRs
- Configuring Route Map Rules to Filter VPN Routes (Optional)

Configuring Route Exchanging Between PEs and CEs

This procedure is similar to Configuring Route Exchanging Between PEs and CEs and is not described here.

Configuring an IGP and MPLS Signaling Protocol in an AS

This procedure is similar to Configuring an MPLS Network and is not described here.

Configuring an ASBR to Cancel the Default RT Filtering Function

This procedure is similar to Configuring an ASBR to Cancel the Default RT Filtering Funtion in Scheme 1 and is not described here.

Setting Up an MP-IBGP Session Between an ASBR and PE and Modifying the Next Hop Address as its Own Address

By default, an ASBR does not modify the next hop of the VPN route received from an MP-EBGP peer when the ASBR sends the route to the MP-IBGP peer. You can configure the ASBR to forcibly modify the next hop of the VPN route to the ASBR address in the local AS. In this manner, the PEs in the local AS are not required to learn the address of the peer ASBR. This is the major difference with Scheme 1 (Next Hop Unchanged Scheme).

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-num*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *pe-address* **remote-as** *asn-num*	Set up an IBGP session with a PE.
DES-7200(config-router)# **neighbor** *pe-address* **update-source** *interface-name*	Specify the local loopback interface as the source address to set up an IBGP session.
DES-7200(config-router)#**address-family vpnv4**	Enter the BGP VPN address family configuration mode.

DES-7200(config-router-af)# **neighbor** *pe-address* **activate**	Enable the VPN route exchange with the peer.
DES-7200(config-router-af)# **neighbor** *pe-address* **next-hop-self**	Set the ASBR to modify the next hop as its own address when sending VPN routes to the IBGP neighbor.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Set up an MP-IBGP session, activate the VPN address family, and modify the next hop address as the ASBR address.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 1
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
DES-7200(config-router-af)# neighbor 1.1.1.1 next-hop-self
DES-7200(config-router-af)# end
```

Setting Up an MP-EBGP Session Between ASBRs

This procedure is similar to Setting Up an MP-EBGP Session Between ASBRs in Scheme 1 and is not described here.

Configuring Route Map Rules to Filter VPN Routes (Optional)

This procedure is similar to Configuring Route Map Rules to Filter VPN Routers (Optoinal) in Scheme 1 and is not described here.

2.3.2.3 OptionC: Multi-Hop MP-EBGP Mode

Both OptionA and OptionB can meet the networking requirements of inter-AS VPNs. In these two schemes, ASBRs are required to maintain and advertise VPN routes. If a large number of inter-AS VPN routes should be advertised in each AS, the ASBRs may become the bottleneck of further network expansion. To address this problem, a third scheme is developed, that is, the multi-hop MP-EBGP. In the multi-hop MP-EBGP mode, the PEs in different ASs set up multi-hop MP-EBGP sessions to directly exchange VPN routes. As a result, the ASBRs are not required to maintain or advertise VPN routes.

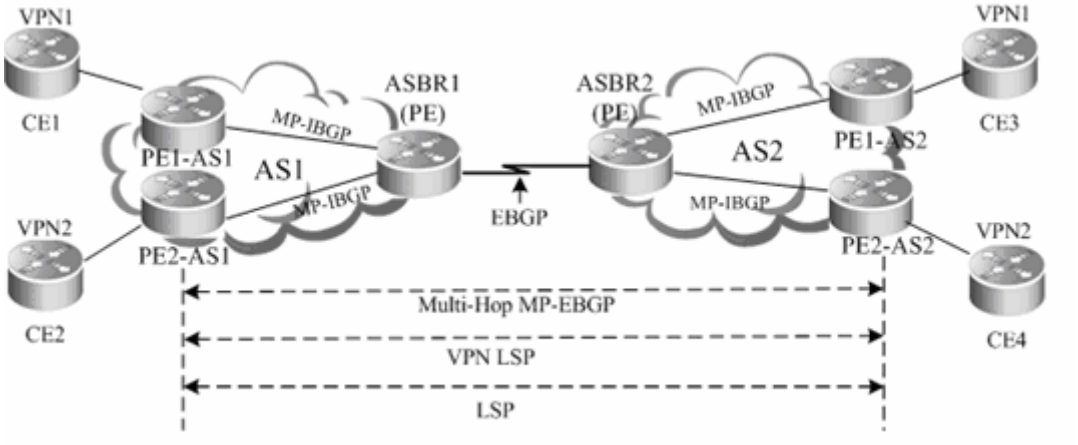


Figure 10 Multi-hope MP-EBGP

Characteristics and limitations

In the multi-hop MP-EBGP mode, only PEs rather than ASBRs are required to store VPN information. This incurs complex configurations. This scheme is applicable to networks to be deployed with inter-AS VPN services in a large scale.

In terms of implementation principle, OptionC is further classified into two modes:

Enable label exchanging of IPv4 routes only between EBGP neighbors.

Enable label exchanging of IPv4 routes between EBGP and IBGP neighbors.

To facilitate scale expansion in OptionC, each AS is generally deployed with a route reflector (RR). The RRs of two ASs set up multi-hop MP-EBGP sessions to exchange VPN routes. Judged from deployment, OptionC can be referred to as the scheme of "Multi-Hop MP-EBGP Session Setup Between RRs".

The following describes the configuration procedures of these solutions.

Scheme 1: Enabling label exchanging of IPv4 routes only Between EBGP Neighbors

In this scheme, the IGP (such as OSPF or RIP) that runs on an ASBR is required to redistribute BGP routes so that each device in the AS can have routes to the PE in another AS. In the AS, you can use the LDP to set up an LSP for label distribution with the PE in another PS. On the directly connected ASBRs of the two ASs, enable label exchanging of IPv4 routes. In this manner, BGP serves as the MPLS signaling to assign labels to the PE in another AS and set up an inter-AS LSP.

The configuration procedure is as follows:

- Configuring Route Exchanging Between PEs and CEs

- Configuring an IGP and MPLS Signaling Protocol in an AS
- Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routes
- Configuring an ASBR to Redistribute Inter-AS PE Routes Learnt from EBGP to the IGP
- Configuring a Multi-Hop MP-EBGP Session

Configuring Route Exchanging Between PEs and CEs

This procedure is similar to Configuring Route Exchanging Between PEs and CEs and is not described here.

Configuring an IGP and MPLS Signaling Protocol in an AS

This procedure is similar to Configuring an MPLS Network and is not described here.

Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routes

Set up an EBGP session between inter-AS ASBRs and enable label exchanging of IPv4 routes. To import PE routes to the BGP, you can use the **network** command in the BGP IPv4 address family mode or run commands to redistribute IGP routes. In view of the AS security in actual applications, you are generally required to configure IPv4 route distribution policies on ASBRs. By configuring route map rules, you can control the routes sent to neighbors and specify whether the routes carry labels. Similar control is available for receiving routes.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-num*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *asbr-address* **remote-as** *asbr-asn-num*	Set up an EBGP session with an ASBR.
DES-7200(config-router)#**address-family ipv4**	Enter the BGP IPv4 address family configuration mode.
DES-7200(config-router-af)# **neighbor** *asbr-address* **send-label**	Configure the device to exchange labeled IPv4 routes with the ASBR peer in another AS.
DES-7200(config-router-af)# **network** *pe-address* **mask** *mask*	(Optional) Configure PE addresses to be imported into the BGP routing table in the local AS, that is, host routes of each PE in the AS.

DES-7200(config-router-af)# **neighbor** *asbr-address* **route-map** *routemap-name* **out**	(Optional) Configure a route distribution policy to control the routes sent to neighbors and specify whether the routes can carry labels, by defining a route map rule.
DES-7200(config-router-af)# **neighbor** *asbr-address* **route-map** *routemap-name* **in**	(Optional) Configure a route distribution policy to receive only labeled routes by defining a route map rule.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Caution

1. You must run the **label-switching** command on the interface that connects two ASBRs to enable MPLS on the interface so that the links between the ASBRs can forward MPLS packets.
2. If the ASBRs do not use directly connected addresses to set up an MP-EBGP session and use the loopback address with 32-bit mask length as the source address to set up an MP-EBGP session, you must use the **neighbor ebgp-multihop** command to enable multi-hop EBGP. At the same time, you must configure static routes on the ASBR to the loopback address on the peer, enable LDP or configure a static FTN (with an outgoing label as 3, indicating that the ASBR is the second but last hop).

Set up an EBGP session between ASBRs, enable label exchanging of IPv4 routes, and run the **network** command to import PE routes to the BGP module.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 20.20.20.2 remote-as 2
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 20.20.20.2 send-label
DES-7200(config-router-af)# network 10.10.10.10 mask 255.255.255.255
DES-7200(config-router-af)# end
```

In actual applications, an ASBR is generally required to distribute labels for PE routes for only inter-AS VPN services. For this purpose, you can run the **set mpls-label** command in the route map mode.

The **set mpls-label** command sets labels for routes. You can create a route map rule to advertise only inter-PE routes to the peer ASBR and set labels for the routes. Set route map

rules and then run the **neighbor** *peer-address* **route-map** *rmap_name* **out** command in the BGP IPv4 address family mode to associate the rules with the route map.

In the following example, a route map is created to assign an MPLS label to the route with a prefix as 1.1.1.1/32, assign a common IPv4 route rather than label to only the route with a prefix as 1.1.1.2/32, and not to send neighbors routes that fail to match acl1 and acl2.

```
Router(config)# ip access-list standard acl1
Router(config-std-nacl)# permit host 1.1.1.1
Router(config-std-nacl)# exit
Router(config)# ip access-list standard acl2
Router(config-std-nacl)# permit host 1.1.1.2
Router(config-std-nacl)# exit
Router(config)# route-map out-as permit 10
Router(config-route-map)# match ip address acl1
Router(config-route-map)# set mpls-label
Router(config-std-nacl)# exit
Router(config)# route-map out-as permit 20
Router(config-route-map)# match ip address acl2
Router(config)# router bgp 100
Router(config-router)# neighbor 30.30.30.2 remote-as 100
Router(config-router)# neighbor 30.30.30.2 route-map out-as out
```

Similarly, to receive only labeled IPv4 routes, you can run the **match mpls-label** command in the route map mode. Set route map rules and then run the **neighbor** *peer-address* **route-map** *rmap_name* **in** command to associate the rules with the route map.

In the following example, a route map is created to receive labeled IPv4 routes from only the BGP peer at 30.30.30.2. The other routes are rejected.

```
Router(config)# route-map match-mpls
Router(config-route-map)# match mpls-label
Router(config)# router bgp 100
Router(config-router)# neighbor 30.30.30.2 remote-as 100
Router(config-router)# neighbor 30.30.30.2 route-map match-mpls in
```

Configuring an ASBR to Redistribute Inter-AS PE Routes Learnt from EBGP to the IGP

When an ASBR learn a route to the PE in another AS from the peer ASBR, the ASBR should inform other PEs in the local AS of the route. The ASBR should also set up an LSP to the PE in another AS. In this manner, the ASBR can redistribute routes learnt from EBGP to the IGP and at the same time, enable the LDP to assign labels to BGP routes and then set up an LSP to the PE in another AS.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router** *igp*	Enter the IGP configuration mode.
DES-7200(config-router)# **redistribute bgp subnets** [**route-map** *routemap-name*]	Redistribute BGP routes. Route filtering by using route map rules is optional.
DES-7200(config-router)# **exit**	Quit the IGP configuration mode.
DES-7200(config)# **mpls router ldp**	Enter the LDP configuration mode.
DES-7200(config-mpls-router)# **ldp router-id interface loopback** *0* **force**	Configure the LDP router ID. The loopback address is generally used as the router ID.
DES-7200(config-mpls-router)# **advertise-labels for bgp-routes** [**acl** *acl-name*]	Assign labels to BGP routes. ACL rules and filtering are optional.
DES-7200(config-mpls-router)# **show running-config**	View all configuration information.

Caution

By default, the LDP assigns labels to only IGP routes and does not assign labels to BGP routes. To assign labels to BGP routes, you can run the **advertise-labels for bgp-routes** command.

Configure an IGP and MPLS signaling in an AS.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# advertise-labels for bgp-routes
DES-7200(config-mpls-router)# end
```

When an IGP redistributes the learnt BGP routes in the OptionC scheme, you can run the **redistribute bgp subnets route-map** *routemap-name* command in the IGP configuration mode to control the BGP routes to be redistributed to the IGP. In the LDP configuration mode, you can

run the **advertise-labels for bgp-routes acl** *acl-name* command to control the labels assigned to BGP routes.

Configure ACL rules and route map routes so that:

The IGP redistributes only routes 1.1.1.1 and 2.2.2.2.

The LDP assigns labels to only routes 1.1.1.1 and 2.2.2.2.

The configuration procedure is as follows:

```
Router(config)# ip access-list extended 101
Router(config-ext-nacl)# permit ip host 1.1.1.1 any
Router(config-ext-nacl)# permit ip host 2.2.2.2 any
Router(config-ext-nacl)# exit
Router(config)# route-map pe-routes
Router(config-route-map)# match ip address 101
Router(config-route-map)# exit
Router(config)# router ospf 1
Router(config-router)# redistribute bgp subnets route-map pe-routes
Router(config-route-map)# exit
Router(config)# mpls router ldp
Router(config-mpls-router)# advertise-labels for bgp-routes acl 101
```

Configuring a Multi-Hop MP-EBGP Session

In the earlier steps, the inter-AS LSP is already set up. At this time, you can directly set up a multi-hop MP-EBGP session on the PE to be deployed with inter-AS VPN services with the PE in another AS. The session can then exchange VPN routes.

To configure a multi-hop MP-EBGP session, you should enter the privilege mode and perform the following configuration steps:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-num*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *ebgp-peer-address* **remote-as** *ebgp-asn-num*	Set up a multi-hop EBGP session with the PE in another AS.

DES-7200(config-router)# **neighbor** *ebgp-peer-address* **update-source** *interface-name*	Specify the device to use the loopback address to set up a neighbor relation with the EBGP peer.
DES-7200(config-router)# **neighbor** *ebgp-peer-address* **ebgp-multihop**	Configure multi-hop attributes.
DES-7200(config-router)#**address-family vpnv4**	Enter the BGP VPN address family configuration mode.
DES-7200(config-router-af)# **neighbor** *ebgp-peer-address* **activate**	Enable the VPN route exchange with the peer.
DES-7200(config-router-af)# **exit**	Quit the BGP VPN address family.
DES-7200(config-router)# **address-family ipv4**	Enter the BGP IPv4 address family configuration mode.
DES-7200(config-router-af)# **no neighbor** *ebgp-peer-address* **activate**	Disable the IPv4 route exchange.
DES-7200(config-router)# **show running-config**	View all configuration information.

Caution

The exchange of IPv4 routes is not required in a multi-hop MP-EBGP session. At least the routes of the two addresses used to set up the BGP session should be avoided. Otherwise, a PE has two routes to the PE in another AS. One route is advertised by the ASBR in the local AS and the other is by the multi-hop EBGP session. According to BGP specifications, the EBGP route has a higher priority over the IGBP route by default. As a result, the BGP module chooses the route advertised by the multi-hop BGP and this results in the continued flapping of routes on the PE to the PE in another AS. The VPN routes are thus not reachable.

Consider an example to set up a multi-hop EBGP session.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 2
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# neighbor 1.1.1.1 ebgp-multihop
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
DES-7200(config-router-af)# exit
```

```
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# no neighbor 1.1.1.1 activate
DES-7200(config-router-af)# end
```

Scheme 2: Enabling label exchanging of IPv4 routes Between EBGP and IBGP Neighbors

In Scheme 1 (**Enabling label exchanging of IPv4 routes Only Between EBGP Neighbors**), the IGP and LDP is one AS are required to maintain the PE routes from another AS. That is, inter-AS PE routes should be advertised to each device on the AS. In view of the AS security in actual applications, the PE routes of another AS are generally not advertised to each device on the local AS. Instead, these routes should be owned by the BGP protocol so that they can be transparent to the IGP and LDP in the local AS. You can enable label exchanging of IPv4 routes between EBGP and IBGP neighbors.

This scheme differs from Scheme 1 in that the IGP on an ASBR is not required to redistribute BGP routes and the LDP is not required to assign labels to BGP routes, though the LDP is still responsible for the setup of the LSP in the local AS. The setup of an inter-AS LSP, however, requires the label exchanging of IPv4 routes between both IBGP and EBGP neighbors. The PEs are also required to push three consecutive layers of labels.

The configuration procedure is as follows:

- Configuring Route Exchanging Between PEs and CEs
- Configuring an IGP and MPLS Signaling Protocol in an AS
- Setting Up an IBGP Session Between a PE and ASBR to Distribute Labels for IPv4 Routes
- Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routes
- Configuring a Multi-Hop MP-EBGP Session

Configuring Route Exchanging Between PEs and CEs

This procedure is similar to Configuring Route Exchanging Between PEs and CEs and is not described here.

Configuring an IGP and MPLS Signaling Protocol in an AS

This procedure is similar to Configuring an MPLS Network and is not described here.

Setting Up an IBGP Session Between a PE and ASBR to Distribute Labels for IPv4 Routes

This scheme differs from Scheme 1 mainly in this configuration procedure. In this scheme, the PE routes that are learnt by EBGP from another AS are not redistributed to the IGP in the local AS. Instead, the IBGP session between an ASBR and PE is used to transmit the PE routes of another AS and the BGP module is used to assign labels to the PE routes.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-number*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *peer-address* **remote-as** *asn-number*	Set up an IBGP session with an ASBR (PE).
DES-7200(config-router)# **neighbor** *peer-address* **update-source** *interface-name*	Configure the device to use the loopback address as the source address to set up the BGP session with an ASBR (PE) peer.
DES-7200(config-router)# **address-family ipv4**	Enter the IPv4 address family.
DES-7200(config-router-af)# **neighbor** *peer-address* **send-label**	Configure the device to exchange labeled IPv4 routes with an ASBR (PE) peer.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Caution

Before you enable the label exchanging of IPv4 routes for an IBGP session with an IBGP peer, run the **neighbor update-source** command to specify the source address of the IBGP session. This source address must be the address of the loopback interface; otherwise, the inter-AS LSP cannot be set up.

Configure a PE to set up an MP-IBGP session with the ASBR at 10.10.10.2.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 10.10.10.2 remote-as 1
DES-7200(config-router)# neighbor 10.10.10.2  update-source loopback 0
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 10.10.10.2 activate
DES-7200(config-router-af)# neighbor 10.10.10.2 send-label
```

```
DES-7200(config-router-af)# exit
```

Configure an ASBR to set up an MP-IBGP session with the PE at 10.10.10.1 in the local AS.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 10.10.10.1 remote-as 1
DES-7200(config-router)# neighbor 10.10.10.1 update-source loopback 0
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 10.10.10.1 send-label
DES-7200(config-router-af)# end
```

Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routes

This procedure is similar to Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routesin Scheme 1 and is not described here.

Configuring a Multi-Hop MP-EBGP Session

This procedure is similar to Configuring a Multi-Hop MP-EBGP Sessionin Scheme 1 and is not described here.

Scheme 3: Setting Up a Multi-Hop MP-EBGP Session Between RRs

In the traditional OptionC scheme, the inter-AS VPN sites should be connected in full mesh mode. The addition of a single VPN site requires the setup of MP-MBGP connections with the PEs in other ASs, hindering the expansion of VPN sites. In this case, you can deploy an RR in each AS to solve this problem. Set up multi-hop MP-EBGP sessions between the RRs to exchange VPN routes.

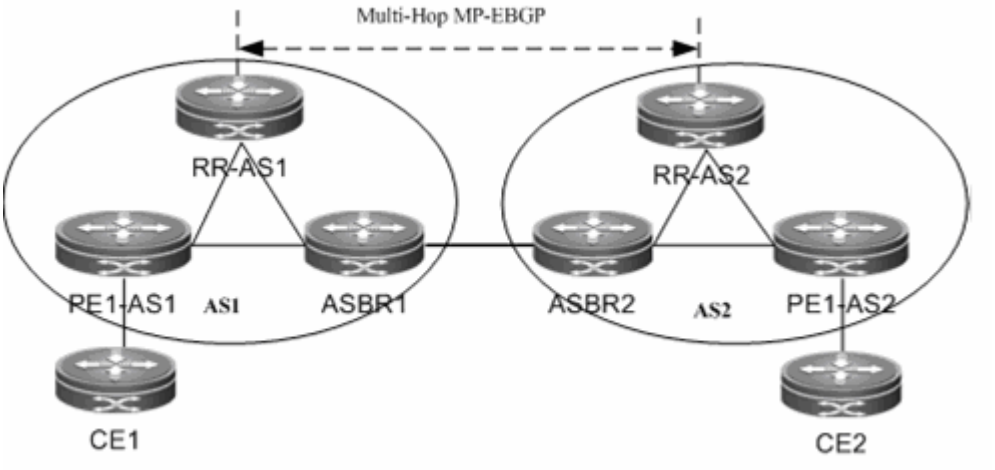


Figure 11 Setting up a multi-hop MP-EBGP session between RRs in OptionC mode

As shown in the preceding figure, the RRs in the two ASs set up a multi-hop MP-EBGP session to exchange VPN routes. The configuration procedure is as follows:

- Configuring Route Exchanging Between PEs and CEs
- Configuring an IGP and MPLS Signaling Protocol in an AS
- Setting Up an MP-IBGP Session Between the RR and PE to Exchange Labels Through IPv4 Routes
- Setting Up an IBGP Session Between the RR and ASBR to Assign Labels to IPv4 Routes
- Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routes
- Configuring a Multi-Hop MP-EBGP Session

Configuring Route Exchanging Between PEs and CEs

This procedure is similar to Configuring Route Exchanging Between PEs and CEsand is not described here.

Configuring an IGP and MPLS Signaling Protocol in an AS

This procedure is similar to Configuring an MPLS Network and is not described here.

Setting Up an MP-IBGP Session Between the RR and PE to Exchange Labels Through IPv4 Routes

Configure a PE to set up an MP-IBGP session with the RR to transmit VPN routes. At the same time, enable label exchanging of IPv4 routes for the session.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-number*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *peer-address* **remote-as** *asn-number*	Set up the IBGP session.
DES-7200(config-router)# **neighbor** *peer-address* **update-source** *interface-name*	Use the address of the loopback address as the source address to set up an IBGP session.

DES-7200(config-router)# **address-family ipv4**	Enter the IPv4 address family.
DES-7200(config-router-af)# **neighbor** *peer-address* **Activate**	Enable IPv4 route exchange.
DES-7200(config-router-af)# **neighbor** *peer-address* **send-label**	Enable label exchanging of IPv4 routes.
DES-7200(config-router-af)# n**eighbor** *peer-address* **route-reflector-client**	Configure all PE peers as the clients of the IPv4 RR.
DES-7200(config-router-af)# **exit**	Quit the IPv4 address family.
DES-7200(config-router)# **address-family vpnv4**	Enter the VPN address family.
DES-7200(config-router-af)# **neighbor** *peer-address* **Activate**	Enable the VPN route exchange with the peer.
DES-7200(config-router-af)# **neighbor** *peer-address* **route-reflector-client**	Configure all PE peers as the clients of the VPN RR.
DES-7200(config-router-af)# **show running-config**	View all configuration information.

Set up an MP-IBGP session between the RR and PE. The configuration on the RR is as follows:

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 10.10.10.1 remote-as 1
DES-7200(config-router)# neighbor 10.10.10.1 update-source loopback 0
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 10.10.10.1 activate
DES-7200(config-router-af)# neighbor 10.10.10.1 send-label
DES-7200(config-router-af)# neighbor 10.10.10.1 route-reflector-client
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 10.10.10.1 activate
DES-7200(config-router-af)# neighbor 10.10.10.1 route-reflector-client
DES-7200(config-router-af)# end
```

Setting Up an IBGP Session Between the RR and ASBR to Assign Labels to IPv4 Routes

Set up an MP-IBGP session between the ASBR and RR to receive routes from the RR to the PEs in the local AS and send routes from the RR to the PEs in another AS. At the same time, enable label exchanging of IPv4 routes for the session.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-number*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *peer-address* **remote-as** *asn-number*	Set up the IBGP session.
DES-7200(config-router)# **neighbor** *peer-address* **update-source** *interface-name*	Use the address of the loopback address as the source address to set up an IBGP session.
DES-7200(config-router)# **address-family ipv4**	Enter the IPv4 address family.
DES-7200(config-router-af)# **neighbor** *peer-address* **activate**	Enable IPv4 route exchange.
DES-7200(config-router-af)# **neighbor** *peer-address* **send-label**	Enable label exchanging of IPv4 routes.
DES-7200(config-router)# **show running-config**	View all configuration information.

Note

For the IBGP session between an RR and ASBR, you are generally not required to set the ASBR as the client of the RR unless the ASBR also serves as a PE.

Set up an IBGP session between the RR and ASBR. The configuration on the RR (the configuration on the ASBR is similar) is as follows:

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 10.10.10.2 remote-as 1
DES-7200(config-router)# neighbor 10.10.10.2 update-source loopback 0
```

```
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 10.10.10.2 activate
DES-7200(config-router-af)# neighbor 10.10.10.2 send-label
DES-7200(config-router-af)# end
```

Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routes

This procedure is similar to Setting Up an EBGP Session Between ASBRs to Exchange Labels Through IPv4 Routes in Scheme 1 and is not described here.

Configuring a Multi-Hop MP-EBGP Session

Set up a multi-hop MP-EBGP session between the RRs of two ASs to exchange inter-AS VPN routes. At the same time, disable the transmission of IPv4 routes for the session. The PE routes are advertised to another AS through the ASBR.

Enter the privilege mode and perform the following configuration procedure:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *asn-number*	Enable BGP and enter the BGP configuration mode.
DES-7200(config-router)# **neighbor** *rr-address* **remote-as** *ebgp-asn-numbe*	Set up the EBGP session.
DES-7200(config-router)# **neighbor** *rr-address* **update-source** *interface-name*	Use the address of the loopback address as the source address to set up an EBGP session.
DES-7200(config-router)# **neighbor** *rr-address* **ebgp-multihop**	Configure multi-hop EBGP attributes.
DES-7200(config-router)# **address-family ipv4**	Enter the IPv4 address family.
DES-7200(config-router-af)# **no neighbor** *rr-address* **activate**	Disable IPv4 route exchange for the session.
DES-7200(config-router-af)# **exit**	Quit the IPv4 address family.
DES-7200(config-router)# **address-family vpnv4**	Enter the VPN address family.

DES-7200(config-router-af)# **neighbor** *rr-address* **Activate**	Enable the device to exchange VPN routes with the RR in another AS.
DES-7200(config-router-af)# **neighbor** *rr-address* **next-hop-unchanged**	(Optional) Configure the device not to change the next hop when advertising VPN routes to the peer.
DES-7200(config-router)# **show running-config**	View all configuration information.

Note

1. By default, the device modifies the next hop of a route as its own address when advertising the route to an EBGP peer. Upon receipt of the VPN route, the PE site in another AS considers the next hop of the route as the RR. As a result, all inter-AS VPN traffic is transmitted through the RR. This is generally not the optimal forwarding path and has high requirements on the forwarding performance of the RR. To avoid the preceding situation, you can run the **neighbor next-hop-unchanged** command in the VPNv4 address family mode to configure the device not to change the next hop of a VPNv4 route sent to the BGP peer when you set up a multi-hop MP-EBGP session on the RR.

2. The exchange of IPv4 routes is not required in a multi-hop MP-EBGP session. At least the routes of the two addresses used to set up the BGP session should be avoided. Otherwise, a PE has two routes to the PE in another AS. One route is advertised by the ASBR in the local AS and the other is by the multi-hop EBGP session. According to BGP specifications, the EBGP route has a higher priority over the IGBP route by default. As a result, the BGP module chooses the route advertised by the multi-hop BGP and this results in the continued flapping of routes on the PE to the PE in another AS. The VPN routes are thus not reachable.

Configure an RR to set up a multi-hop MP-EBGP session with the RR in another AS.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 30.30.30.2 remote-as 2
DES-7200(config-router)# neighbor 30.30.30.2 update-source loopback 0
DES-7200(config-router)# neighbor 30.30.30.2 ebgp-multihop
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# no neighbor 30.30.30.2 activate
```

```
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 30.30.30.2 activate
DES-7200(config-router-af)# neighbor 30.30.30.2 next-hop-unchanged
DES-7200(config-router-af)# end
```

2.3.3 Configure Carrier's Carrier (CSC)

In a basic MPLS VPN, each site is a traditional IP network with simple network structure. However, in there are some special VPN users. For example, the VPN user itself is also a service provider who leases the VPN service of MPLS VPN service provider and then provides specific services for users. In such a case, the MPLS VPN service provider is called Provider Carrier or First Carrier, while the VPN user who is also a service provider is called Customer Carrier or Second Carrier. This networking model is called Carrier's Carrier (CSC).

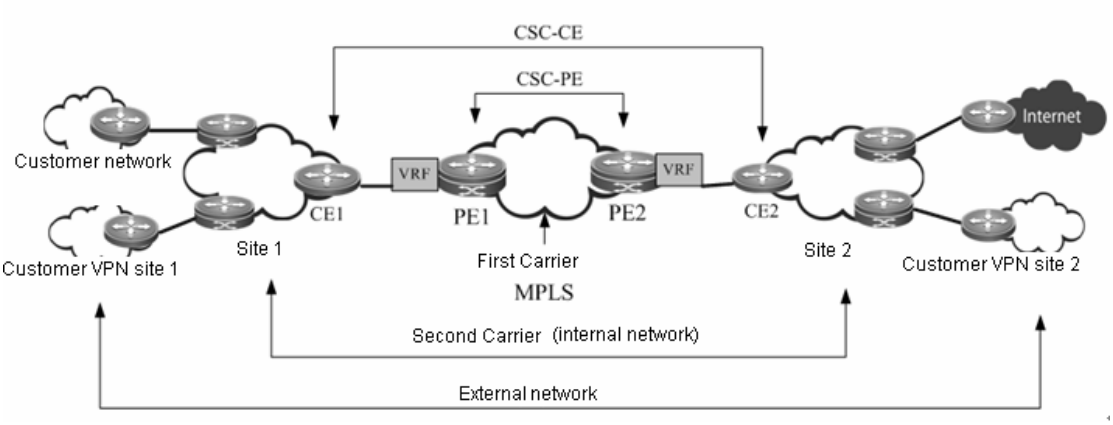


Fig 12 Model of Carrier's Carrier

2.3.3.1 Basic concepts

First Carrier

First Carrier is also called Provider Carrier, who provides MPLS VPN services for Second Carriers. In order to support Second Carriers to provide services for their users, the PE device of First Carrier must support CSC. The First Carrier PE providing services for Second Carriers is also called CSC-PE.

Second Carrier

Second Carrier is also called Customer Carrier, who leases the MPLS L3VPN service from First Carrier in order to build its own internal network and then provide services for users. The Second Carrier CE connecting to the First Carrier is also called CSC-CE.

Internal route

The internal routes refer to the routes inside the network of Second Carrier, namely the intra-AS routes. The internal routes are used to guarantee the intercommunication of Second Carrier's own network. Such routes must be jointly maintained by the First Carrier PE and the Second Carrier.

External route

Since the Second Carrier is a service provider, its network may be connected to multiple third-party networks. The route between Second Carrier and the third-party network is called external route. If the Second Carrier provides traditional IP service for users, then the external routes will include routes of user network; if the Second Carrier is connected to Internet, then the external routes will include Internet routes; if the Second Carrier provides MPLS VPN service for users, then the external routes will include user's VPN routes.

Generally, there are tremendous external routes. To maintain good scalability, the First Carrier will not maintain external routes, which will be maintained independently by the Second Carrier.

VPN tunnel

VPN tunnel is the LSP tunnel established between VPN devices. In the CSC model, the LSP tunnel between Second Carrier devices is the VPN tunnel.

2.3.3.2 Working principle

PE-CE route and label distribution

To achieve good scalability, the number of routes to be maintained by the First Carrier must be reduced. Therefore, the CSC model hands over external route maintenance to the Second Carrier, while the external traffic must use the VPN tunnel to cross First Carrier. To support CSC model, the First Carrier PE must support VPN tunnel.

To support VPN tunnel, the First Carrier PE (CSC-PE) and the Second Carrier CE (CSC-CE) must distribute the label binding information to each other. Depending on whether the CSC-PE and CSC-CE are in the same autonomous system, the following routing protocols may be used to exchange and distribute internal routes:

- If CSC-PE and CSC-CE are in the same autonomous system, IGP is generally used to exchange internal routes, and LDP is used to exchange label binding information.

- If CSC-PE and CSC-CE are in different autonomous systems, then EBGP is generally used to exchange internal routes, and EBGP IPv4 route/label distribution capability is also enabled to exchange internal routes and label binding information.

Typical application scenarios

The Second Carrier can be ordinary ISP or MPLS service provider. Depending on the type of Second Carrier network and the services provided by the Second Carrier for users, there are following typical application scenarios:

Scenario I: IP core second-level ISP

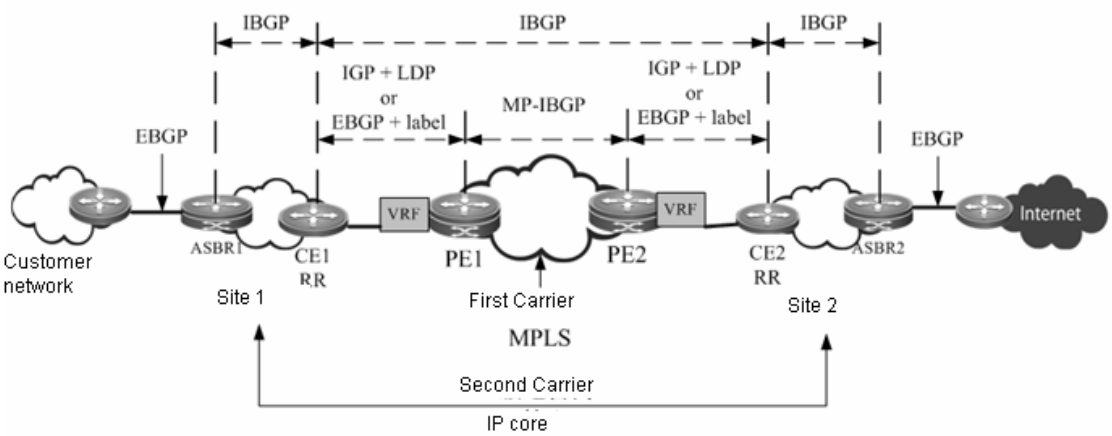


Fig 13 Scenario I: IP core second-level ISP

As shown in Fig 13, the Second Carrier is the IP core and provides network access service for users. Adjacencies are established between ASBR1, ASBR2, CE1 and CE2 to exchange external routes. CE1 and CE2 are Route Reflectors (RR) to reflect external routes between different sites. The Internet-access traffic of user flows from ASBR1 into the network of Second Carrier and then flows out of the Second Carrier network from ASBR2. When the traffic flows from CE1 to CE2, the traffic is forwarded in the VPN LSP tunnel.

Scenario II: MPLS core second-level ISP

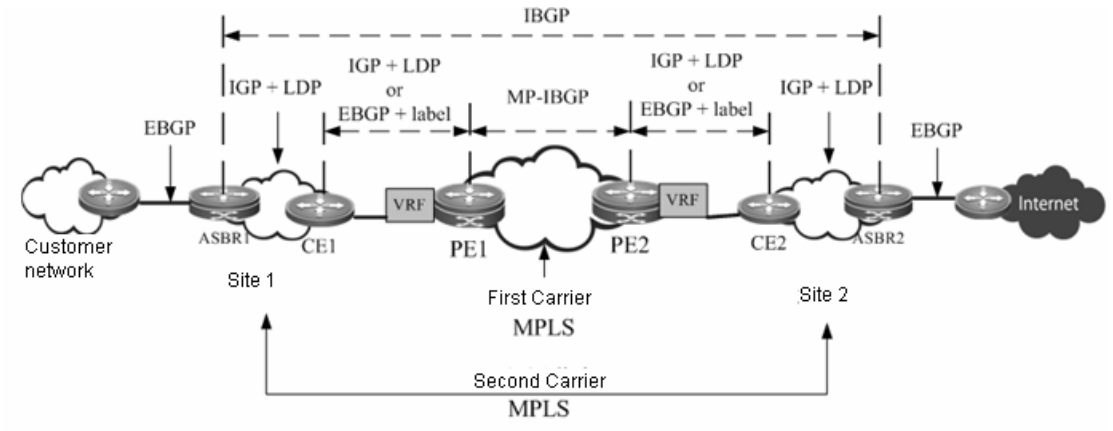


Fig 14 Scenario II: MPLS core second-level ISP

As shown in Fig 14, the Second Carrier is the MPLS core and provides network access service for users. Adjacency is established between ASBR1 and ASBR2 to exchange external routes. The Internet-access traffic of user flows from ASBR1 into the network of Second Carrier and then flows out of the Second Carrier network from ASBR2. When the traffic flows from ASBR1 to ASBR2, the traffic is forwarded in the VPN LSP tunnel.

Scenario III: MPLS core second-level VPN provider

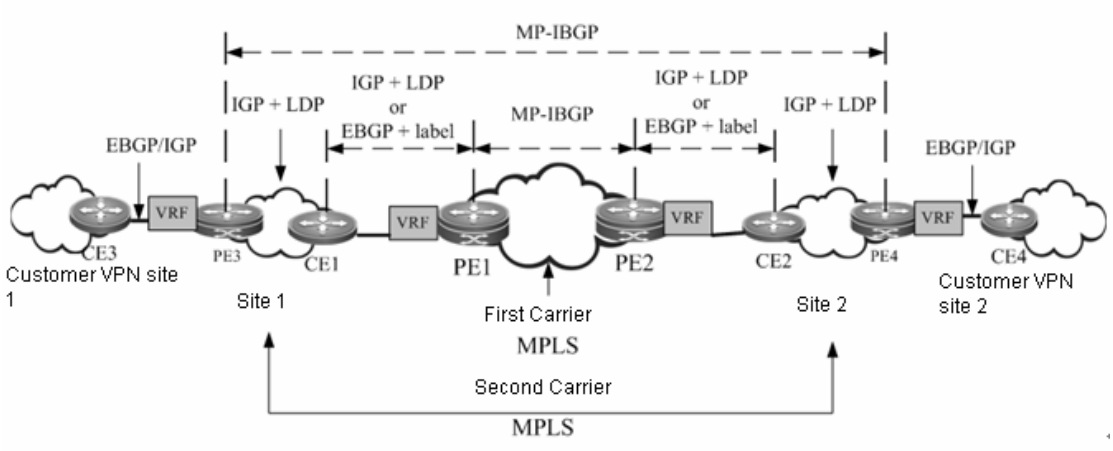


Fig 15 Scenario III: MPLS core second-level VPN provider

As shown in Fig 15, the Second Carrier is the MPLS core and provides MPLS L3VPN service for users. MP-IBGP adjacency is established between PE3 and PE4 to exchange user's VPN routes. The VPN LSP between PE3 and PE4 will act as the external tunnel of user VPN.

2.3.3.3 Configuration steps

CSC configuration involves:

- Configure basic BGP/MPLS VPN for First Carrier
- Configure First Carrier to enable CSC
- Configure Second Carrier
- Configure user access for Second Carrier

Configure basic BGP/MPLS VPN for First Carrier

The configuration of basic BGP/MPLS VPN involves:

- Configure MPLS network
- Configure VRF
- Configure MP-IBGP neighbor
- Configure route exchanging between PE and CE

Configure MPLS network

The configurations of this section is the same as "Configuring an MPLS network" in the previous section of "Configuring basic BGP/MPLS VPN Functions".

Configure VRF

The configurations of this section is the same as "Configuring a VPN routing instance" in the previous section of "Configuring basic BGP/MPLS VPN Functions".

Caution

CSC configuration requires "per-route" label allocation. Therefore, you need to execute "**alloc-label per-route**" command in VRF configuration mode to select the label allocation mode.

Configure MP-IBGP neighbor

The configurations of this section are the same as "Configuring PEs to Transmit VPN Routes" in the previous section of "Configuring basic BGP/MPLS VPN Functions".

Configure route exchanging between PE and CE

The configurations of this section is the same as "Configuring Route Exchanging Between PEs and CEs" in the previous section of "Configuring basic BGP/MPLS VPN Functions".

Caution

In Scenario I (Fig 13): In the network of IP core second-level ISP, if PE and CE use EBGP to exchange internal routes, and since the external routes are exchanged using BGP and CE is the route reflector, a route map needs to be configured for PE-CE to filter external routes and avoid leaking external routes into the PE of First Carrier.

Configure First Carrier to enable CSC

Configure on the First Carrier PE to enable CSC. Depending on the protocol used for exchanging routes between PE and CE, the following two cases may apply:

- PE and CE use LDP to distribute labels
- PE and CE use EBGP to distribute labels

PE and CE use LDP to distribute labels

If PE and CE use IGP to exchange routes, then execute the following commands on PE and CE respectively to configure PE and CE to use LDP to distribute labels.

The configuration steps of PE are shown below:

Command	Function
DES-7200(config)# **mpls router ldp** *vrf-name*	VRF to enable LDP (PE).
DES-7200(config-mpls-router)# **ldp router-id interface** *interface-name* **force**	Configure the RouterID of LDP.
DES-7200(config-mpls-router)# **advertise-labels for bgp-routes** [**acl** *acl-name*]	Configure to distribute labels for BGP routes. By default, LDP will not allocate labels for BGP routes.
DES-7200(config-mpls-router)# **exit**	Exit LDP instance configuration mode.

DES-7200(config)# **interface** *interface-name*	Configure the interface connecting CE.
DES-7200(config-if)# **label-switching**	Enable MPLS forwarding.
DES-7200(config-if)# **mpls ip**	Enable LDP.
DES-7200(config-if)# **ip ref**	In case of a router, enable fast forwarding (not applicable to a switch).
DES-7200(config-if)# **end**	Exit interface configuration mode.
DES-7200# **show running-config**	Display existing configurations.
DES-7200# **show mpls ldp bindings vrf** *vrf-name*	Display LDP label binding information under this VRF instance.

The configuration steps of CE are shown below:

Command	**Function**
DES-7200(config)# **mpls router ldp**	Enable LDP (CE).
DES-7200(config-mpls-router)# **ldp router-id interface** *interface-name* **force**	Configure the RouterID of LDP.
DES-7200(config-mpls-router)# **exit**	Exit LDP instance configuration mode.
DES-7200(config)# **interface** *interface-name*	Configure the interface connecting PE.
DES-7200(config-if)# **label-switching**	Enable MPLS forwarding.
DES-7200(config-if)# **mpls ip**	Enable LDP.
DES-7200(config-if)# **end**	Exit interface configuration mode.
DES-7200# **show running-config**	Display existing configurations.
DES-7200(config-if)# **ip ref**	In case of a router, enable fast forwarding (not applicable to a switch).
DES-7200# **show mpls ldp bindings**	Display LDP label binding information.

PE and CE use EBGP to distribute labels

If PE and CE use EBGP to exchange routes, then execute the following commands on PE and CE respectively to configure PE and CE to use EBGP to distribute labels.

The configuration steps of PE are shown below:

Command	Function
DES-7200(config)# **interface** *interface-name*	Configure the interface connecting CE.
DES-7200(config-if)# **ip ref**	In case of a router, enable fast forwarding (not applicable to a switch).
DES-7200(config-if)# **label-switching**	Enable MPLS on the interface.
DES-7200(config-if)# **router bgp** *asn*	Enter BGP configuration mode
DES-7200(config-router)# **address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode
DES-7200(config-router-af)# **neighbor** {*peer-address* | *peer-group-name*} **send-label**	Enable BGP to carry labels for IP routes
DES-7200(config-router-af)# **end**	Return to privilege mode
DES-7200# **show running-config**	Display existing configurations.
DES-7200# **show bgp vpnv4 unicast vrf** *vrf-name* **labels**	Display BGP label information

The configuration steps of CE are shown below:

Command	Function
DES-7200(config)# **interface** *interface-name*	Configure the interface connecting PE.
DES-7200(config-if)# **label-switching**	Enable MPLS on the interface.
DES-7200(config-if)# **ip ref**	In case of a router, enable fast forwarding (not applicable to a switch).
DES-7200(config-if)# **router bgp** *asn*	Enter BGP configuration mode

DES-7200(config-router)# **address-family ipv4**	Enter IPv4 address family configuration mode
DES-7200(config-router-af)# **neighbor** {*peer-address* | *peer-group-name*} **send-label**	Enable BGP to carry labels for IP routes
DES-7200(config-router-af)# **end**	Return to privilege mode
DES-7200# **show running-config**	Display existing configurations.
DES-7200# **show ip bgp labels**	Display BGP label information

Configure Second Carrier

Before configuration, please configure IGP for the Second Carrier network in order to guarantee the connectivity of Second Carrier network. Depending on the application scenarios of the Second Carrier, different configuration schemes will be adopted:

- Scenario I: IP core second-level ISP
- Scenario II: MPLS core second-level ISP
- Scenario III: MPLS core second-level VPN provider

Second Carrier provides Internet service based on IP core

In Scenario I, adjacencies are established between ASBRs and CEs to exchange external routes. CEs are route reflectors to reflect external routes between different sites. The configuration task mainly involves:

- Configure an intra-site BGP session
- Configure a BGP session between CSC-CEs of different sites
- Configure route map filtering

Configure an intra-site IBGP session

Configure an IBGP session between intra-site ASBR and CSC-CE, and configure CSC-CE as route reflector.

Command	Function
DES-7200(config)# **router bgp** *asn*	Configure BGP router

DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **remote-as** *asn*	Configure BGP neighbor
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **route-reflector-client**	Configure CSC-CE as the route reflector client
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **update-source** *interface-name*	Configure BGP source address
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **next-hop-self**	For ASBR, when configuring the router to advertise BGP routes, change the next hop to the router itself.

Configure an IBGP session between CSC-CEs of different sites

A fully meshed IBGP session is established between CSC-CEs of different sites to exchange external routes of different sites.

Command	Function
DES-7200(config)# **router bgp** *asn*	Configure BGP
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **remote-as** *asn*	Configure BGP neighbor
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **update-source** *interface-name*	Configure BGP source address
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **route-reflector-client**	(Optional) Configure the CSC-CE of peer site as the router reflector client.
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **next-hop-self**	When CSC-CE establishes a session with the CSC-CE of peer site, the next hop must be changed to itself.

Configure route map filtering

When BGP is used to exchange internal routes, since CSC-CE is responsible for both external route propagation and internal route propagation, we must guarantee that only the EBGP session between CSC-CE and CSC-PE can propagate internal routes, and the IBGP session

between CSC-CEs and between CSC-CE and ASBR can only propagate external routes, or else routing loop or chaos may incur. To achieve this goal, we must execute "**neighbor route-map {in | out}**" on IBGP neighbor and EBGP neighbor to filter the corresponding routes, and the AS-path filtering rule is generally used. Of course, you can also use other rules.

Command	Function
DES-7200(config)# **ip as-path access-list** *access-list-number* {**permit** | **deny**} *regex*	Configure AS-path ACL
DES-7200(config)# **route-map** *route-map-name* {**permit** | **deny**} *sequence-number*	Configure route map
DES-7200(config-route-map)# **match as-path** *access-list-number*	Match AS-path ACL
DES-7200(config-route-map)# **exit**	Exit global configuration mode
DES-7200(config)# **router bgp** *asn*	Configure BGP router
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **route-map** *route-map-name* {**in** | **out**}	Apply route map to BGP neighbor

Second Carrier provides Internet service based on MPLS

In Scenario II, the Second Carrier is a MPLS core network in which adjacencies are established between ASBRs to exchange external routes. There is no need to propagate external routes via CSC-CE. The configuration task mainly involves:

- Configure intra-site MPLS network
- Configure inter-site IBGP session

Configure intra-site MPLS network

The configuration of Second Carrier intra-site MPLS network is the same as "Configuring an MPLS network" in the previous section of "Configuring basic BGP/MPLS VPN Functions".

Note

You need to enable LDP on CSC-CE in order to establish sessions with other intra-site devices in order to build MPLS network. If CSC-CE and CSC-PE use BGP to exchange routes, then you must execute "**advertise-labels for bgp-routes**" on CSC-CE to allow LDP to distribute labels for BGP routes.

Configure IBGP session between ASBRs of different sites

Configure the BGP session between local ASBR and ASBR of peer site in order to exchange external routes.

Command	Function
DES-7200(config)# **router bgp** *asn*	Configure BGP
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **remote-as** *asn*	Configure BGP neighbor
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **update-source** *interface-name*	Configure BGP source address
DES-7200(config-router)# **neighbor** {*peer-address* | *peer-group-name*} **next-hop-self**	When configuring the ASBR router to advertise external routes, change the next hop to the router itself.

Note

To reduce the configuration cost of fully meshed IBGP session, the RR role can be configured inside the site. Intra-site ASBR can establish BGP session with RR, while inter-site BGP session will only be established between RRs.

Second Carrier provides VPN service based on MPLS core

In Scenario III, the Second Carrier is a MPLS core network in which MP-IBGP adjacencies are established between Second Carrier PEs to exchange user's VPN routes. The configuration task mainly involves:

- Configure intra-site MPLS network
- Configure MP-IBGP neighbor

Configure intra-site MPLS network

The configuration of Second Carrier intra-site MPLS network is the same as "Configuring an MPLS network" in the previous section of "Configuring basic BGP/MPLS VPN Functions".

Note

You need to enable LDP on CSC-CE in order to establish sessions with other intra-site devices in order to build MPLS network. If CSC-CE and CSC-PE use BGP to exchange routes, then you must execute "**advertise-labels for bgp-routes**" on CSC-CE to allow LDP to distribute labels for BGP routes.

Configure PEs to establish MP-IBGP neighbors

Configure to establish MP-IBGP sessions between intra-site PEs of respective Second Carriers and between PEs of different sites in order to propagate VPN private routes served by the Second Carriers. The configuration of Second Carrier PE is the same as the PE configuration in the section of "Configuring Basic BGP/MPLS VPN Functions".

Note

To reduce the configuration cost of fully meshed MP-IBGP session, the RR role can be configured inside the site. Intra-site PEs can establish MP-IBGP session with RR, while inter-site MP-IBGP session will only be established between RRs.

Configure user access for Second Carrier

The configurations in this section are related to the services provided by the Second Carrier, and have nothing to do with the "Carrier's Carrier" model. If the Second Carrier provides IP service for users, please refer to the section of IP routing configuration; if the Second Carrier provides MPLS VPN service for users, please refer to the section of MPLS VPN configuration.

2.3.4 Configure MPLS VPN Over GRE

Note

Currently, only router products of DES-7200 support MPLS VPN Over GRE. This feature is not supported by DES-7200's switch products.

2.3.4.1 Basic concepts

The traditional MPLS VPN uses Label Switching Path (LSP) as the public-network tunnel -- VPN traffic flows from upstream PE to the downstream PE by means of label switching -- this will require the carrier's core network to fully support MPLS. For certain considerations or due to certain limitations, if the carrier's core network cannot fully support MPLS, the MPLS VPN over GRE can provide a mechanism to allow the carrier to take GRE tunnel as a hop on the LSP tunnel, so as to guarantee the integrity of public-network LSP.

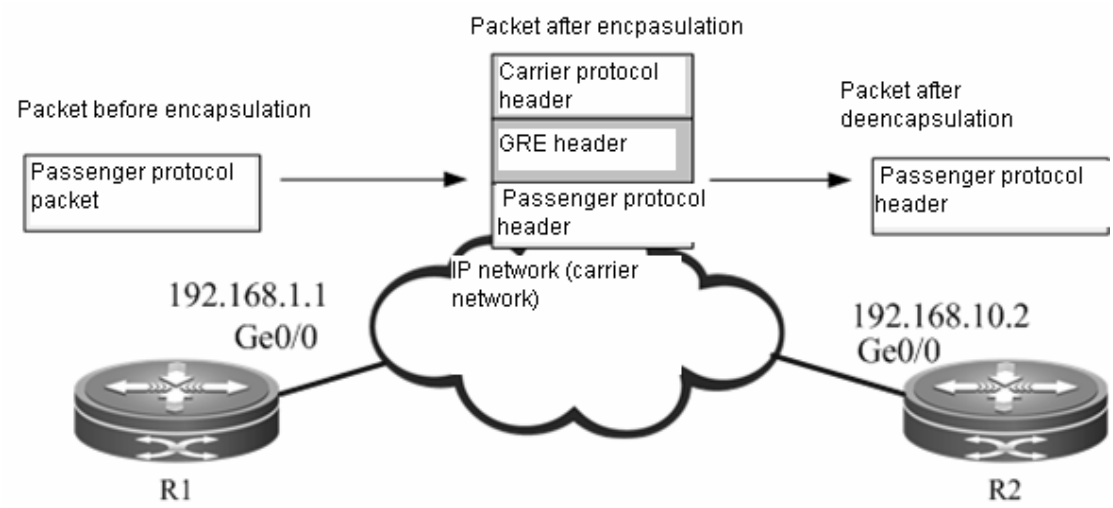


Fig 16 GRE tunnel

GRE tunnel

GRE (Generic Routing Encapsulation) provides a mechanism to encapsulate the packets of one protocol (passenger protocol) into another protocol (carrier protocol). The encapsulated packets consist of: carrier protocol header, GRE header and original passenger protocol header. After being encapsulated by the carrier protocol, the passenger protocol packets can then be forwarded in the carrier network. After the encapsulated packets reach the destination address of carrier protocol, the destination device will de-encapsulate the packets and then forward the packets according to the inner-layer passenger protocol used by packets. Such an encapsulation technology allows passenger protocol packets to cross heterogeneous carrier network and reach the destination device. It is a tunnel encapsulation technology.

Passenger protocol

Passenger protocol is the protocol being encapsulated during the process of GRE encapsulation. In the application scenario of MPLS VPN over GRE, the passenger protocol refers to packets carrying MPLS labels.

Carrier protocol

Carrier protocol is the protocol used to encapsulate passenger protocol during the process of GRE encapsulation. In the application scenario of MPLS VPN over GRE, the carrier protocol is generally IPv4.

Source address and destination address

While encapsulating the passenger protocol, we need to know the source address and destination address of carrier protocol, so that the encapsulated packets can be forwarded on the carrier network. The abovementioned source address and destination address are the source address and destination address of GRE tunnel.

Tunnel endpoint

When packets are transported on the tunnel, there is always one device carrying out carrier protocol encapsulation and another device carrying out de-encapsulation. The passenger protocol information can only be known and handled by these two devices, while other carrier network devices between them are unaware of the existence of passenger protocol. These two devices are the endpoints of GRE tunnel.

2.3.4.2 Working principle

In the traditional MPLS VPN, private-network traffic carrying inner-layer VPN label and outer-layer public-network label reaches the peer PE by means of label switching. When non-MPLS network exists in the backbone network, the LSP will become discontinuous. The GRE tunnel can help MPLS packets cross non-MPLS domain and realize continuous LSP.

GRE tunnel is a tunneling mechanism in IP network and support GRE with MPLS as the passenger protocol, so that two devices on both sides of the IP network can exchange MPLS packets. Considering GRE tunnel as a point-to-point logical link, devices at both ends of the tunnel directly establish IGP adjacency and LDP adjacency on this link to distribute routes and labels for LSP, while GRE tunnel becomes one hop of LSP.

MPLS as a passenger protocol

Take MPLS as the GRE tunnel of passenger protocol so that two devices interconnected through non-MPLS network can forward MPLS packets to each other. After label operation at one end of the tunnel, MPLS packets are encapsulated and then transported over the carrier network to the other end of tunnel; label switching is then carried out after packet de-encapsulation at the other end of tunnel. Fig 17 shows the format of encapsulated packets with IPv4 being the carrier protocol and MPLS being the passenger protocol.

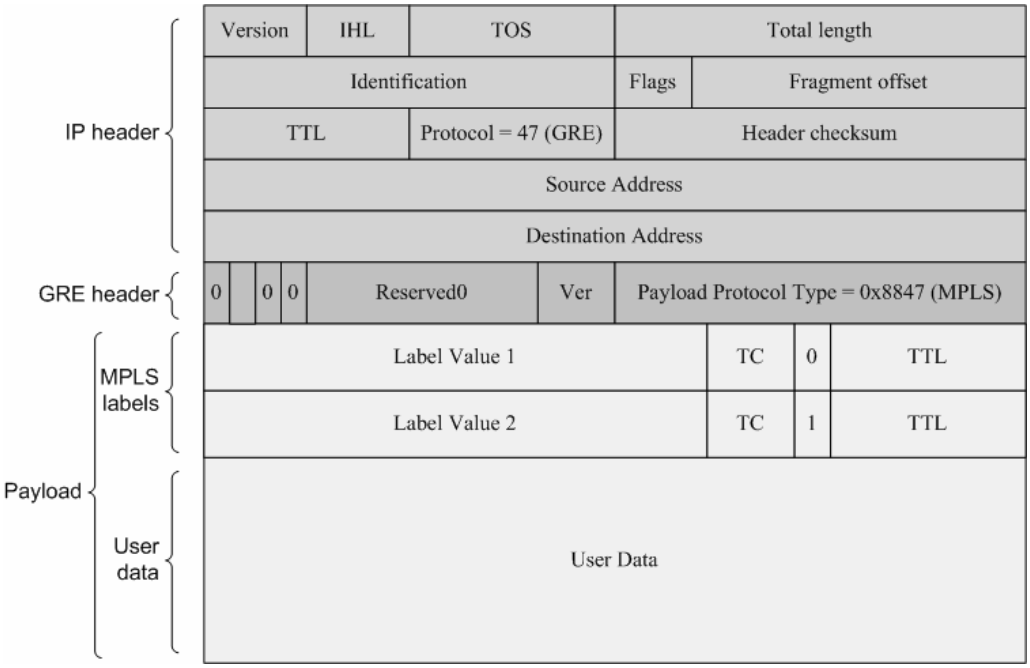


Fig 17 MPLS as the passenger protocol

GRE tunnel as a point-to-point link

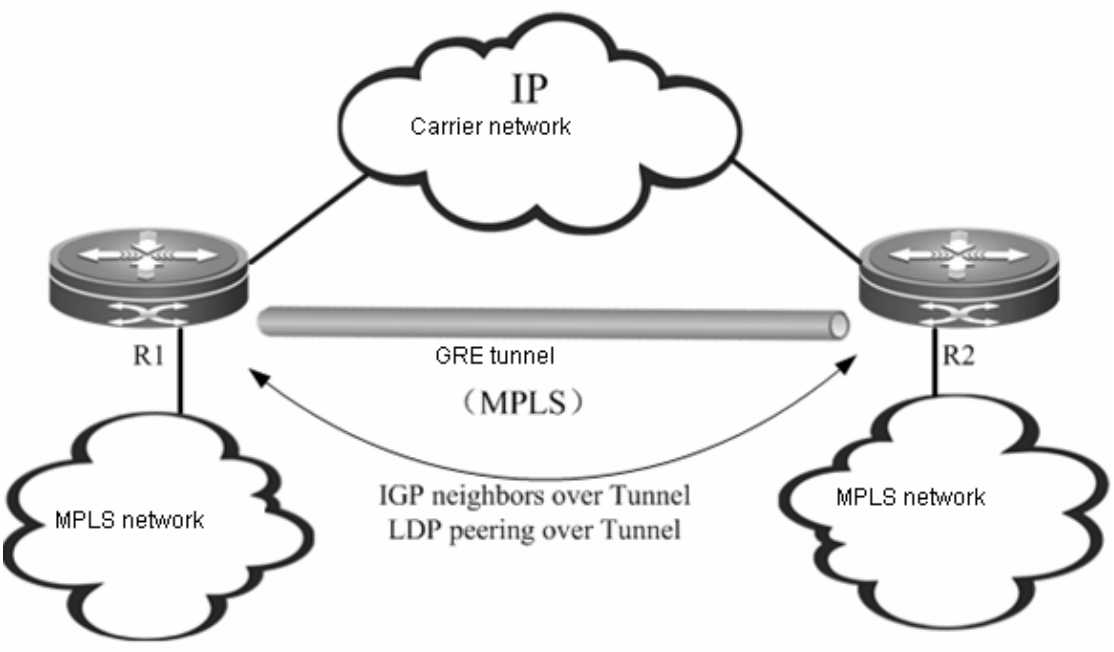


Fig 18 GRE tunnel link

As shown in Fig 18, R1 and R2 are connected to a MPLS network respectively, while both routers are interconnected via a carrier network (IP). The GRE tunnel allows both endpoints (R1 and R2) to use the carrier network (IP) to transmit MPLS packets, so that two separated MPLS networks can be connected. GRE tunnel is the point-to-point logical link between R1 and R2. It bypasses the carrier network (IP) and becomes one part of the MPLS network, so that the MPLS networks at both ends of the tunnel can maintain continuity. Considering GRE tunnel as a point-to-point link, IGP protocol can run on the link, while LDP can also distribute labels between R1 and R2.

Introduction of tunnel traffic

In either carrier network (IP) or MPLS network, the traffic forwarding is driven by router. Therefore, dynamic routing protocol needs to be run in the carrier network (IP) and MPLS network. There are two possible scenarios: single routing instance and dual routing instances.

Single routing instance

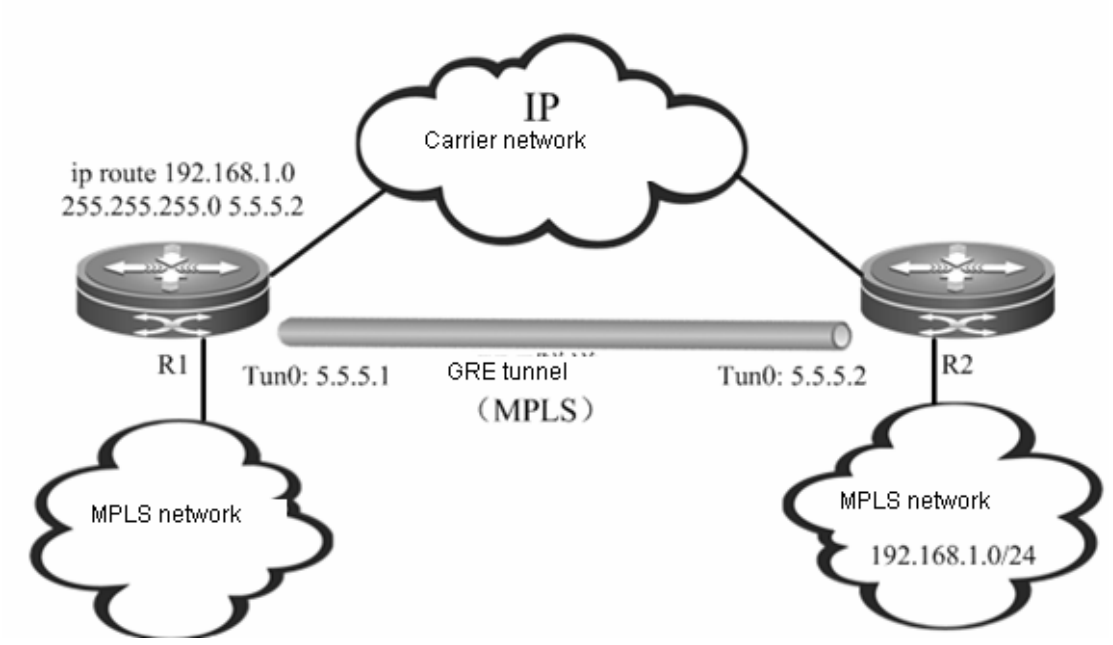


Fig 19 Single routing instance

In this scenario, MPLS network and carrier network (IP) are in the same routing instance, and the entire network is of plane form, as shown in Fig 19. By default, since the Metric value of GRE tunnel is far greater than the ordinary link, no traffic will be introduced into the GRE tunnel (which means GRE tunnel is not the next-hop interface of any route). Therefore, we must configure static routes in order to introduce MPLS traffic into the GRE tunnel. The static routes must be

configured in this scenario, and the number of static routes depends on the number of routing prefixes to be introduced into the GRE tunnel. The scalability is not satisfactory.

Dual routing instances

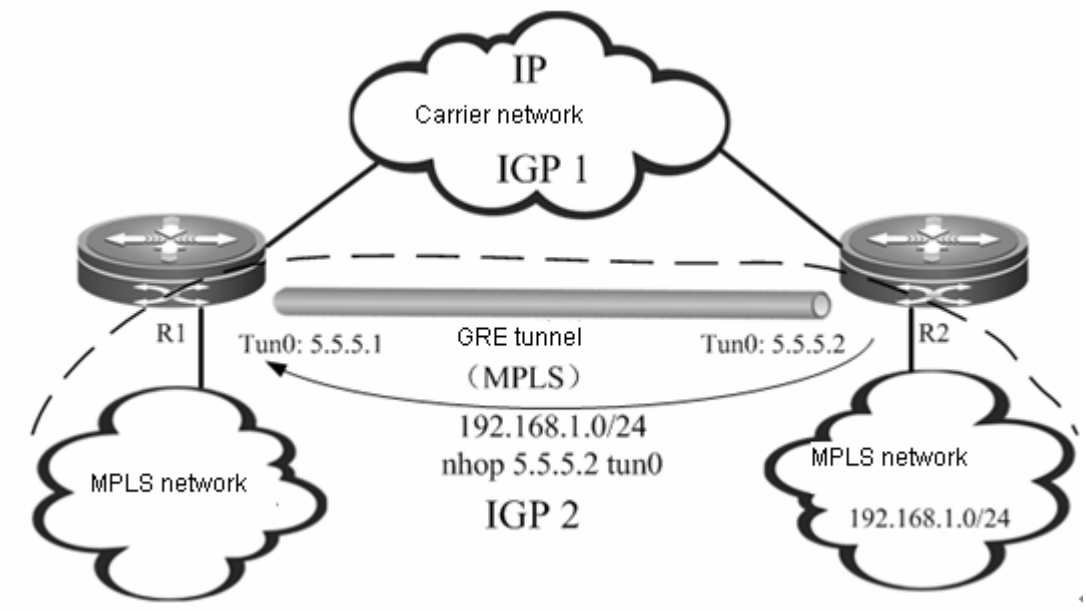


Fig 20 Dual routing instances

In this scenario, there are two different routing instances on each endpoint device of the GRE tunnel, as shown in Fig 20. One routing instance participates in route exchange in the carrier network (IP), while the other routing instance will participate in the route exchange in the MPLS network (including GRE tunnel link). By this time, R1 learns the route to remote MPLS network through GRE tunnel, with egress interface being GRE tunnel. The traffic can be introduced into GRE tunnel without configuring any static route.

Dual routing instances are actually dividing the network into different layers. As the upper-layer network, MPLS network (including GRE tunnel) acts as the backbone network running concurrent IGP instances, supporting MPLS and providing MPLS VPN service. As the bottom-layer network, the carrier network (IP) is the local network between R1 and R2 and runs independent IGP instances. If GRE tunnel is the "layer-3 interface" between R1 and R2, then the IP network and the IGP instance between R1 and R2 will be the "layer-2 network" and "layer-2 link protocol" between R1 and R2, as they guarantees the link state of GRE tunnel. Such relation can be indicated in Fig 21.

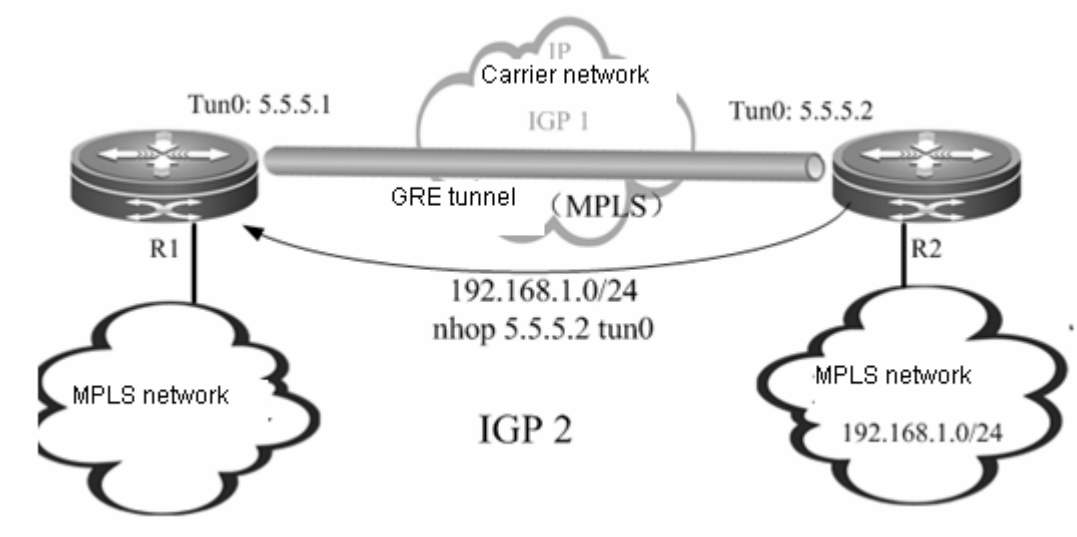


Fig 21 Dual IGP instances

The scenario of dual routing instances divides the network into different layers and boasts better scalability. The following example is mainly based on this scenario.

Typical application

Establish a GRE tunnel between PEs

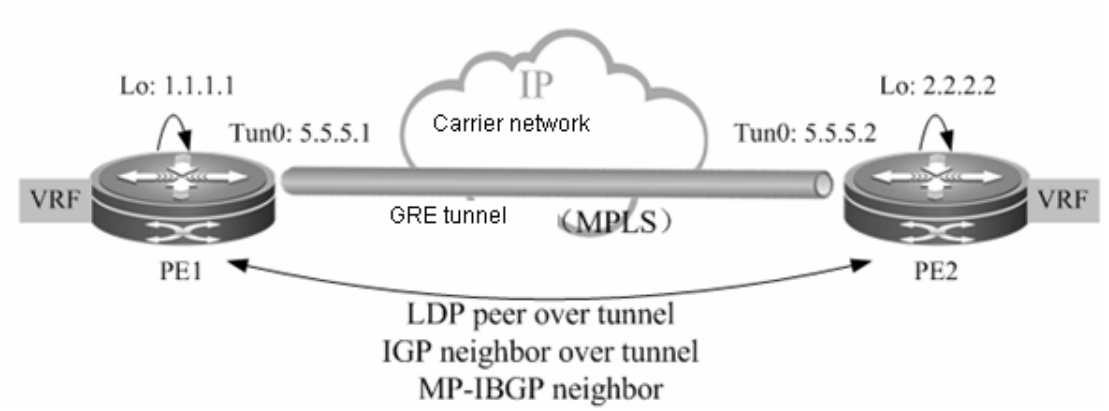


Fig 22 Scenario I: PE-PE

As shown in Fig 22, the core network between PEs is completely an IP network. GRE tunnel is established between two PEs, and the LSP between PE1 and PE2 has only one hop.

Establish a GRE tunnel between Ps

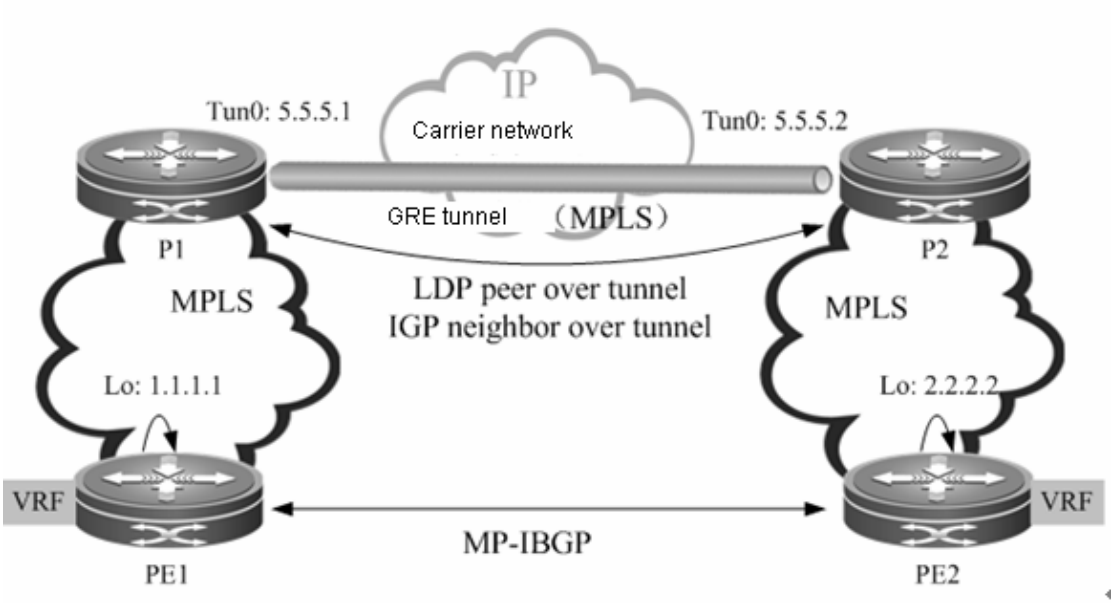


Fig 23 Scenario II: P-P

As shown in Fig 23, PE1 and PE2 are in two MPLS domains. P1 and P2 are interconnected through IP network. The GRE tunnel is established between P1 and P2. The public-network LSP between PE1 and PE2 goes through P1 and P2, and the GRE tunnel between P1 and P2 is one hop of LSP.

Establish a GRE tunnel between P and PE

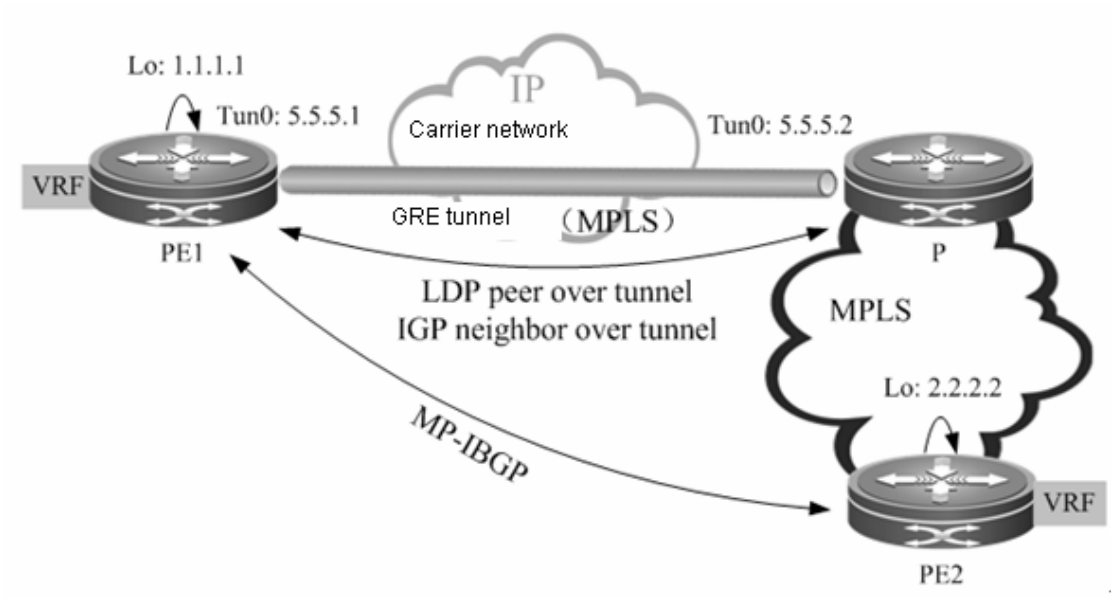


Fig 24 Scenario III: P-PE

As shown in Fig 24, the network between PE1 and P doesn't support MPLS. The LSP is connected by establishing a GRE tunnel between PE1 and P device.

2.3.4.3 Protocol specification

- RFC 4023: Encapsulating MPLS in IP or GRE.
- RFC 4797: Use of Provider Edge to Provider Edge (PE-PE) Generic Routing Encapsulation (GRE) or IP in BGP/MPLS IP Virtual Private Networks.

2.3.4.4 Configuration steps

The configuration of MPLS VPN over GRE involves:

- Create tunnel interface
- Configure IGP route
- Configure MPLS network
- Configure MPLS VPN

Create tunnel

Execute the following command to create GRE tunnel (interface).

Command	Function
DES-7200(config)# **interface tunnel** *tunnel-id*	Create tunnel interface.
DES-7200(config)# **tunnel mode gre ip**	Configure the tunnel as GRE in IP tunnel.
DES-7200(config-if)# **ip address** *ip-address address-mask*	Configure the address for tunnel interface.
DES-7200(config-if)# **tunnel source** {*ip-address* | *interface-name*}	Configure the source address of GRE tunnel.
DES-7200(config-if)# **tunnel destination** *ip-address*	Configure the destination address of GRE tunnel.
DES-7200(config-if)# **no shutdown**	Enable interface.

Configure the route to introduce traffic into the tunnel

There are two ways to introduce traffic into the tunnel, including:

Configure IGP

Configure static route

Configure IGP

Generally, multiple OSPF processes are used to create different routing instances. One OSPF process learns the route to reach the destination address of tunnel, and the tunnel interface will become "UP" if the route is reachable. Another OSPF process will run OSPF on the GRE tunnel to establish session in order to learn the route to destination address of PE. For the configuration steps of multiple OSPF processes, please refer to the section about unicast routing protocol configuration.

Configure static route

Configure static route directly: configure tunnel interface as the next hop of the route to the specified PE address.

Command	Function
DES-7200(config)# **ip route** *ip-address address-mask* **tunnel** *tunnel-id*	Configure static route.

Caution

If static route is used to introduce traffic into the tunnel, then the destination address of tunnel cannot be the routing prefix of static route, namely the address of specified PE and the destination address of tunnel must be different. This is because the state of tunnel interface depends on the route to the destination address of tunnel, while the static route will cause the route to such destination address to rely on the state of tunnel interface, thus leading to the state oscillation of tunnel interface.

Configure tunnel interface to enable MPLS

Enable LDP protocol on the tunnel interface and enable MPLS forwarding function.

Command	Function

DES-7200(config)# **mpls ip**	Enable MPLS globally.
DES-7200(config)# **mpls router ldp**	Enable LDP globally.
DES-7200(config-mpls-router)# **ldp router-id interface** *interface-name*	Configure the RouterID of LDP.
DES-7200(config-mpls-router)# **exit**	Exit LDP configuration mode.
DES-7200(config)# **interface tunnel** *tunnel-id*	Enter tunnel interface configuration mode.
DES-7200(config-if)# **ip ref**	In case of a router, enable fast forwarding (not applicable to a switch).
DES-7200(config-if)# **mpls ip**	Enable LDP on the interface.
DES-7200(config-if)# **label-switching**	Enable MPLS forwarding on the interface.
DES-7200(config-if)# **exit**	Exit interface configuration mode.

Note

Currently, only router products support MPLS VPN Over GRE-in-IPv4 tunnel. This feature is not supported by switch products.

Configure MPLS VPN

The configuration of MPLS VPN involves:

- Configure VRF
- Configure MP-IBGP
- Configure route exchanging between PE and CE

The configurations are detailed in the section of "Configuring Basic BGP/MPLS VPN Functions".

2.3.5 Configure OSPF VPN extension

2.3.5.1 Introduction to L3VPN OSPF VPN extension

PE-CE OSPF feature

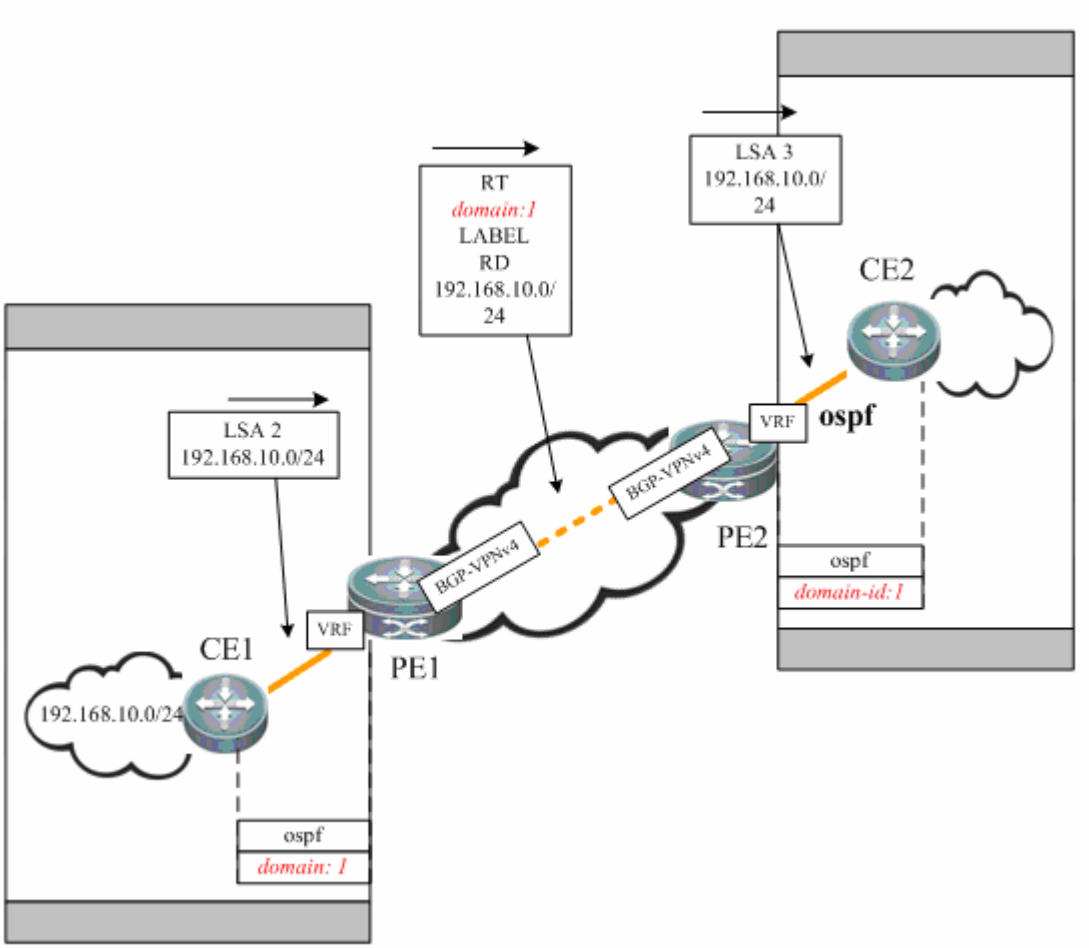
OSPF is widely applied IGP protocol. In most of the existing application scenarios, VPN user generally selects OSPF as the interior routing protocol. If OSPF protocol is deployed between PE and CE, you won't have to run other routing protocols again, thus simplifying CE configuration and management.

PE-CE OSPF feature will be introduced from the following four aspects.

Domain ID

Domain ID refers to the OSPF domain to which the route belongs. When CE has learned an OSPF route from interior site of VPN, this route will be advertised to PE in type-1, type-2 or type-3 LSAs and redistributed to BGP to form VPN route. Meanwhile, the domain ID will also be redistributed to BGP together with the route and advertised as the Extended Communities attribute in the VPN route. When other PEs receive this VPN route and redistribute to the VRF OSPF instance, the domain ID will also be redistributed to the corresponding VRF OSPF instance together with this route. If VRF OSPF instance confirms that domain ID contained in the route is same as the domain ID of this VRF OSPF instance, then the route will be advertised to CE as an internal route. Contrarily, if VRF OSPF instance confirms the domain ID contained in the route is different from the domain ID of this VRF OSPF instance, then the route will be advertised to CE as an external route.

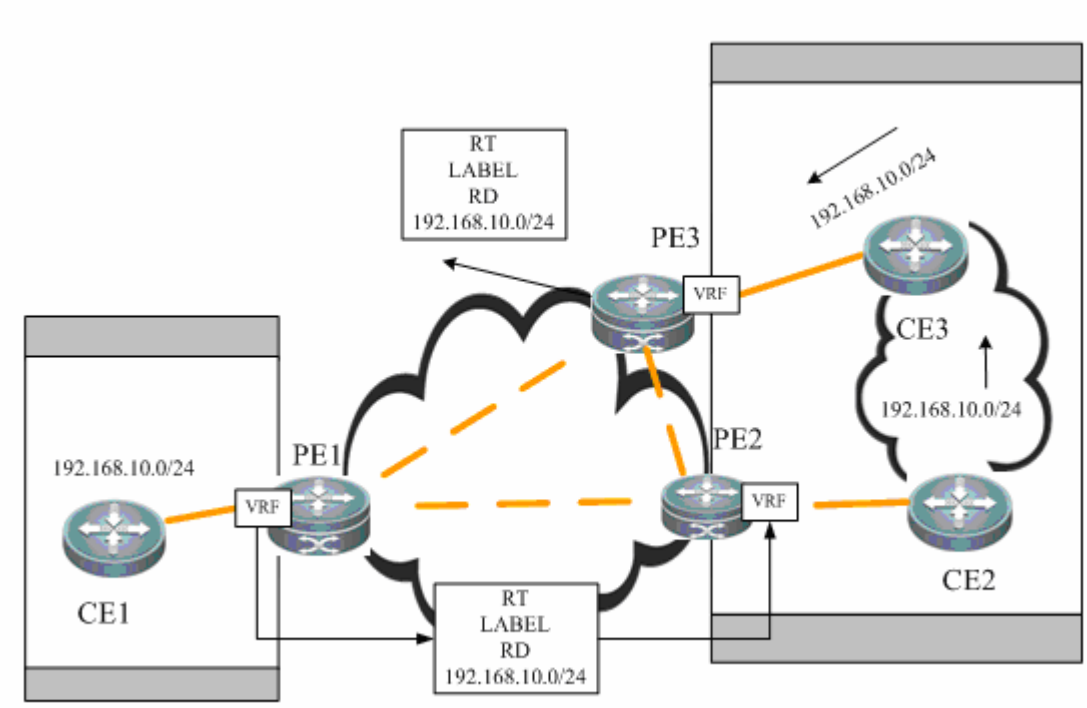
As shown below, for a route that belongs to the same OSPF domain, CE1 advertises the route to PE1 in type-2 LSA and then VPN route is formed and advertised to PE2, which will receive this route and redistribute to VRF OSPF instance. Since the VRF OSPF instance shares the same domain ID with this VPN route, this site will eventually be advertised to VPN sites in the form of internal route.



DN bit

DN bit is a loop detection technique when OSPF protocol is run between PE and CE. In certain circumstance, running OSPF between PE and CE may cause loops. For example, when multiple PEs are connected to one VPN site, if one PE advertises the VPN route learned to the VPN site, and such route is further advertised to another PE by running OSPF protocol inside the VPN site and then broadcasted, routing loop may take place.

As shown below: The route from 192.168.10.0/24 is advertised by PE1 to PE2 and PE3. CE2 advertises the route to CE3 through OSPF protocol. The route is then advertised to PE3 and redistributed to the BGP protocol of PE3. PE3 selects the protocol redistributed by OSPF and converts this route into VPN-IPV4 route before advertisement, thus causing routing loop.



To avoid such potential loop, when PE advertises type-3, type-5 or type-7 LSAs to CE, it will set DN bit in the optional field of LSA. When other PE sites receives any LSA containing DN bit in the optional field, the OSPF protocol on PE won't allow this LSA to participate in OSPF computation.

VPN route tag

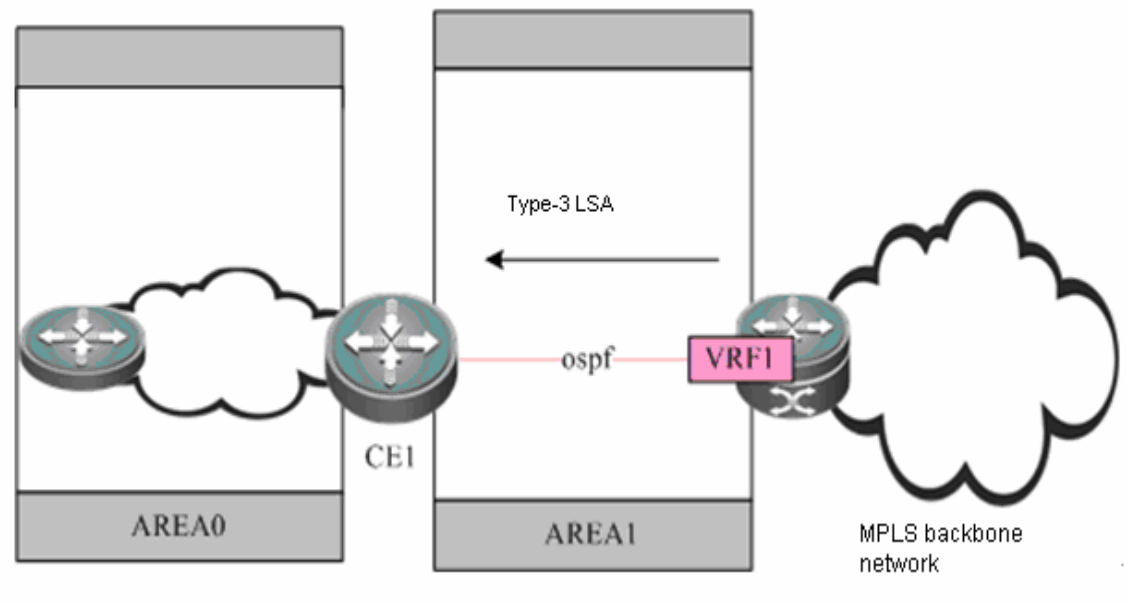
VPN route tag is another loop detection technique. When OSPF protocol is run between PE and CE, the corresponding VRF OSPF instance on PE will by default have a route tag called "VPN route tag". The VRF OSPF instance on PE introduces VPN route and converts the route into type-5 or type-7 LSA. When LSA is advertised to CE, this LSA will carry VPN route tag. In the circumstance in which one VPN site is connected with multiple PEs, if PE receives a type-5 or type-7 LSA that carries VPN route tag and this VPN route tag is the same as the that of OSPF instance, then this LSA won't participate in OSPF route calculation.

PE-CE inter-area deployment

Under normal circumstances, the link between PE and CE can be in any OSPF area. However, if the link between PE-CE falls into a non-0 area, then PE is an ABR to the OSPF area where the CE is in. This may cause some problems as the OSPF protocol acting as ABR device has the following features:

- ABR only calculates the type-3 LSA in the backbone area
- ABR only forwards type-3 LSA in the backbone area to the non-backbone area

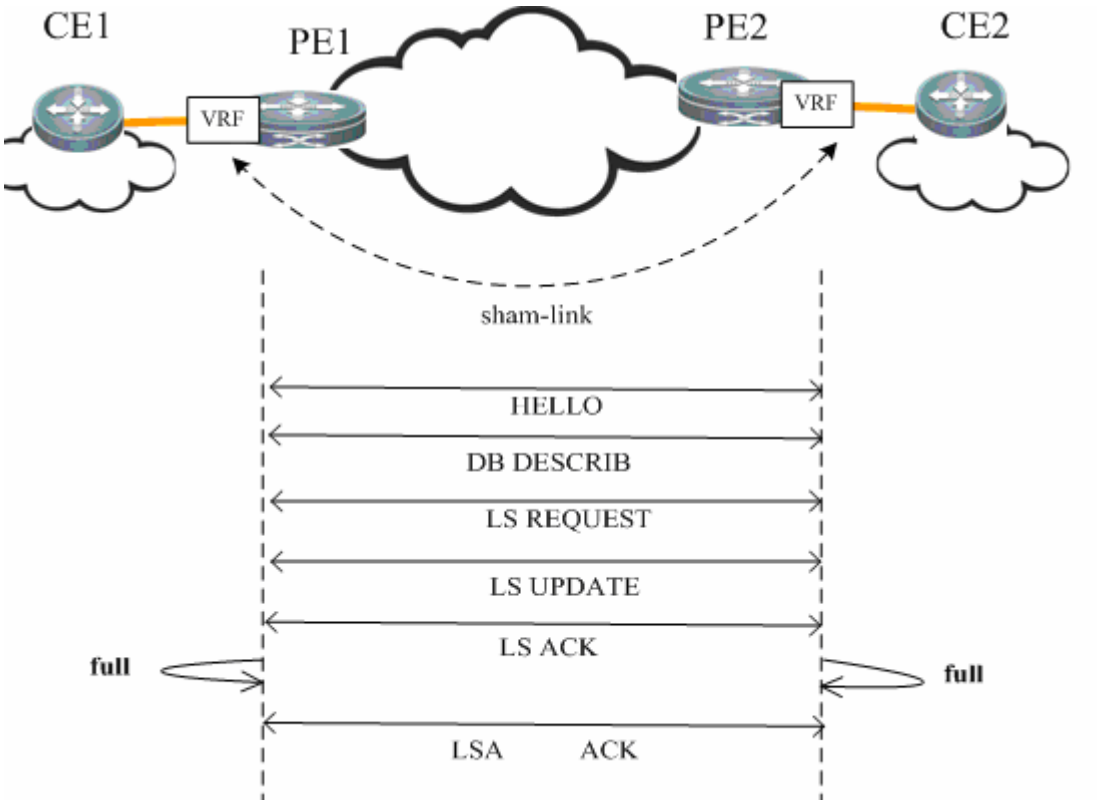
As shown below, if the link between PE and CE is in non-0 area, then PE will redistribute the VPNv4 route advertised by MP-BGP to OSPF and restore to type-3 LSA to be advertised to CE1, which will not calculate the non-backbone area LSAs. Therefore, these LSAs will not be advertised to routers in Area0, and intra-VPN sites won't learn the route to other sites. Accordingly, special attention shall be paid when deploying non-0 area between PE and CE.



Generally, in L3VPN applications, if OSP protocol is run between PE and CE to exchange VPN routes, it is suggested not to deploy backbone area at intra-VPN site. In practice, if intra-VPN routers other than the PE sites also fall into the backbone area, then there must be at least one router at this intra-VPN site to connect with PE, and the link between CE and PE must belong to Area 0, so that intra-area routes and external routes can be propagated between PE and VPN site.

Sham link

Sham-link is not a real link. It refers to the "virtual link" established between the VRFs of two PEs. The Sham-link is same as the normal OSPF link. With its own OSPF interface, it can send OSPF protocol packets, establish neighbors and send LSAs. When LSAs are flooded over the sham link, all OSPF route types won't be changed, as shown below.



The purpose of establishing sham-link between VRF OSPF instances on different PEs include:

- The approach of using MP-IBGP to carry private-network route will only propagate the route, and the restoration work after reaching the peer PE is only to introduce the original OSPF routing information as far as possible, during which the OSPF topology information cannot be truly communicated. By establishing an OSPF link through sham-link, all OSPF instances inside each site can be truly connected and work out all-round topology information.

- Different sites in the same VPN exchanges information via MPLS backbone network, but a link is established between VPN sites so that VPN sites can still communicate via this link when MPLS backbone network fails. This link is called the "backdoor link". If two sites of VPN user fall into the same OSPF area and there is a "backdoor link" connecting these two sites, then routes will be exchanged via both MPLS backbone network and the "backdoor link". Since the routes exchanged via MPLS backbone network are inter-area routes and the routes exchanged via the "backdoor link" are intra-area routes, and the intra-area routes are apparently superior to inter-area routes, the route forwarding between two sites will hence use the backdoor link. This goes against the purpose of establishing "backdoor link". Therefore, the sham link shall be used in such applications.

Protocol specification

RFC4576 and RFC4577 describe the mechanism to realize L3VPN OSPF.

2.3.5.2 Default configurations

Function	Default setting
domain-tag	AS ID local BGP
domain-id	Default value: NULL; default type: 0x0005
capability vrf-lite	By default, PE-CE OSPF feature is supported by VRF OSPF instance
extcommunity-type	In the OSPF instance Extended Communities attribute carried by BGP: the default type of route-id is 0x0107, and the default type of route-type is 0x0306.

2.3.5.3 Configure domain ID (optional)

Domain ID is used to indicate the domain to which the OSPF instance belongs. Generally, all VRF OSPF instances belonging to the same VPN shall be configured to the same domain ID. The configuration steps are shown below:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **router ospf** *ospf-id* **vrf** *vrf-name*	Create OSPF instance and enter OSPF configuration mode
DES-7200(config-router)# **domain-id** *value* **[secondary]**	(Optional) Configure the domain ID of OSPF instance. The OSPF domain ID is 0 by default.
DES-7200(config-router)# **show running-config**	Display existing configurations.

Note

- This command is only applicable to OSPF instance associated with VRF.
- VRF OSPF instance can be configured with multiple domain IDs, but there is only one primary domain ID. Others are secondary domain IDs. The only primary domain ID is configured with "**domain-id** *value*" command, while multiple secondary domain IDs are configured with "**domain-id** *value* **secondary**" command. OSPF routes are advertised when converted to VPN routes, and VPN routes only contain the primary domain ID.
- Different VRF OSPF instances can have the same domain ID. However, VRF OSPF instances in the same VPN must be configured with the same domain ID in order to guarantee the correctness of route advertisement.

Configure the primary domain ID and secondary domain ID of VRF OSPF protocol to 4.4.4.4 and 5.5.5.5 respectively.

```
DES-7200# configure terminal

DES-7200(config)# router ospf 10 vrf vrf1

DES-7200(config-router)# domain-id 4.4.4.4

DES-7200(config-router)# domain-id 5.5.5.5 secondary
```

2.3.5.4 Configure VPN route tag (optional)

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **router ospf** *ospf-id* **vrf** *vrf-name*	Create OSPF instance and enter OSPF configuration mode
DES-7200(config-router)# **domain-tag** *value*	(Optional) Configure VPN route tag (1-4294967295) for OSPF instance.
DES-7200(config-router)# **show running-config**	Display existing configurations

Note

- This command is only applicable to OSPF instance associated with VRF.
- If the domain-tag of VRF is not configured manually, then the default value is the AS number of local BGP protocol.
- In L3VPN, if one VPN site is connected with multiple PEs, then the VPN route learned by PE through MP-BGP will be advertised to VPN site in type-5 or type-7 LSA. Such route may also be learned by other PEs connecting to this VPN site and then advertised, hence causing loop. To avoid such loop, the same VPN route tag must be configured on PE for VRF OSPF instances connecting to the same VPN site. When VRF OSPF instance sends type-4 or type-7 LSAs to the VPN site, this LSA will also carry the VPN route tag. When other PEs receive such type-5 or type-7 LSA containing the VPN route tag, if such route tag is the same as the route tag of corresponding OSPF instance, this LSA won't participate in OSPF computation.
- Generally, OSPF instances associated with the same VPN must be configured with the same VPN route tag.

Configure the domain-tag of VRF OSPF protocol to 10.

```
DES-7200# configure terminal

DES-7200(config)# router ospf 10 vrf vrf1

DES-7200(config-router)# domain-tag 10
```

2.3.5.5 Configure sham-link (optional)

Sham-link is mainly used in the scenario where there is a backdoor link between VPN sites. If you still expect to transmit VPN data via the MPLS backbone network, then you can establish sham-link between the VRF OSPF instances of two PEs. Both instances can establish OSPF neighbor through this sham-link and distribute LSA packets over the sham-link.

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **router ospf** *ospf-id* **vrf** *vrf-name*	Create OSPF instance and enter OSPF configuration mode
DES-7200(config-router)# **area** *area-id* **sham-link** *source-address destination-address*	(Optional) Configure the area ID, source address and destination address of sham-link

DES-7200(config-router)# **show running-config**	Display existing configurations

Note

- The sham-link must be configured on two PEs intending to establish the sham-link, which won't be established if only one PE is configured.
- The following conditions must be met in order to establish the sham-link between two PEs:

  1. The area-id of the sham-link configured on two PEs must be identical;
  2. The <source address, destination address> of sham-link configured on one PE must correspond to the <source address, destination address> of sham-link configured on another PE;
  3. The source address and destination address used to establish sham-link on the PE must be 32-bit Loopback address bound to VRF;

Caution The source address to establish sham-link must be redistributed to the BGP protocol of VRF, but it cannot participate in the calculation of VRF OSPF instance.

Configure sham-link for VRF OSPF instance, with area ID being 0, source address being 1.1.1.1 and destination address being 2.2.2.2.

```
DES-7200# configure terminal

DES-7200(config)# router ospf 10 vrf vrf1

DES-7200(config-router)# area 0 sham-link 1.1.1.1 2.2.2.2
```

2.3.5.6 Configure capability vrf-lite (optional)

The PE-CE OSPF feature of VRF OSPF instance involves LSA conversion as per domain ID, DN bit and VPN route tag. In certain circumstances, if you don't want VRF OSPF instance to support PE-CE OSPF feature, you can execute "**capability vrf-lite**" command to disable the feature.

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode

DES-7200(config)# **router ospf** *ospf-id* **vrf** *vrf-name*	Create OSPF instance and enter OSPF configuration mode
DES-7200(config-router)# **capability vrf-lite**	(Optional) Disable PE-CE OSPF feature of VRF OSPF instance
DES-7200(config-router)# **show running-config**	Display existing configurations

Note

- This command is only applicable to OSPF instance associated with VRF.
- In certain circumstances, you may expect to disable the loop check function of VRF OSPF instance. For example: VPN user uses MCE device to exchange VPN routes with PE. If MCE and PE exchanges VPN routes via OSPF protocol, to allow the VPN site to learn the routes of other VPN sites, you must execute "**capability vrf-lite**" command on MCE device to disable the loop check function of VRF OSPF instance.

Disable loop check function of VRF OSPF instance

```
DES-7200# configure terminal

DES-7200(config)# router ospf 10 vrf vrf1

DES-7200(config-router)# capability vrf-lite
```

2.3.5.7 Configure extcommunity-type (optional)

While form VPN route for BGP, OSPF route redistribution will also carry the Extended Communities attribute of OSPF route, including router-id and route-type. By default, the type of Extended Communities attribute of router-id is 0x0107, and that of route-type is 0x0306. However, the user can manually configure the Extended Communities attribute of "rouer-id" and "route-typ".

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **router ospf** *ospf-id* **vrf** *vrf-name*	Create OSPF instance and enter OSPF configuration mode

DES-7200(config-router)# **extcommunity-type** {**router-id** {**0107**|**8001**} | **route-type** {**0306**|**8000**}}	(Optional) Configure the Extended Communities attribute of OSPF router-id and route-type.
DES-7200(config-router)# **show running-config**	Display existing configurations

Note

- This command is only applicable to OSPF instance associated with VRF.
- The type configuration of router-id provides good compatibility with multiple manufacturers. For example, some manufacturers only support the router-id type of 0x0107. When interconnecting with such manufacturers, you must execute "**extcommunity-type**" command to set the type of router-id to 0x0107.
- The type configuration of route-type provides good compatibility with multiple manufacturers. For example, some manufacturers only support the route-type type of 0x8000. When interconnecting with such manufacturers, you must execute "**extcommunity-type**" command to set the type of route-type to 0x8000.

Configure the type of router-id of VRF OSPF protocol to 0x0107

```
DES-7200# configure terminal

DES-7200(config)# router ospf 10 vrf vrf1

DES-7200(config-router)# extcommunity-type router-id 0107
```

2.4 Verifying the L3VPN Configuration

This section describes how to verify the L3VPN configurations and VPN routes. Enter the privilege mode and run the following commands.

Command	Function
DES-7200# **show ip vrf** [*vrf_name*]	Display the VRF configuration information.

DES-7200# **show bgp vpnv4 unicast all** [*network* | **neighbor** [*peer-address*] | **summary** | **label**]	Display the VPN routing information.
DES-7200# **show ip route vrf** *vrf_name* [*ip-address* | **bgp | connected | isis | ospf | rip | static**]	Display the information about the VRF forwarding table.

Display the VPN routing information.

```
DES-7200# show bgp vpnv4 unicast all
Network              Nexthop       Metric   Localprf         Path
Route Distinguisher: 100:2
*>i 192.168.0.1/32  192.168.0.2       0      100     10 ?
*>i 192.168.1.0/32  192.168.0.2    0      100     ?
Route Distinguisher : 100:30
*>i 192.168.0.1/32  192.168.0.2       0      100     10 ?
*> 192.168.4.0  192.168.4.1          0             20 ?
* 192.168.4.0    0.0.0.0          0      32768     ?
```

Field	Description
*****	Indicates a valid route.
s (lower-case)	Indicates that the route is suppressed by an aggregated route.
s (upper-case)	Indicates that the route is a stale entry.
>	Indicates that the route is an optimal one.
I	Indicates that the route is learnt from the IBGP.
Nexthop	Indicates the next hop information of the route.
Metric	Indicates the route metric.
Localprf	Indicates the local preference of the route.
Path	Indicates the AS path included in the route.
I	Indicates that the origin of the route is IGP.
E	Indicates that the origin of the route is EGP.
?	Indicates that the origin of the route is another attribute except IGP or EGP (for example, a redistributed BGP route).

Display the information about the VRF routing table.

```
DES-7200# show ip route vrf vrf1
```

```
Codes: C - connected, S - static, R - RIP,B - BGP
O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
* - candidate default
B   192.168.0.1/32 , [200/0] via 192.168.0.2, 01:02:33
B   192.168.0.3/32 , [200/0] via 192.168.4.1 , 01:02:33
C   192.168.4.0/24 is directly connected ,eth1
```

Display the VRF configuration information.

```
DES-7200# show ip vrf vrf1
VRF vrf1; default RD: 100: 2
Interfaces:
Eth0
Export VPN route-target communities:
RT: 100: 30
No import VPN route-target community
No import route-map
```

2.5 Examples for Configuring BGP/MPLS VPN

2.5.1 Intranet Configuration Examples

Requirements: There are two VPN users: VPNA and VPNB. VPNA has sites in SITEA, SITEB, and SITEC and VPNB has sites in SITEB and SITEC. It is now required that the users in different sites of VPNA access each other, the users in different sites of VPNB access each other, and the users in the two VPNs not access each other, as shown in the following figure.

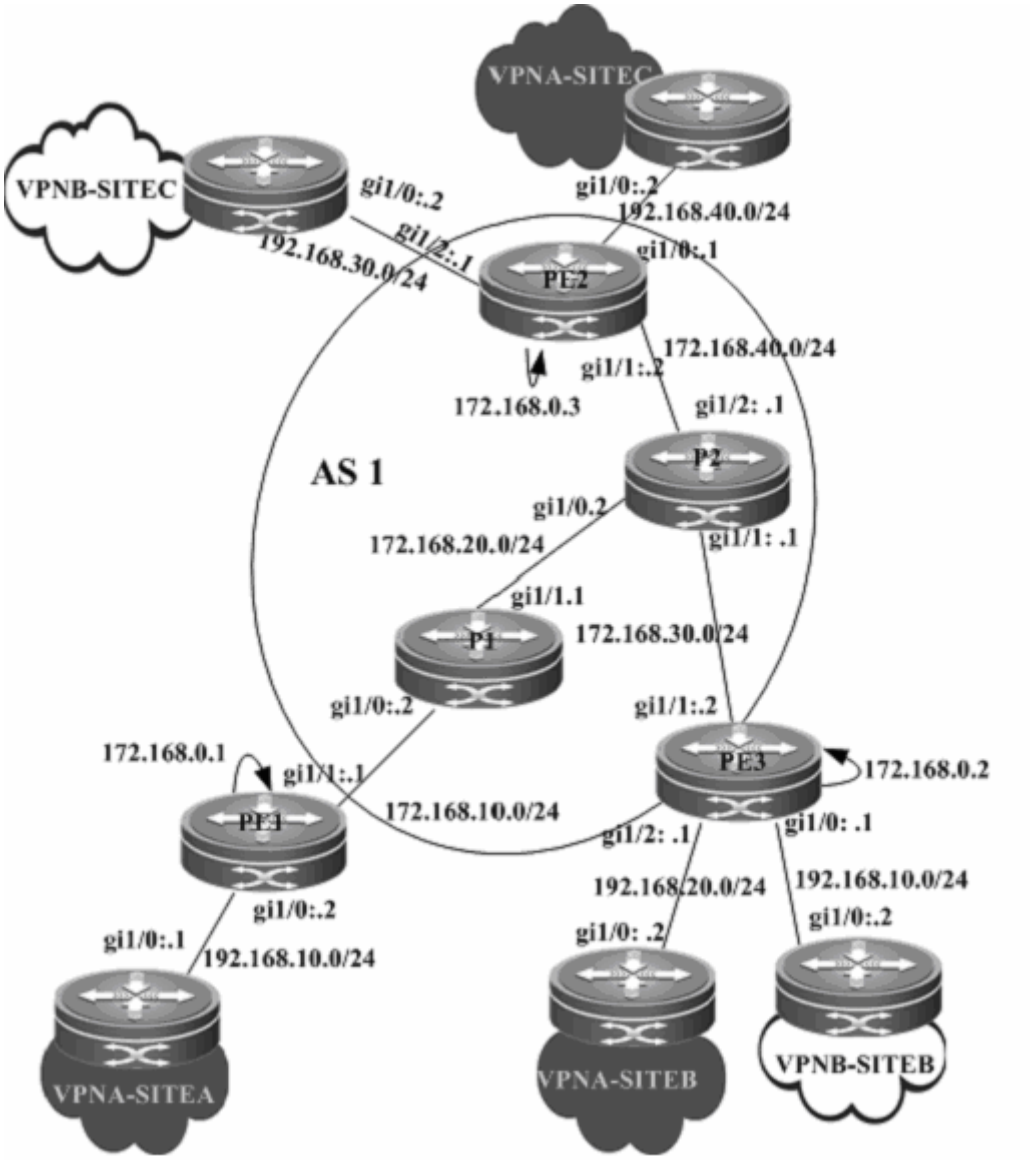


Figure 12

Configuration procedure:

PE1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.1 255.255.255.255
```

Configure the VRF.

Create one VRF instance: VPNA . Set the RD and RT values, and associate the VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# end
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)#ip vrf forwarding VPNA
DES-7200(config-if-GigabitEthernet 1/0)#ip address 192.168.10.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Enable BGP and set up MP-IBGP sessions with PE2 and PE3.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.2 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.2 update-source loopback 0
DES-7200(config-router)# neighbor 172.168.0.3 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.3 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.2 activate
DES-7200(config-router-af)# neighbor 172.168.0.3 activate
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# neighbor 172.168.10.1 remote-as 65002
DES-7200(config-router-af)# end
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

PE2:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.3 255.255.255.255
```

Configure the VRF.

Create two VRFs: VPNA and VPNB. Set the RD and RT values, and associate the VRFs with their corresponding interfaces.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# exit
DES-7200(config)# ip vrf VPNB
DES-7200(config-vrf)# rd 1:200
```

```
DES-7200(config-vrf)# route-target both 1:200
DES-7200(config-vrf)# exit
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip vrf forwarding VPNB
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)#ip vrf forwarding VPNA
DES-7200(config-if-GigabitEthernet 1/1)#ip address 192.168.20.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# exit
```

Enable BGP and set up MP-IBGP sessions with PE2 and PE3.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.1 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.1 update-source loopback 0
DES-7200(config-router)# neighbor 172.168.0.3 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.3 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.1 activate
DES-7200(config-router-af)# neighbor 172.168.0.3 activate
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# neighbor 172.168.20.2 remote-as 65003
DES-7200(config-router-af)# exit
```

```
DES-7200(config)# address-family ipv4 vrf VPNB
DES-7200(config-router-af)# neighbor 172.168.10.2 remote-as 65004
DES-7200(config-router-af)# end
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.30.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 172.168.30.0 255.255.255.0 area 0
DES-7200(config-router)# network 172.168.0.2 255.255.255.255 area 0
DES-7200(config-router)# end
```

PE3:

The configuration procedure is similar to that of PE2.

VPNA-SITEA:

Set up an EBGP session with PE1.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 65002
DES-7200(config-router)# neighbor 172.168.10.2 remote-as 1
DES-7200(config-router-af)# end
```

VPNA-SITEB:

The configuration procedure is similar to that of VPNA-SITEA.

VPNA-SITEC:

The configuration procedure is similar to that of VPNA-SITEA.

VPNB-SITEB:

The configuration procedure is similar to that of VPNA-SITEA.

VPNB-SITEC:

The configuration procedure is similar to that of VPNA-SITEA.

P1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.5 255.255.255.255
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip address 172.168.10.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# label-switching
```

```
DES-7200(config-if-GigabitEthernet 1/0)# mpls ip
DES-7200(config-if-GigabitEthernet 1/0)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.20.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.20.0 0.0.0.255 area 0
DES-7200(config-router)# end
```

P2:

The configuration procedure is similar to that of P1.

2.5.2 Extranet Configuration Examples

Requirements: There are two VPN users: VPNA and VPNB. Mutual access is required in a VPN. The two VPNs cannot access each other but can access some shared resources. As shown in the following figure, VPNA and VPNB sites should access the resources of VPN-SITEA.

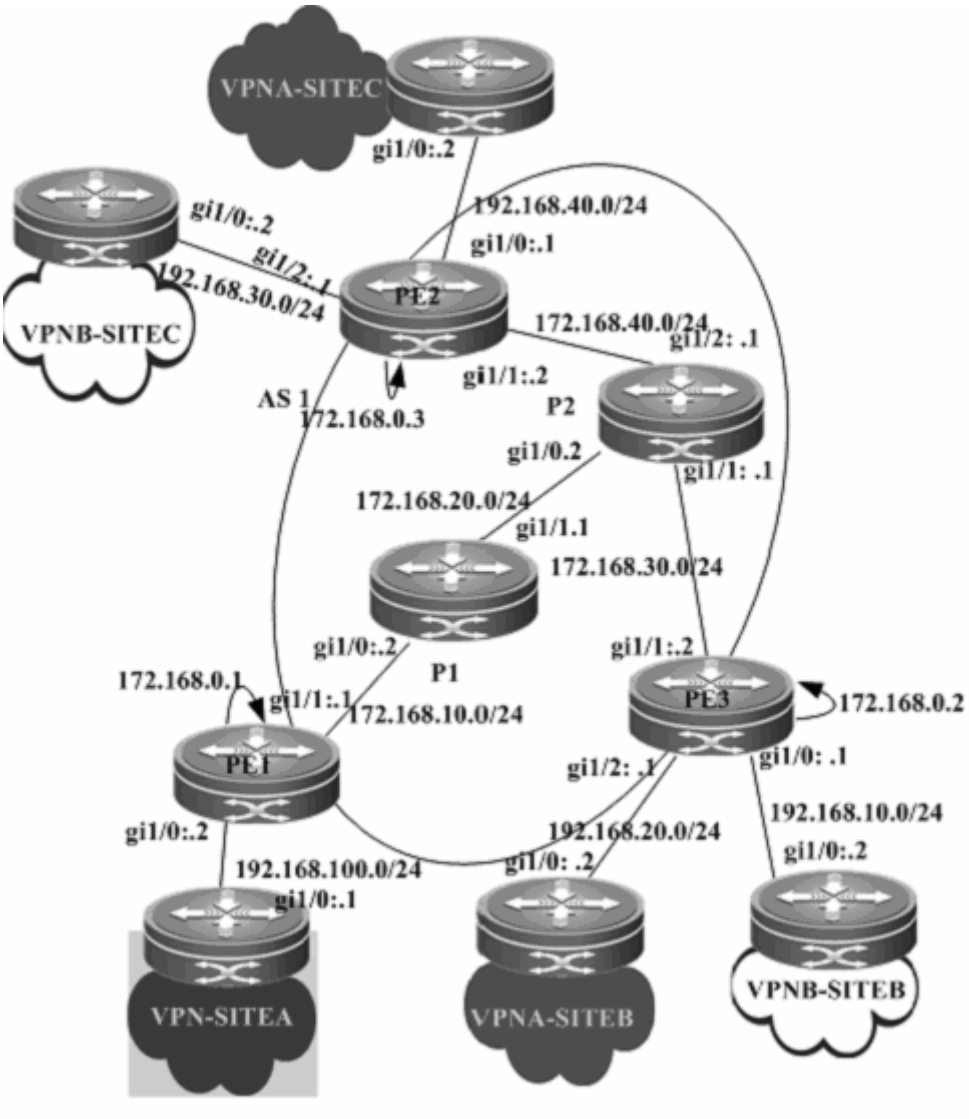


Figure 13

Configuration procedure:

PE1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.1 255.255.255.255
```

Configure the VRF.

Create one VRF instance: VPN_EXTRA. Set the RD and RT values, and associate the VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPN_EXTRA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# route-target both 1:200
DES-7200(config-vrf)# end
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip vrf forwarding VPN_EXTRA
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.100.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Enable BGP and set up MP-IBGP sessions with PE2 and PE3.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.2 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.2 update-source loopback 0
DES-7200(config-router)# neighbor 172.168.0.3 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.3 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.2 activate
DES-7200(config-router-af)# neighbor 172.168.0.3 activate
DES-7200(config-router-af)# end
```

Enable OSPF to exchange routes with a CE.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPN_EXTRA
DES-7200(config-router)# network 192.168.100.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPN_EXTRA
DES-7200(config-router-af)# redistribute ospf 10
DES-7200(config-router-af)# end
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

PE2:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.3 255.255.255.255
```

Configure the VRF.

Create two VRF instances: VPNA and VPNB. Set the RD and RT values, and associate the VRFs with their corresponding interfaces.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# exit
```

```
DES-7200(config)# ip vrf VPNB
DES-7200(config-vrf)# rd 1:200
DES-7200(config-vrf)# route-target both 1:200
DES-7200(config-vrf)# exit
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip vrf forwarding VPNB
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.10.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip vrf forwarding VPNA
DES-7200(config-if-GigabitEthernet 1/1)# ip address 192.168.20.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# exit
```

Enable BGP and set up MP-IBGP sessions with PE2 and PE3.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.1 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.1 update-source loopback 0
DES-7200(config-router)# neighbor 172.168.0.3 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.3 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.1 activate
DES-7200(config-router-af)# neighbor 172.168.0.3 activate
DES-7200(config-router-af)# end
```

Enable OSPF to exchange VPN routes with a CE.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPNA
```

```
DES-7200(config-router)# network 192.168.20.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config)# router ospf 20 VPNB
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# redistribute ospf 10
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family ipv4 vrf VPNB
DES-7200(config-router-af)# redistribute ospf 20
DES-7200(config-router-af)# exit
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.30.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.30.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.2 0.0.0.0 area 0
DES-7200(config-router)# end
```

PE3:

The configuration procedure is similar to that of PE2.

VPNA-SITEA:

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 192.168.100.0 255.255.255.0 area 0
DES-7200(config-router)# end
```

VPNA-SITEB:

The configuration procedure is similar to that of VPNA-SITEA.

VPNA-SITEC:

The configuration procedure is similar to that of VPNA-SITEA.

VPNB-SITEB:

The configuration procedure is similar to that of VPNA-SITEA.

VPNB-SITEC:

The configuration procedure is similar to that of VPNA-SITEA.

P1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.5 255.255.255.255
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
```

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip address 172.168.10.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# label-switching
DES-7200(config-if-GigabitEthernet 1/0)# mpls ip
DES-7200(config-if-GigabitEthernet 1/0)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.20.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.20.0 0.0.0.255 area 0
DES-7200(config-router)# end
```

P2:

The configuration procedure is similar to that of P1.

For the protocol between PEs and CEs, you can choose EBGP, OSPF, RIP, or other routing protocol as required.

2.5.3 Configuration Example for Hub-and-Spoke

Requirement: The VPN internal data should not be directly exchanged. Instead, the data must be exchanged through the unified control center. Only the control center is entitled to access all resources of a VPN. Any VPN users who want to obtain the VPN resources, must be notified through the control center. As shown in the following figure, to access VPNA-SITEB resources, VPNA-SITEA must pass the control center VPNA-SITEC. Direct access is not available.

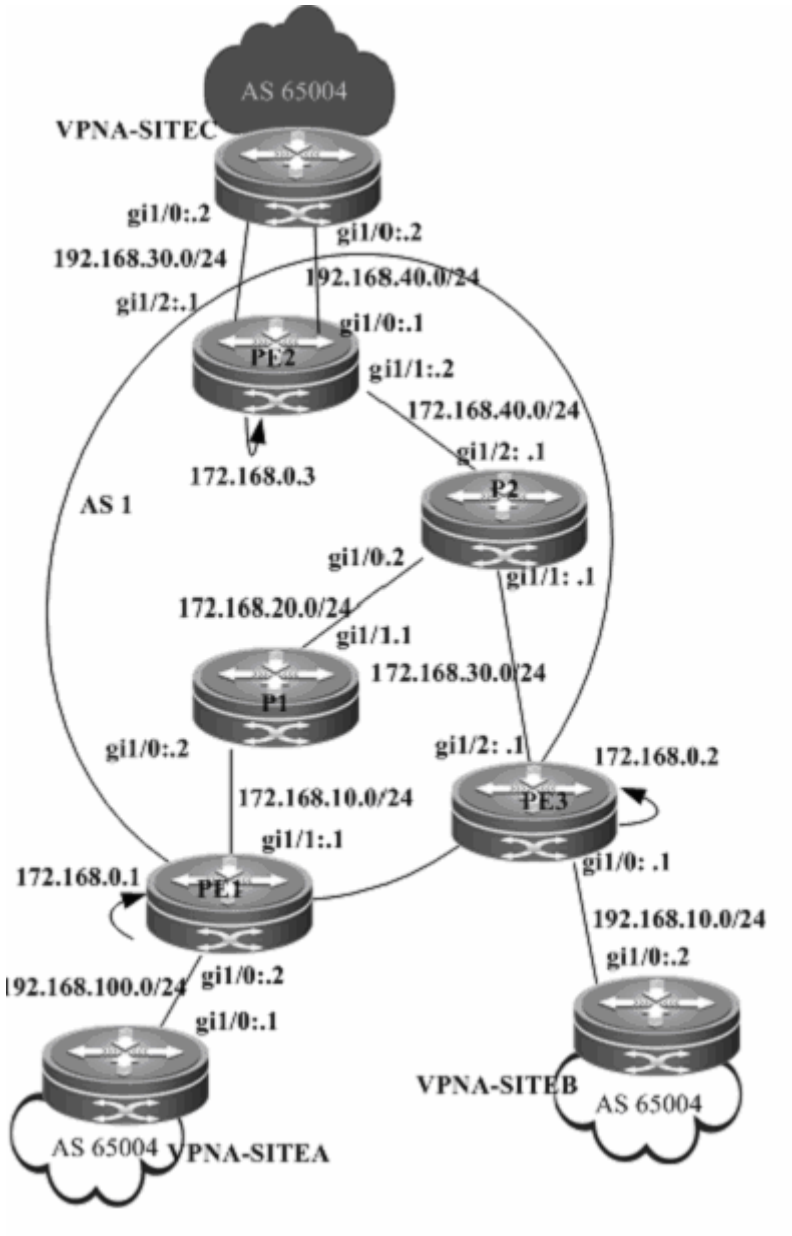


Figure 14

Configuration procedure:

PE1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.1 255.255.255.255
```

Configure the VRF.

Create one VRF instance: spoke1. Set the RD and RT values, and associate the VPNA with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf spoke1
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target export 1:200
DES-7200(config-vrf)# route-target import 1:100
DES-7200(config-vrf)# end
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip vrf forwarding spoke1
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.100.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Enable BGP and set up MP-IBGP sessions with PE3.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.3 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.3 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.3 activate
DES-7200(config-router-af)# neighbor 172.168.0.3 allowas-in
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config)# address-family ipv4 vrf spoke1
DES-7200(config-router-af)# neighbor 192.168.100.1 remote-as 65004
DES-7200(config-router-af)# neighbor 192.168.100.1 as-override
DES-7200(config-router-af)# end
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

PE2:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.3 255.255.255.255
```

Configure the VRF.

Create one VRF instance: spoke2. Set the RD and RT values, and associate the VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf spoke2
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target export 1:300
DES-7200(config-vrf)# route-target import 1:100
DES-7200(config-vrf)# exit
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip vrf forwarding spoke2
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.10.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# exit
```

Enable BGP and set up MP-IBGP sessions with PE3.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.3 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.3 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.3 activate
DES-7200(config-router-af)# neighbor 172.168.0.3 allowas-in
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf spoke2
DES-7200(config-router-af)# neighbor 192.168.10.2 remote-as 65004
DES-7200(config-router-af)# neighbor 192.168.10.2 as-override
DES-7200(config-router-af)# end
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.30.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 172.168.30.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.2 0.0.0.0 area 0
DES-7200(config-router)# end
```

PE3:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.2 255.255.255.255
```

Configure the VRF.

Create two VRF instances: from-spoke and from-hub. Set the RD and RT values, and associate the VRFs with their corresponding interfaces.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf from-spoke
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target import 1:300
DES-7200(config-vrf)# route-target import 1:200
DES-7200(config-vrf)# exit
```

```
DES-7200(config)# ip vrf from-hub
DES-7200(config-vrf)# rd 1:200
DES-7200(config-vrf)# route-target export 1:100
DES-7200(config-vrf)# exit
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip vrf forwarding from-hub
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.40.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip vrf forwarding from-spoke
DES-7200(config-if-GigabitEthernet 1/1)# ip address 192.168.30.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# exit
```

Enable BGP and set up MP-IBGP sessions with PE1 and PE2.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.1 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.1 update-source loopback 0
DES-7200(config-router)# neighbor 172.168.0.2 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.2 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.3 activate
DES-7200(config-router-af)# neighbor 172.168.0.2 activate
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
```

```
DES-7200(config-router)# address-family ipv4 vrf from-spoke
DES-7200(config-router-af)# neighbor 192.168.30.2 remote-as 65004
DES-7200(config-router-af)# neighbor 192.168.30.2 as-override
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family ipv4 vrf from-hub
DES-7200(config-router-af)# neighbor 192.168.40.2 remote-as 65004
DES-7200(config-router-af)# neighbor 192.168.40.2 allows-in
DES-7200(config-router-af)# exit
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
```

DES-7200(config)# interface gigabitethernet 1/1

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.30.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 172.168.30.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.2 0.0.0.0 area 0
DES-7200(config-router)# end
```

VPNA-SITEA:

Configure a PE session through EBGP.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 65004
DES-7200(config-router)# neighbor 192.168.100.2 remote-as 1
```

```
DES-7200(config-router)# exit
```

The configuration of VPNA-SITEB is similar to that of VPNA-SITEA.

VPNA-SITEC:

Configure a PE session through EBGP.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 65004
DES-7200(config-router)# neighbor 192.168.30.1 remote-as 1
DES-7200(config-router)# neighbor 192.168.40.1 remote-as 1
DES-7200(config-router)# exit
```

2.5.4 Inter-AS VPN OptionB: Next Hop Unchanged

Requirement: One VPN user has sites at both ASs. It is required that the VPN sites in different ASs access each other.

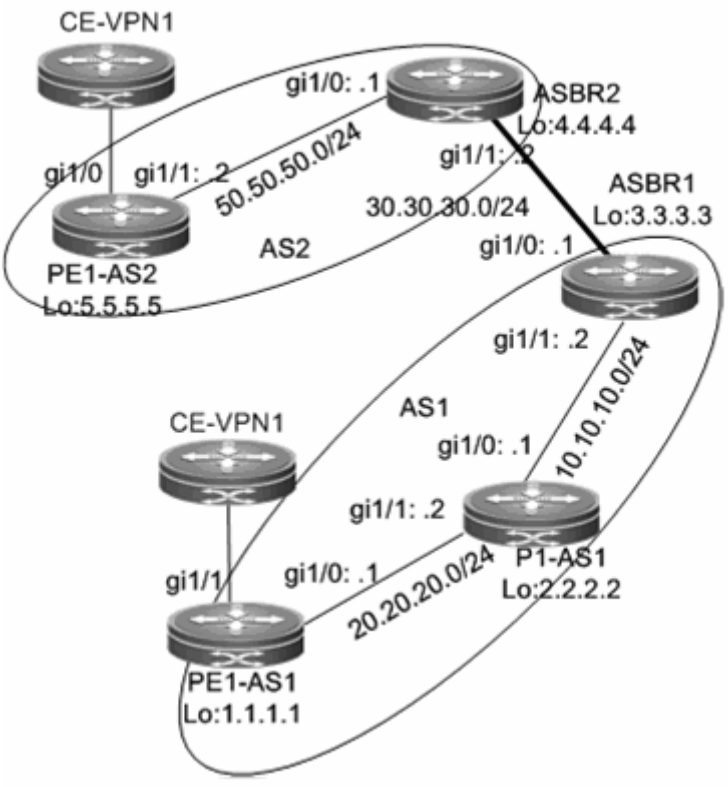


Figure 15 OptionB: Next Hop Unchanged

The configuration scheme is as follows:

PE1-AS1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 1.1.1.1 255.255.255.255
```

Configure the VRF.

Create one VRF instance: VPN1. Set the RD and RT values, and associate the VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPN1
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# end
```

Associate the VRF with an interface.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip vrf forwarding VPN1
DES-7200(config-if-GigabitEthernet 1/1)# ip address 192.168.16.2
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Enable BGP and set up MP-IBGP sessions with ASBR1.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 3.3.3.3 remote-as 1
DES-7200(config-router)# neighbor 3.3.3.3 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 3.3.3.3 activate
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

Refer to the configuration procedure in Running BGP Between a PE and CE to Transmit VPN Routes and the related configurations in **Intranet Configuration Examples**.

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip address 20.20.20.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# label-switching
DES-7200(config-if-GigabitEthernet 1/0)# mpls ip
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 20.20.20.0 0.0.0.255 area 0
DES-7200(config-router)# network 1.1.1.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

The procedure of **PE1-AS2** is similar to the preceding one.

P1-AS1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 2.2.2.2 255.255.255.255
```

Configure the MPLS signaling on the backbone network and enable MPLS on the public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-GigabitEthernet 1/0)# ip address 10.10.10.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# label-switching
DES-7200(config-if-GigabitEthernet 1/0)# mpls ip
DES-7200(config-if-GigabitEthernet 1/0)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-GigabitEthernet 1/1)# ip address 20.20.20.2
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
```

Configure routing protocols on the backbone network.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 20.20.20.0 0.0.0.255 area 0
DES-7200(config-router)# network 10.10.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 2.2.2.2 0.0.0.0 area 0
DES-7200(config-router)# end
```

ASBR1:

Configure the loopback interface.

```
DES-7200# configure terminal
```

```
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 3.3.3.3 255.255.255.255
```

Enable BGP, disable the BGP RF filtering function, and set up neighbor relations with PE1-AS1 and ASBR2.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# no bgp default route-target filter
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 1
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# neighbor 30.30.30.2 remote-as 2
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
DES-7200(config-router-af)# neighbor 30.30.30.2 activate
DES-7200(config-router-af)# end
```

Configure MPLS signaling and enable MPLS on a public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
DES-7200(config-if-gigabitethernet 1/1)# ip address 10.10.10.2
255.255.255.0
DES-7200(config-if-gigabitethernet 1/1)# label-switching
DES-7200(config-if-gigabitethernet 1/1)# mpls ip
DES-7200(config-if-gigabitethernet 1/1)# end
```

Run OSPF on the backbone network to transmit routes and redistribute directly connected network routes.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 10.10.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 3.3.3.3 0.0.0.0 area 0
DES-7200(config-router)# redisteibute connected subnets
DES-7200(config-router)# end
```

Assign an IP address to the interface connected to ASBR2.

```
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-gigabitethernet 1/0)# ip address 30.30.30.1
255.255.255.0
# Enable label switching on an interface.
DES-7200(config-if-gigabitethernet 1/0)# label-switching
```

The configuration of ASBR2 is similar to that of ASBR1.

2.5.5 Inter-AS VPN OptionB: Next Hop Changed

Requirement: One VPN user has sites at both ASs. It is required that the VPN sites in different ASs access each other.

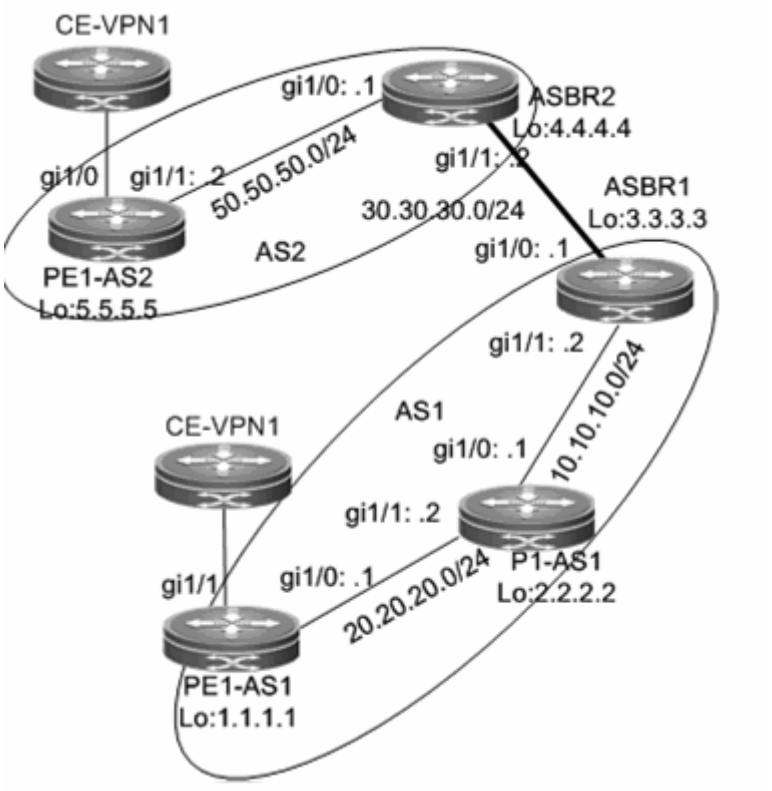


Figure 16 OptionB: Next Hop Changed

The configuration scheme is as follows:

PE1-AS1:

The configuration procedure is similar to that of PE1-AS1 in Inter AS VPN OptionB: Next Hop Unchanged and is not described here.

P1-AS1:

The configuration procedure is similar to that of P1-AS1 in Inter AS VPN OptionB: Next Hop Unchangedand is not described here.

ASBR1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 3.3.3.3 255.255.255.255
```

Enable BGP, disable the BGP RT filtering function, set up neighbor relations with the PE and ASBR, and modify the next hop of routes to the neighbor PE as the local address.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# no bgp default route-target filter
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 1
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# neighbor 30.30.30.2 remote-as 2
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
DES-7200(config-router-af)# neighbor 1.1.1.1 next-hop-self
DES-7200(config-router-af)# neighbor 30.30.30.2 activate
DES-7200(config-router-af)# end
```

Configure MPLS signaling and enable MPLS on a public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-gigabitethernet 1/1)# no switchport
DES-7200(config-if-gigabitethernet 1/1)# ip address 10.10.10.2
255.255.255.0
DES-7200(config-if-gigabitethernet 1/1)# label-switching
DES-7200(config-if-gigabitethernet 1/1)# mpls ip
DES-7200(config-if-gigabitethernet 1/1)# end
```

Run OSPF on the backbone network to transmit routing information.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 10.10.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 3.3.3.3 0.0.0.0 area 0
DES-7200(config-router)# end
```

Assign an IP address to the interface connected to ASBR2.

```
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-gigabitethernet 1/0)# ip address 30.30.30.1
255.255.255.0
# Enable label switching on an interface.
DES-7200(config-if-gigabitethernet 1/0)# label-switching
```

The configuration of ASBR2 is similar to that of ASBR1.

2.5.6 Inter-AS VPN OptionC: Enabling IPv4 Label Exchange Between EBGP Neighbors

Requirement: One VPN user has sites at both ASs. It is required that the VPN sites in different ASs access each other.

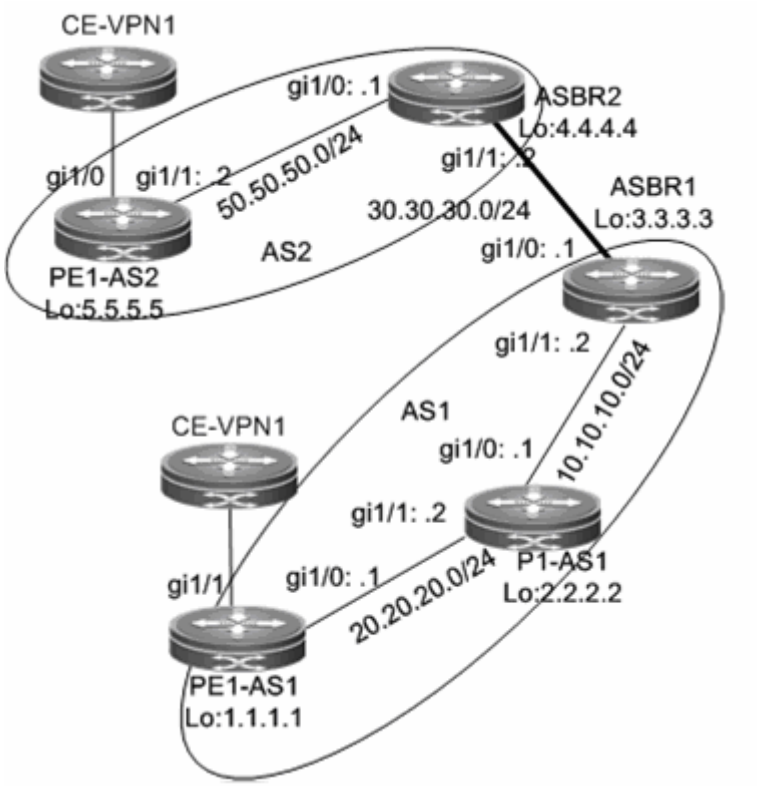


Figure 17 OptionC: enabling IPv4 label switching between EBGP neighbors

The configuration scheme is as follows:

PE1-AS1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 1.1.1.1 255.255.255.255
```

Configure the VRF.

The configuration procedure is similar to that of PE1-AS1 in Inter AS VPN OptionB: Next Hop Unchanged and is not described here.

Configure a multi-hop MP-EBGP session and disable IPv4 route exchange for the session.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 5.5.5.5 remote-as 2
DES-7200(config-router)# neighbor 5.5.5.5 update-source loopback 0
DES-7200(config-router)# neighbor 5.5.5.5 ebgp-multihop
```

```
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# no neighbor 5.5.5.5 activate
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# neighbor 5.5.5.5 activate
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

Refer to the configuration procedure in Running BGP Between a PE and CE to Transmit VPN Routes and the related configurations in Intranet Configuration Examples 错误！未指定书签。.

Configure MPLS signaling and enable MPLS on a public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-gigabitethernet 1/1)# no switchport
DES-7200(config-if-gigabitethernet 1/1)# ip address 20.20.20.1
255.255.255.0
DES-7200(config-if-gigabitethernet 1/1)# label-switching
DES-7200(config-if-gigabitethernet 1/1)# mpls ip
DES-7200(config-if-gigabitethernet 1/1)# end
```

Run OSPF on the backbone network to transmit routing information.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 20.20.20.0 0.0.0.255 area 0
DES-7200(config-router)# network 1.1.1.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

P1-AS1:

The configuration mainly includes the MPLS signaling protocol and IGP and is not described here. You can refer to the P1-AS1 configuration in Inter AS VPN OptionB: Next Hop Unchanged

ASBR1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 3.3.3.3 255.255.255.255
```

Configure ACL rules and route map rules to assign labels to or set labels only for routes that match the rules.

```
DES-7200# configure terminal
DES-7200(config)# ip access-list extended 101
DES-7200(config-ext-nacl)# permit ip host 1.1.1.1 any
uijie(config-ext-nacl)# exit
DES-7200(config)# ip access-list extended 102
DES-7200(config-ext-nacl)# permit ip host 5.5.5.5 any
DES-7200(config-ext-nacl)# exit
DES-7200(config)# route-map set-mpls
DES-7200(config-route-map)# match ip address 101
DES-7200(config-route-map)# set mpls-label
DES-7200(config-route-map)# exit
DES-7200(config)# route-map external-pe-route
DES-7200(config-route-map)# match ip address 102
DES-7200(config-route-map)# end
```

Set up an EBGP session with ASBR2 and configure route map rules to assign labels to PE routes that match the rules (the route map rules are optional and allow BGP to assign labels to only certain routes), and configure static routes to PEs in the local AS.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 30.30.30.2 remote-as 2
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 30.30.30.2 send-label
DES-7200(config-router-af)# neighbor 30.30.30.2 route-map set-mpls out
DES-7200(config-router-af)# network 1.1.1.1 mask 255.255.255.255
DES-7200(config-router-af)# end
```

Configure MPLS to assign label to certain BGP routes through ACL rules (The ACL rules are optional and allow you to reduce the number of unnecessary routes).

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
```

```
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# advertise-labels for bgp-routes acl 102
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-Gigabitethernet 1/1)# no switchport
DES-7200(config-if-Gigabitethernet 1/1)# ip address 10.10.10.2 255.255.255.0
DES-7200(config-if-Gigabitethernet 1/1)# label-switching
DES-7200(config-if-Gigabitethernet 1/1)# mpls ip
DES-7200(config-if-Gigabitethernet 1/1)# end
```

Configure a routing protocol on the backbone network to redistribute only BGP routes that match the route map rules (The route map rules are optional and allow you to reduce the number of unnecessary routes).

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 10.10.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 3.3.3.3 0.0.0.0 area 0
DES-7200(config-router)# redisteibute bgp subnets route-map external-pe-route
DES-7200(config-router)# end
```

Assign an IP address to the interface connected to ASBR2.

DES-7200(config)# **interface gigabitethernet** *1/0*

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-gigabitethernet 1/0)# ip address 30.30.30.1
255.255.255.0
# Enable label switching on an interface.
DES-7200(config-if-gigabitethernet 1/0)# label-switching
```

The configuration of ASBR2 is similar to that of ASBR1.

2.5.7 Inter-AS VPN OptionC: Enabling IPv4 Label Exchange Between Both EBGP and IBGP Neighbors

Requirement: One VPN user has sites at both ASs. It is required that the VPN sites in different ASs access each other.

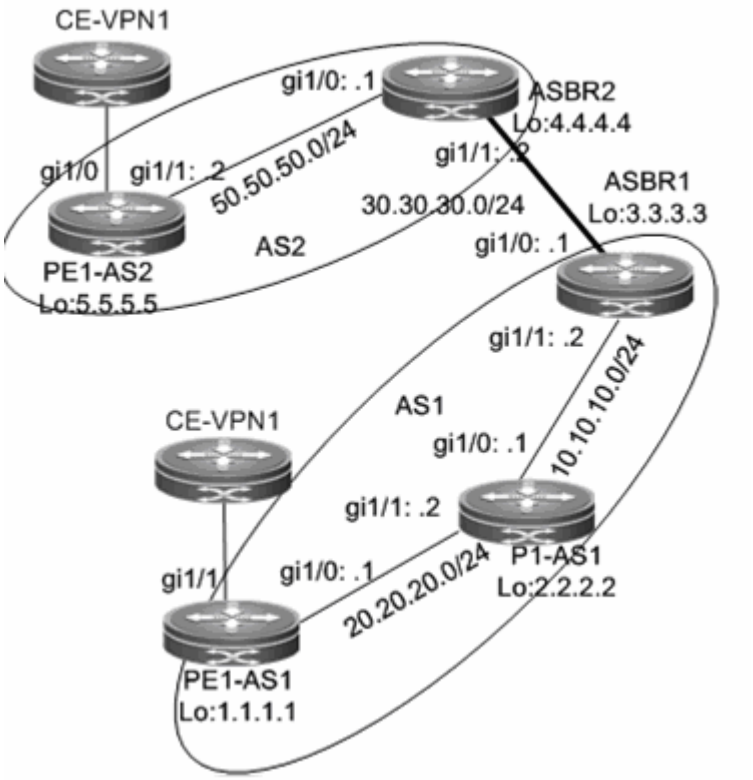


Figure 18 OptionC: enabling IPv4 label switching between both EBGP and IBGP neighbors

The configuration scheme is as follows:

PE1-AS1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 1.1.1.1 255.255.255.255
```

Configure the VRF.

The configuration procedure is similar to that of PE1-AS1 in Inter AS VPN OptionB: Next Hop Unchanged and is not described here.

Configure a multi-hop MP-EBGP session and disable IPv4 route exchange for the session.

The configuration procedure is similar to that of Inter AS VPN OptionC: Enabling IPv4 Label Exchange Between EBGP Neighbors and is not described here.

Set up an IBGP session with the ASBR and enable IPv4 label switching.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 3.3.3.3 remote-as 1
DES-7200(config-router)# neighbor 3.3.3.3 update-source loopback 0
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 3.3.3.3 activate
DES-7200(config-router-af)# neighbor 3.3.3.3 send-label
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

Refer to the configuration procedure in Running BGP Between a PE and CE to Transmit VPN Routes and the related configurations in Intranet Configuration Examples.

Configure MPLS signaling and enable MPLS on a public network interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-gigabitethernet 1/0)# no switchport
DES-7200(config-if-gigabitethernet 1/0)# ip address 20.20.20.1
255.255.255.0
DES-7200(config-if-gigabitethernet 1/0)# label-switching
DES-7200(config-if-gigabitethernet 1/0)# mpls ip
DES-7200(config-if-gigabitethernet 1/0)# end
```

Run OSPF on the backbone network to transmit routing information.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 20.20.20.0 0.0.0.255 area 0
```

```
DES-7200(config-router)# network 1.1.1.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

The configuration of PE1-AS2 is similar to that of PE1-AS1.

P1-AS1:

The configuration mainly includes the MPLS signaling protocol and IGP and is not described here. It is similar to Example for Configuring Basic MPLS Functions.

ASBR1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 3.3.3.3 255.255.255.255
```

Configure ACL rules and route map rules to assign labels to or set labels only for routes that match the rules.

```
DES-7200# configure terminal
DES-7200(config)# ip access-list extended 101
DES-7200(config)# permit ip host 1.1.1.1 any
DES-7200(config)# exit
DES-7200(config)# ip access-list extended 102
DES-7200(config)# permit ip host 5.5.5.5 any
DES-7200(config)# route-map internal-mpls-route permit 10
DES-7200(config-route-map)# match ip address 101
DES-7200(config-route-map)# set mpls-label
DES-7200(config-route-map)# exit
DES-7200(config)# route-map external-mpls-route permit 10
DES-7200(config-route-map)#  match ip address 102
DES-7200(config-route-map)#  set mpls-label
DES-7200(config-route-map)#  end
```

Set up an EBGP session with the ASBR and configure route map rules to assign labels to PE routes that match the rules (the route map rules are optional and allow BGP to assign labels to only certain routes), and configure static routes to PEs in the local AS.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
```

```
DES-7200(config-router)# neighbor 30.30.30.2 remote-as 2
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 1
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 30.30.30.2 send-label
DES-7200(config-router-af)# neighbor 30.30.30.2 route-map internal-mpls-route out
DES-7200(config-router-af)# neighbor 1.1.1.1 send-label
DES-7200(config-router-af)# neighbor 1.1.1.1 route-map external-mpls-route out
DES-7200(config-router-af)#  network 1.1.1.1 mask 255.255.255.255
DES-7200(config-router-af)# end
```

Configure MPLS signaling and enable MPLS on an interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-Gigabitethernet 1/1)# no switchport
DES-7200(config-if-Gigabitethernet 1/1)# ip address 10.10.10.2
255.255.255.0
DES-7200(config-if-Gigabitethernet 1/1)# label-switching
DES-7200(config-if-Gigabitethernet 1/1)# mpls ip
DES-7200(config-if-Gigabitethernet 1/1)# end
```

Run OSPF on the backbone network to transmit routing information.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 10.10.10.0 255.255.255.0 area 0
DES-7200(config-router)# network 3.3.3.3 0.0.0.0 area 0
DES-7200(config-router)# end
```

Assign an IP address to the interface connected to ASBR2.

DES-7200(config)# **interface gigabitethernet** *1/0*

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-gigabitethernet 1/0)# ip address 30.30.30.1
255.255.255.0
# Enable label switching on an interface.
DES-7200(config-if-gigabitethernet 1/0)# label-switching
```

The configuration of ASBR2 is similar to that of ASBR1.

2.5.8 Inter-AS VPN OptionC: RR Networking Scheme

In the two implementation modes of OptionC, another problem exists. If the sites of the same VPN user are located at different ASs, a common OptionC scheme requires full mesh BGP connections for the inter-AS PEs to ensure the connectivity of the VPN sites. As shown in the following figure, the sites of the VPN user are at three different ASs. If a new VPN site is added, the new site has to set up BGP connections with the other VPN sites. This restricts the application of the common OptionC scheme. To address the preceding expansion problem, you can add an RR to each AS in the OptionC scheme. The RRs set up multi-hop MP-EBGP connections to exchange inter-AS VPN routes. At the same time, you can set up MP-IBGP sessions between PEs and the RR in the AS.

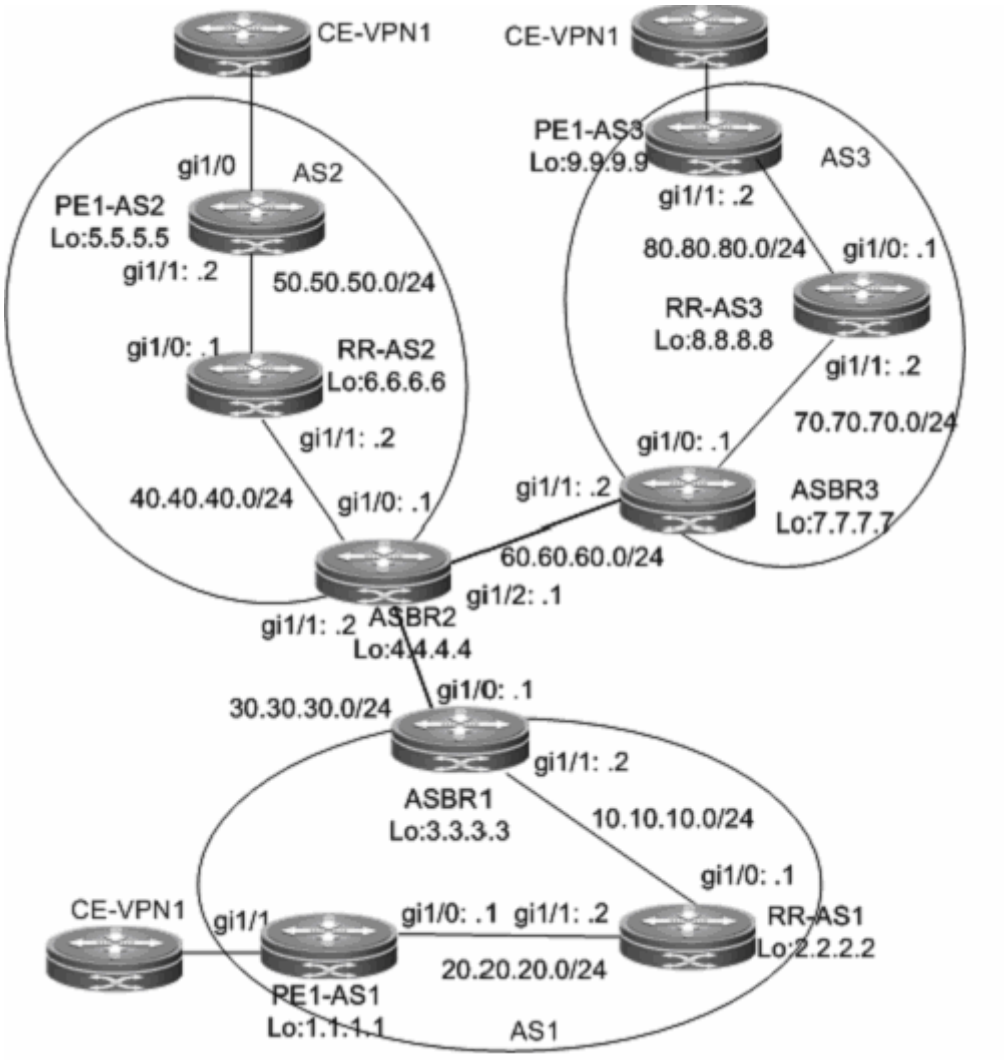


Figure 19 Setting up multi-hop MP-EBGP sessions between RRs in the OptionC scheme

The configuration scheme is as follows:

PE1-AS1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 1.1.1.1 255.255.255.255
```

Configure the VRF.

The configuration procedure is similar to that of PE1-AS1 in Inter AS VPN OptionB: Next Hop Unchangedand is not described here.

Set up an MP-IBGP session with the RR and enable label exchanging of IPv4 routes.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 2.2.2.2 remote-as 1
DES-7200(config-router)# neighbor 2.2.2.2 update-source loopback 0
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# neighbor 2.2.2.2 activate
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 2.2.2.2 activate
DES-7200(config-router-af)# neighbor 2.2.2.2 send-label
DES-7200(config-router-af)# end
```

Configure CE neighbors through EBGP.

Refer to the configuration procedure in Running BGP Between a PE and CE to Transmit VPN Routes and the related configurations in Intranet Configuration Examples.

The configurations of PE1-AS2 and PE1-AS3 are similar to that of PE1-AS1.

RR-AS1

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 2.2.2.2 255.255.255.255
```

Set up an MP-IBGP session with the PE, specify the PE as the RR client, and enable label exchanging of IPv4 routes.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 1.1.1.1 remote-as 1
DES-7200(config-router)# neighbor 1.1.1.1 update-source loopback 0
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
DES-7200(config-router-af)# neighbor 1.1.1.1 route-reflector-client
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family ipv4
```

```
DES-7200(config-router-af)# neighbor 1.1.1.1 activate
DES-7200(config-router-af)# neighbor 1.1.1.1 send-label
DES-7200(config-router-af)# neighbor 1.1.1.1 route-reflector-client
DES-7200(config-router-af)# end
```

Set up a multi-hop MP-EBGP session with the RR, do not modify the next hop of VPN routes exchanged with the RR, and disable the IPv4 route exchange with the RR.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 6.6.6.6 remote-as 2
DES-7200(config-router)# neighbor 6.6.6.6 update-source loopback 0
DES-7200(config-router)# neighbor 6.6.6.6 ebgp-multihop
DES-7200(config-router)# neighbor 8.8.8.8 remote-as 3
DES-7200(config-router)# neighbor 8.8.8.8 update-source loopback 0
DES-7200(config-router)# neighbor 8.8.8.8 ebgp-multihop
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# no neighbor 6.6.6.6 activate
DES-7200(config-router-af)# no neighbor 8.8.8.8 activate
DES-7200(config-router-af)# exit-address-family
DES-7200(config-router)# address-family vpnv4 unicast
DES-7200(config-router-af)# neighbor 6.6.6.6 activate
DES-7200(config-router-af)# neighbor 6.6.6.6 next-hop-unchanged
DES-7200(config-router-af)# neighbor 8.8.8.8 activate
DES-7200(config-router-af)# neighbor 8.8.8.8 next-hop-unchanged
DES-7200(config-router-af)# end
```

Set up an IBGP session with the ASBR and enable IPv4 label switching.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 3.3.3.3 remote-as 1
DES-7200(config-router)# neighbor 3.3.3.3 update-source loopback 0
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 3.3.3.3 activate
DES-7200(config-router-af)# neighbor 3.3.3.3 send-label
DES-7200(config-router-af)# end
```

Configure MPLS.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
```

```
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-gigabitethernet 1/1)# no switchport
DES-7200(config-if-gigabitethernet 1/1)# ip address 20.20.20.2
255.255.255.0
DES-7200(config-if-gigabitethernet 1/1)# label-switching
DES-7200(config-if-gigabitethernet 1/1)# mpls ip
DES-7200(config-if-gigabitethernet 1/1)# exit
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-gigabitethernet 1/0)# no switchport
DES-7200(config-if-gigabitethernet 1/0)# ip address 10.10.10.1
255.255.255.0
DES-7200(config-if-gigabitethernet 1/0)# label-switching
DES-7200(config-if-gigabitethernet 1/0)# mpls ip
DES-7200(config-if-gigabitethernet 1/0)# end
```

Run OSPF on the backbone network to transmit routing information.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 20.20.20.0 0.0.0.255 area 0
DES-7200(config-router)# network 2.2.2.2 0.0.0.0 area 0
DES-7200(config-router)# network 10.10.10.0 0.0.0.255 area 0
DES-7200(config-router)# end
```

The procedures of RR-AS2 and RR-AS3 are similar to the preceding procedure.

ASBR1:

Configure the loopback interface.

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 3.3.3.3 255.255.255.255
```

Configure ACL rules and route map rules.

```
DES-7200# configure terminal
DES-7200(config)# ip access-list extended 101
DES-7200(config-ext-nacl)# permit ip host 1.1.1.1 any
DES-7200(config-ext-nacl)# exit
DES-7200(config)# ip access-list extended 102
DES-7200(config-ext-nacl)# permit ip host 5.5.5.5 any
DES-7200(config-ext-nacl)# permit ip host 9.9.9.9 any
DES-7200(config-ext-nacl)# exit
DES-7200(config)# route-map internal-mpls-route permit 10
DES-7200(config-route-map)# match ip address 101
DES-7200(config-route-map)# set mpls-label
DES-7200(config-route-map)# exit
DES-7200(config)# route-map external-mpls-route permit 10
DES-7200(config-route-map)# match ip address 102
DES-7200(config-route-map)# set mpls-label
DES-7200(config-route-map)# end
```

Set up an EBGP session with the ASBR, enable label switching of IPv4 routes, and configure route map rules to assign labels to PE routes that match the rules (the route map rules are optional and allow the BGP to assign labels to only certain routes). Set up an IBGP session with the RR, enable label switching of IPv4 routes, and configure route map rules to assign labels to inter-PE routes that match the rules. Configure static routes to the PEs in the local AS.

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 30.30.30.2 remote-as 2
DES-7200(config-router)# neighbor 2.2.2.2 remote-as 1
DES-7200(config-router)# neighbor 2.2.2.2 update-source loopback 0
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 30.30.30.2 send-label
DES-7200(config-router-af)# neighbor 30.30.30.2 route-map internal-mpls-route out
DES-7200(config-router-af)# neighbor 2.2.2.2 send-label
DES-7200(config-router-af)# neighbor 2.2.2.2 route-map external-mpls-route out
DES-7200(config-router-af)# network 1.1.1.1 mask 255.255.255.255
DES-7200(config-router-af)# end
```

Configure MPLS signaling and enable MPLS on an interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
```

```
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-Gigabitethernet 1/1)# no switchport
DES-7200(config-if-Gigabitethernet 1/1)#ip address 10.10.10.2
255.255.255.0
DES-7200(config-if-Gigabitethernet 1/1)# label-switching
DES-7200(config-if-Gigabitethernet 1/1)# mpls ip
DES-7200(config-if-Gigabitethernet 1/1)# end
```

Run OSPF on the backbone network to transmit routing information.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 10.10.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 3.3.3.3 0.0.0.0 area 0
DES-7200(config-router)# end
```

Assign an IP address to the interface connected to ASBR2.

```
DES-7200(config)# interface gigabitethernet 1/0
```

The **no switchport** command is used to switch the port mode on switches to routed port mode. It is not applicable to routers. You are not required to run this command on routers.

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
DES-7200(config-if-gigabitethernet 1/0)# ip address 30.30.30.1
255.255.255.0
# Enable label switching on an interface.
DES-7200(config-if-gigabitethernet 1/0)# label-switching
```

The configurations of ASBR2 and ASBR3 are similar to that of ASBR1.

2.5.9 CSC: Second Carrier provides Internet service based on IP core

2.5.9.1 Networking requirements

A carrier owns a private network in City A, and this network has the BGP gateways to ISP A and ISP B. This carrier utilizes its private network to provide Internet service to users in City A. Currently, this carrier expects to expand service to City B, and therefore leases MPLS VPN service from VPN carrier in the hope of connecting two cities via VPN, so that users in City B can access Internet through the existing Internet gateways. The internal routes are exchanged via IGP (OSPF), and the external routes are exchanged via BGP.

2.5.9.2 Network topology

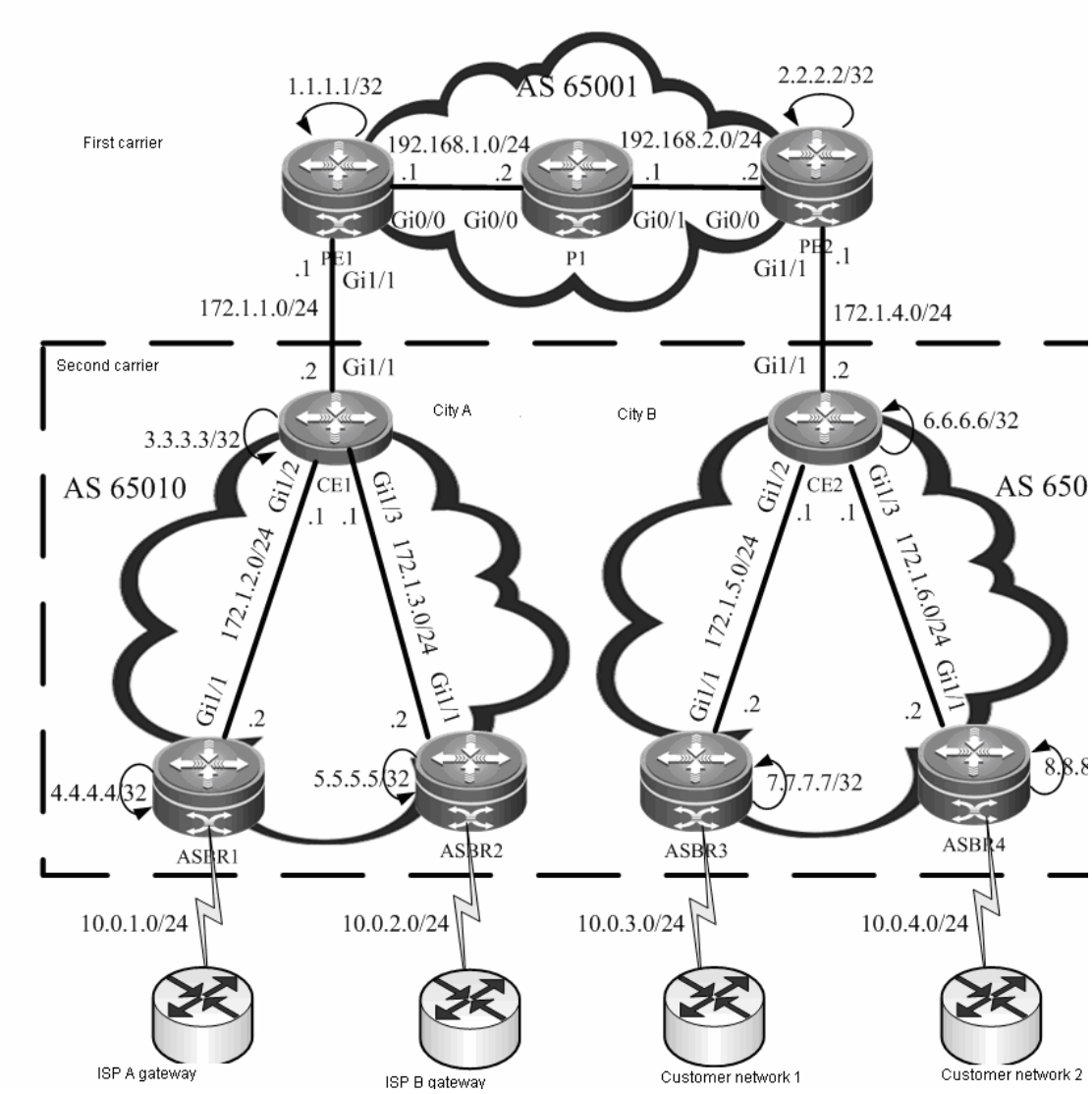


Fig 20 Network topology of scenario I

2.5.9.3 Configuration tips

Configure basic BGP/MPLS VPN for First Carrier

- Enable CSC function
- Configure Second Carrier
- Configure user access

2.5.9.4 Configuration steps

Configure basic BGP/MPLS VPN for First Carrier

Configure MPLS network: Here we will take PE1 as the example. The configurations of P1 and PE2 are the same.

Configure Loopback interface

```
DES-7200(config)# interface Loopback 0
DES-7200(config-if)# ip address 1.1.1.1 255.255.255.255
DES-7200(config-if)# exit
```

Globally enable MPLS and LDP

```
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp rouer-id interface Loopback 0
DES-7200(config-mpls-router)# exit
```

Enable MPLS and LDP on the interface

```
DES-7200(config)# interface gigabitEthernet 0/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# label-switching
DES-7200(config-if)# mpls ip
```

```
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
```

Configure IGP (OSPF)

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 1.1.1.1 0.0.0.0 area 0
DES-7200(config-router)# network 192.168.1.0 0.0.0.255 area 0
DES-7200(config-router)# exit
```

Configure MP-IBGP neighbor: Here we will take PE1 as the example. The configurations of PE2 are the same.

```
DES-7200(config)# router bgp 65001
DES-7200(config-router)# neighbor 2.2.2.2 remote-as 65001
DES-7200(config-router)# neighbor 2.2.2.2 update-source Loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 2.2.2.2 activate
DES-7200(config-router-af)# neighbor 2.2.2.2 send-community both
```

Configure VRF: Here we will take PE1 as the example. The configurations of PE2 are the same.

```
DES-7200(config)# ip vrf vpn1
DES-7200(config-vrf)# rd 65001:20
DES-7200(config-vrf)# route-target both 65001:20
DES-7200(config-vrf)# alloc-label per-route
DES-7200(config-vrf)# exit
DES-7200(config)# interface loopback 1
DES-7200(config-if)# ip vrf forwarding vpn1
DES-7200(config-if)# ip address 10.1.1.1 255.255.255.255
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip vrf forwarding vpn1
DES-7200(config-if)# ip address 172.1.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
```

Configure CE to connect with PE: Here we will take CE1 as the example. The configurations of CE2 are the same.

```
DES-7200(config)# interface gigabitEthernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 172.1.1.2 255.255.255.0
DES-7200(config-if)# no shutdown
```

Configure PE-CE route exchanging: Here we will take PE1-CE1 as the example. The configurations of PE2-CE2 are the same.

Configure on PE1:

```
DES-7200(config)# router ospf 100 vrf vpn1
DES-7200(config-router)# network 172.1.1.0 0.0.0.255 area 0
DES-7200(config-router)# redistribute bgp 65001 subnets
DES-7200(config-router)# exit
DES-7200(config)# router bgp 65001
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router-af)# redistribute ospf 100 vrf vpn1
DES-7200(config-router-af)# exit
DES-7200(config-router)# exit
```

Then, configure on CE1:

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.1.1.0 0.0.0.255 area 0
DES-7200(config-router)# exit
```

Enable CSC function

Enable CSC on PE: Here we will take PE1 as the example. The configurations of PE2 are the same.

```
DES-7200(config)# mpls router ldp vpn1
DES-7200(config-mpls-router)# ldp rouer-id interface Loopback 1
DES-7200(config-mpls-router)# advertise-labels for bgp-routes
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitEthernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
```

```
DES-7200(config-if)# label-switching
DES-7200(config-if)# mpls ip
```

Enable MPLS and LDP on CE: Here we will take CE1 as the example. The configurations of CE2 are the same.

```
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp rouer-id interface Loopback 0
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitEthernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# label-switching
DES-7200(config-if)# mpls ip
```

Configure Second Carrier

Configure interface and IGP: Here we will take CE1 as the example. The configurations of CE2, ASBR1, ASBR2, ASBR3 and ASBR4 are the same.

```
DES-7200(config)# interface gigabitEthernet 1/2
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 172.1.2.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet 1/3
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 172.1.3.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
```

```
DES-7200(config)# interface Loopback 0
DES-7200(config-if)# ip address 3.3.3.3 255.255.255.255
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 3.3.3.3 0.0.0.0 area 0
DES-7200(config-router)# network 172.1.2.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.1.3.0 0.0.0.255 area 0
DES-7200(config-router)# exit
```

On ASBR, configure CE as the BGP neighbor: Here we will take ASBR1 as the example. The configurations of ASBR2, ASBR3 and ASBR4 are the same.

```
DES-7200(config)# router bgp 65010
DES-7200(config-router)# neighbor 3.3.3.3 remote-as 65010
DES-7200(config-router)# neighbor 3.3.3.3 update-source Loopback 0
DES-7200(config-router)# neighbor 3.3.3.3 next-hop-self
```

On CE, configure ASBR and peer site PE as the route reflector client: Here we will take CE1 as the example. The configurations of CE2 are the same.

```
DES-7200(config)# router bgp 65010
DES-7200(config-router)# neighbor 4.4.4.4 remote-as 65010
DES-7200(config-router)# neighbor 4.4.4.4 update-source Loopback 0
DES-7200(config-router)# neighbor 4.4.4.4 route-reflector-client
DES-7200(config-router)# neighbor 5.5.5.5 remote-as 65010
DES-7200(config-router)# neighbor 5.5.5.5 update-source Loopback 0
DES-7200(config-router)# neighbor 5.5.5.5 route-reflector-client
DES-7200(config-router)# neighbor 6.6.6.6 remote-as 65010
DES-7200(config-router)# neighbor 6.6.6.6 update-source Loopback 0
DES-7200(config-router)# neighbor 6.6.6.6 route-reflector-client
DES-7200(config-router)# neighbor 6.6.6.6 next-hop-self
```

Configure user access

Here we will connect user network 1 with ASBR3. The configurations of other external networks (user network and Internet gateway) are the same.

On ASBR3

```
DES-7200(config)# interface gigabitEthernet 1/2
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
```

```
DES-7200(config-if)# ip address 10.0.3.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# router bgp 65010
DES-7200(config-router)# neighbor 10.0.3.2 remote-as 100
DES-7200(config-router)# exit
```

On the edge router of user network 1

```
DES-7200(config)# interface gigabitEthernet 0/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 10.0.3.2 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet 0/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 64.21.33.9 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# router bgp 100
DES-7200(config-router)# neighbor 10.0.3.1 remote-as 65010
DES-7200(config-router)# network 64.21.33.0 mask 255.255.255.0
```

2.5.9.5 Verification

Display VRF routes and labels on PE: Here we will take PE1 as the example. The configurations of PE2 are the same.

// In the VRF routing table of PE, there are only internal routes of the Second Carrier. There is no external route (i.e.: 64.30.4.0/24).

```
DES-7200# show ip route vrf vpn1
Routing Table: vpn1

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
O    3.3.3.3/32 [110/11] via 172.1.1.2, 00:00:07, gigabitEthernet 1/1
C    172.1.1.0/24 is directly connected, gigabitEthernet 1/1
C    172.1.1.1/32 is local host.
O    172.1.2.0/24 [110/12] via 172.1.1.2, 00:00:07, gigabitEthernet 1/1
B    172.1.4.0/24 [200/0] via 2.2.2.2, 00:00:30
......
DES-7200# show mpls ldp bindings vrf vpn1
VRF vpn1(id 1)
    lib entry: 3.3.3.3/32
        local binding:  to lsr:   172.1.1.2:0, label: 1025
        remote binding: from lsr: 172.1.1.2:0, label: imp-null
    lib entry: 172.1.1.0/24
        local binding:  to lsr:   172.1.1.2:0, label: imp-null
        remote binding: from lsr: 172.1.1.2:0, label: imp-null
    lib entry 172.1.2.0/24
        local binding:  to lsr:   172.1.1.2:0, label: 1026
        remote binding: from lsr: 172.1.1.2:0, label: 1024
    ......
```

In ASBR and user network, display the routing table

// On ASBR, there are both external routes and internal routes (taking ASBR3 as the example)

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
......
O    3.3.3.3/24 [110/12] via 172.1.5.1, 00:00:30, gigabitEthernet 1/1
B    61.10.55.0/24 [200/0] via 3.3.3.3, 00:00:40
B    64.21.33.0/24 [200/0] via 10.0.3.2, 00:00:31
```

```
.....
```

// In the user network, there are external routes (taking the edge device of user network 1 as the example)

```
DES-7200# show ip route
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
......
B    61.10.55.0/24 [200/0] via 10.0.3.1, 00:00:40
C    64.21.33.0/24 is directly connected, gigabitEthernet 0/1
C    64.21.33.9/32 is local host.
......
```

Verify that the external networks are interconnected

// On the edge device of user network 1

```
DES-7200# ping 61.10.55.1 source 64.21.33.9
Sending 5, 100-byte ICMP Echoes to 61.10.55.1, timeout is 2 seconds:
Packet sent with a source address of 64.21.33.9
  < press Ctrl+C to break >
!!!!!
```

2.5.10 CSC: Second Carrier provides Internet service based on MPLS core

2.5.10.1 Networking requirements

A carrier is providing Internet service for users in City A. Considering that it may need to provide MPLS service for users in the future, this carrier has deployed MPLS on its backbone network. Now this carrier intends to expand its service to City B, and has built MPLS network in City B. To interconnect the core networks in two cities, this carrier leases the VPN service from another MPLS VPN service provider. Therefore, this carrier has become a Second Carrier, while the MPLS VPN service provider is the First Carrier.

The First Carrier PE and Second Carrier CE will exchange (internal) routes via BGP. The Second Carrier will directly establish BGP neighbors between ASBRs to exchange external

routes. The traffic will flow from the external network into the Second Carrier network and be forwarded on the tunnel until the traffic leaves the Second Carrier network.

2.5.10.2 Network topology

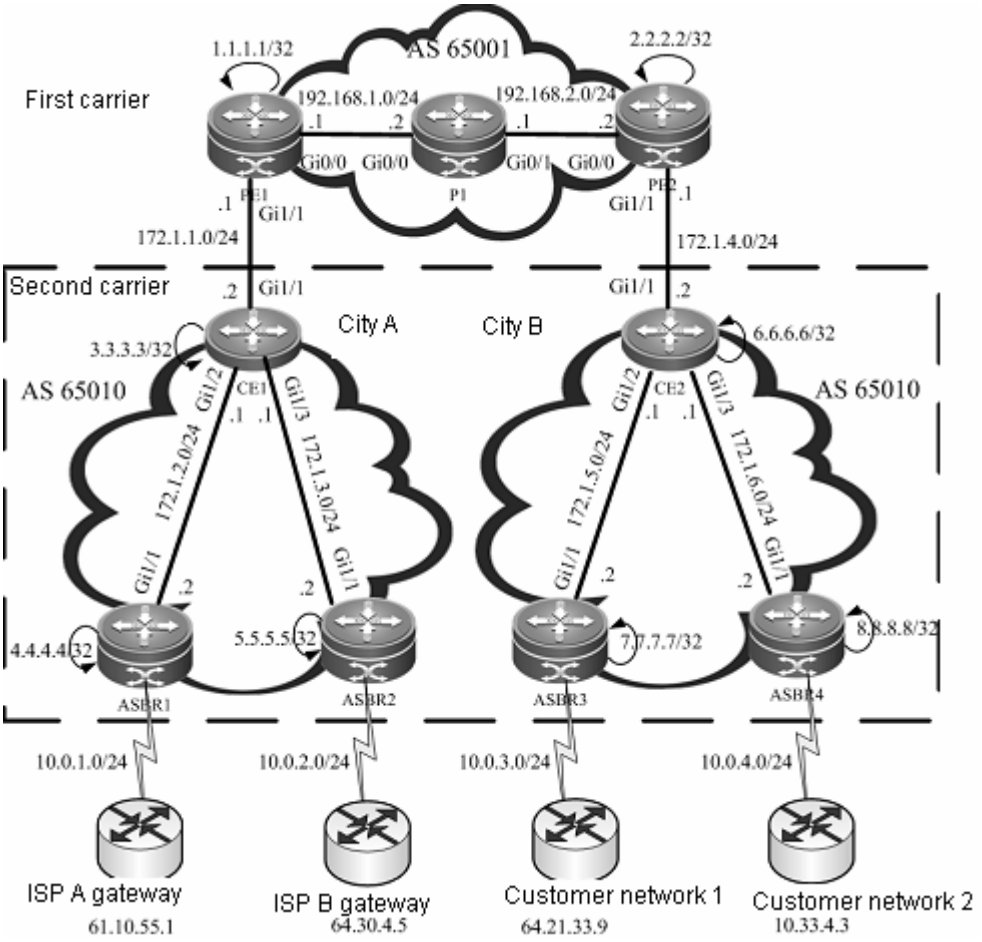


Fig 21 Network topology of scenario II

2.5.10.3 Configuration tips

Configure basic BGP/MPLS VPN for First Carrier

- Enable CSC function
- Configure Second Carrier
- Configure user access

2.5.10.4 Configuration steps

Configure basic BGP/MPLS VPN for First Carrier

The configuration steps are the same as Scenario I. The difference is that routes are exchanged between PE and CE. Only PE-CE route exchanging configurations will be shown below. For other configurations, please refer to the section of "Configuring Basic BGP/MPLS VPN Functions" for the example of "Second Carrier provides Internet service based on IP core".

Configure route exchanging between PE and CE

Configure on PE (taking PE1 as the example)

```
DES-7200(config)# router bgp 65001
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router-af)# neighbor 172.1.1.2 remote-as 65010
DES-7200(config-router-af)# neighbor 172.1.1.2 as-override
DES-7200(config-router-af)# exit
DES-7200(config-router)# exit
```

Then, configure on CE (taking CE1 as the example)

```
DES-7200(config)# router bgp 65010
DES-7200(config-router)# neighbor 172.1.1.2 remote-as 65001
DES-7200(config-router)# redistribute ospf 1
DES-7200(config-router)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# redistribute bgp 65010 subnets
DES-7200(config-router)# exit
```

Enable CSC function

Enable CSC on PE: Here we will take PE1 as the example. The configurations of PE2 are the same.

```
DES-7200(config)# interface gigabitEthernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip vrf forwarding vpn1
DES-7200(config-if)# ip address 172.1.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# router bgp 65001
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router-af)# neighbor 172.1.1.2 send-label
```

```
DES-7200(config-router-af)# exit
DES-7200(config-router)# exit
```

Enable MPLS and BGP label distribution on CE

```
DES-7200(config)# interface gigabitEthernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# label-switching
DES-7200(config-if)# ip address 172.1.1.2 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# router bgp 65010
DES-7200(config-router)# neighbor 172.1.1.1 send-label
DES-7200(config-router)# exit
```

Configure Second Carrier

Configure MPLS network: Please refer to the section of "Configure MPLS Network" for the example of "Second Carrier provides Internet service based on IP core". Configuration objects are CE1, CE2 and ASBRs (1-4).

Note

You need to enable LDP on CSC-CE in order to establish sessions with other intra-site devices in order to build MPLS network. If CSC-CE and CSC-PE use BGP to exchange routes, then you must execute "**advertise-labels for bgp-routes**" on CSC-CE to allow LDP to distribute labels for BGP routes.

Configure BGP neighbor: Establish BGP adjacency between two ASBRs.

Configure ASBR2 as the BGP neighbor on ASBR1. The configurations of other ASBRs are the same.

```
DES-7200(config)# router bgp 65010
DES-7200(config-router)# neighbor 5.5.5.5 remote-as 65010
DES-7200(config-router)# neighbor 5.5.5.5 update-source Loopback 0
DES-7200(config-router)# neighbor 5.5.5.5 next-hop-self
DES-7200(config-router)# exit
```

Configure user access

Please refer to the section of "Configure user access" for the example of "Second Carrier provides Internet service based on IP core".

2.5.10.5 Verification

Display VRF routes and labels on First Carrier PE: Here we will take PE1 as the example. The configurations of PE2 are the same.

// In the VRF routing table of PE1, there are only internal routes of the Second Carrier. There is no external routes (i.e.: 64.30.4.0/24).

```
DES-7200# show ip route vrf vpn1
Routing Table: vpn1

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
B    3.3.3.3/32 [200/0] via 172.1.1.2, 00:00:07
C    172.1.1.0/24 is directly connected, gigabitEthernet 1/1
C    172.1.1.1/32 is local host.
B    172.1.2.0/24 [200/0] via 172.1.1.2, 00:00:07
B    172.1.4.0/24 [200/0] via 2.2.2.2, 00:00:30
......
DES-7200# show bgp vpnv4 unicast vrf vpn1 labels
BGP table version is 1, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network         Next Hop       In Label/Out Label
Route Distinguisher: 65001:20 (Default for VRF vpn1)
*> 3.3.3.3/32      172.1.1.2        2048/1024
*> 172.1.2.0/24    172.1.1.2       2049/1025
*>i6.6.6.6/32      2.2.2.2          2050/2112
......
```

In ASBR and user network, display the routing table

// On ASBR (taking ASBR3 as the example)

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
```

```
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
......
B    61.10.55.0/24 [200/0] via 4.4.4.4, 00:00:40
B    64.21.33.0/24 [200/0] via 10.0.3.2, 00:00:31
......
```

// In the user network, we will take the edge device of user network 1 as the example

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
......
B    61.10.55.0/24 [200/0] via 10.0.3.1, 00:00:40
C    64.21.33.0/24 is directly connected, gigabitEthernet 0/1
C    64.21.33.9/32 is local host.
......
```

Verify that the external networks are interconnected

```
// On the edge device of user network 1
DES-7200# ping 61.10.55.1 source 64.21.33.9
Sending 5, 100-byte ICMP Echoes to 61.10.55.1, timeout is 2 seconds:
Packet sent with a source address of 64.21.33.9
  < press Ctrl+C to break >
!!!!!
```

2.5.11 CSC: Second Carrier provides VPN service based on MPLS core

2.5.11.1 Networking requirements

A carrier owns MPLS core network in City A and provides MPLS VPN service for users in this city. Now this carrier intends to expand service to City B, and has built MPLS core network in City B. In order to interconnect the core networks in these two cities, this carrier leases the VPN service from another MPLS VPN service provider, and thus forming the networking model of "Carrier's Carrier".

The First Carrier PE and Second Carrier CE will exchange (internal) routes via BGP. MP-IBGP neighbor is established between Second Carrier PEs to exchange user VPN routes. OSPF is deployed between Second Carrier PE and user VPN CE to exchange routes.

2.5.11.2 Network topology

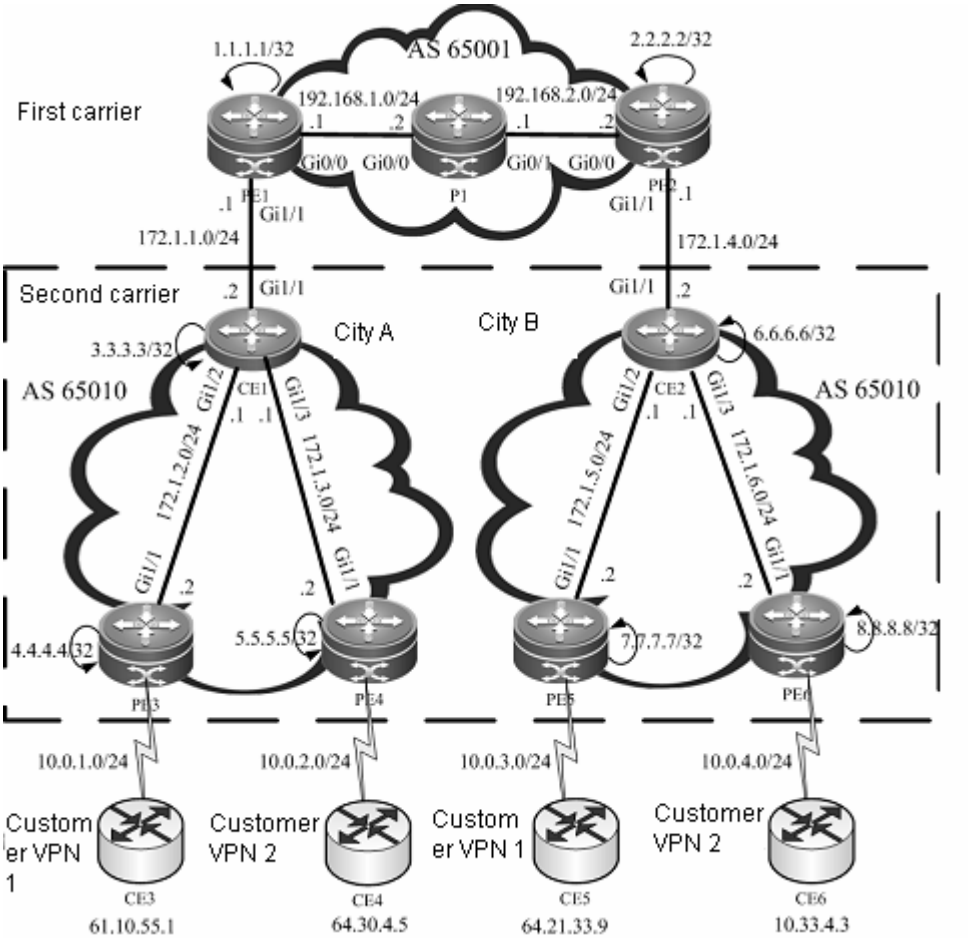


Fig 22 MPLS core second-level VPN provider

2.5.11.3 Configuration tips

Configure basic BGP/MPLS VPN for First Carrier

- Enable CSC function
- Configure Second Carrier
- Configure user access

2.5.11.4 Configuration steps

Configure basic BGP/MPLS VPN for First Carrier

Please refer to the section of "Configuring Basic BGP/MPLS VPN Functions" for the example of "Second Carrier provides Internet service based on MPLS core".

Enable CSC function

Please refer to the section of "Enable CSC Function" for the example of "Second Carrier provides Internet service based on MPLS core".

Configure Second Carrier

Configure MPLS network: Please refer to the section of "Configure MPLS Network" for the example of "Second Carrier provides Internet service based on IP core". Configuration objects are CE1, CE2 and PEs (3-6).

Note

You need to enable LDP on CSC-CE in order to establish sessions with other intra-site devices in order to build MPLS network. If CSC-CE and CSC-PE use BGP to exchange routes, then you must execute "**advertise-labels for bgp-routes**" on CSC-CE to allow LDP to distribute labels for BGP routes.

Configure MP-IBGP neighbor: Please refer to the section of "Configure MP-IBGP Neighbor" for the example of "Second Carrier provides Internet service based on IP core". Configure the MP-IBGP adjacencies between PE3, PE4, PE5 and PE6.

Configure user access

The configurations of this section involve VRF configuration, PE-CE route exchanging configuration and etc. These configurations are the same as that of BGP/MPLS VPN. Here we will connect CE3 with PE3.

On PE3

```
DES-7200(config)# ip vrf customer_vpn1
DES-7200(config-vrf)# rd 65010:1
DES-7200(config-vrf)# route-target both 65010:1
DES-7200(config-vrf)# exit
DES-7200(config)# interface gigabitEthernet 1/2
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable MPLS fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip vrf forwarding customer_vpn1
DES-7200(config-if)# ip address 10.0.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# router ospf 10 vrf customer_vpn1
DES-7200(config-router)# network 10.0.1.0 0.0.0.255 area 0
DES-7200(config-router)# redistribute bgp 65010 subnets
DES-7200(config-router)# exit
DES-7200(config)# router bgp 65010
DES-7200(config-router)# address-family ipv4 vrf customer_vpn1
DES-7200(config-router-af)# redistribute ospf 10 vrf customer_vpn1
DES-7200(config-router-af)# exit
DES-7200(config-router)# exit
```

On CE3

```
DES-7200(config)# interface gigabitEthernet 0/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 10.0.1.2 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config)# interface gigabitEthernet 0/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 61.10.55.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 10.0.1.0 0.0.0.255 area 0
DES-7200(config-router)# network 61.10.55.0 0.0.0.255 area 0
DES-7200(config-router)# exit
```

2.5.11.5 Verification

Display VRF routes and labels on First Carrier PE: Here we will take PE1 as the example. The configurations of PE2 are the same.

// In the VRF routing table of PE1, there are only internal routes of the Second Carrier. There is no VPN route (i.e.: 64.30.4.0/24).

```
DES-7200# show ip route vrf vpn1
Routing Table: vpn1

Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
B    3.3.3.3/32 [200/0] via 172.1.1.2, 00:00:07
C    172.1.1.0/24 is directly connected, gigabitEthernet 1/1
C    172.1.1.1/32 is local host.
B    172.1.2.0/24 [200/0] via 172.1.1.2, 00:00:07
B    172.1.4.0/24 [200/0] via 2.2.2.2, 00:00:30
......
DES-7200# show bgp vpnv4 unicast vrf vpn1 labels
BGP table version is 1, local router ID is 1.1.1.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
            S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network         Next Hop       In Label/Out Label
Route Distinguisher: 65001:20 (Default for VRF vpn1)
*> 3.3.3.3/32      172.1.1.2        2048/1024
```

```
*> 172.1.2.0/24     172.1.1.2       2049/1025
*>i6.6.6.6/32       2.2.2.2         2050/2112
......
```

In the VRF of Second Carrier PE and user VPN CE, display the routing table.

// On PE (taking PE3 as the example)

```
DES-7200# show ip route vrf customer_vpn1
Routing Table: customer_vpn1

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
......
O    61.10.55.0/24 [200/0] via 10.0.1.2, 00:00:40, gigabitEthernet 1/2
B    64.21.33.0/24 [200/0] via 7.7.7.7, 00:00:31
......
```

// In user VPN CE (taking CE3 as the example)

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
......
C    61.10.55.0/24 is directly connected, gigabitEthernet
C    61.10.55.1/32 is local host.
O    64.21.33.0/24 [200/0] via 10.0.1.1, 00:00:42, gigabitEthernet 0/0
......
```

Verify that the user VPN networks are interconnected

//On CE3

```
DES-7200# ping 64.21.33.9
Sending 5, 100-byte ICMP Echoes to 64.21.33.9, timeout is 2 seconds:
```

```
 < press Ctrl+C to break >
!!!!!
```

2.5.12 MPLS VPN over GRE

2.5.12.1 Networking requirements

In an IP core network, the edge router of PE supports MPLS VPN. Now it is required to use "MPLS VPN over GRE" to use the IP core network to provide MPLS VPN service for users. The IP core network adopts dual OSPF instances to introduce VPN traffic into the GRE tunnel, while PE and CE exchange routes via OSPF.

2.5.12.2 Network topology

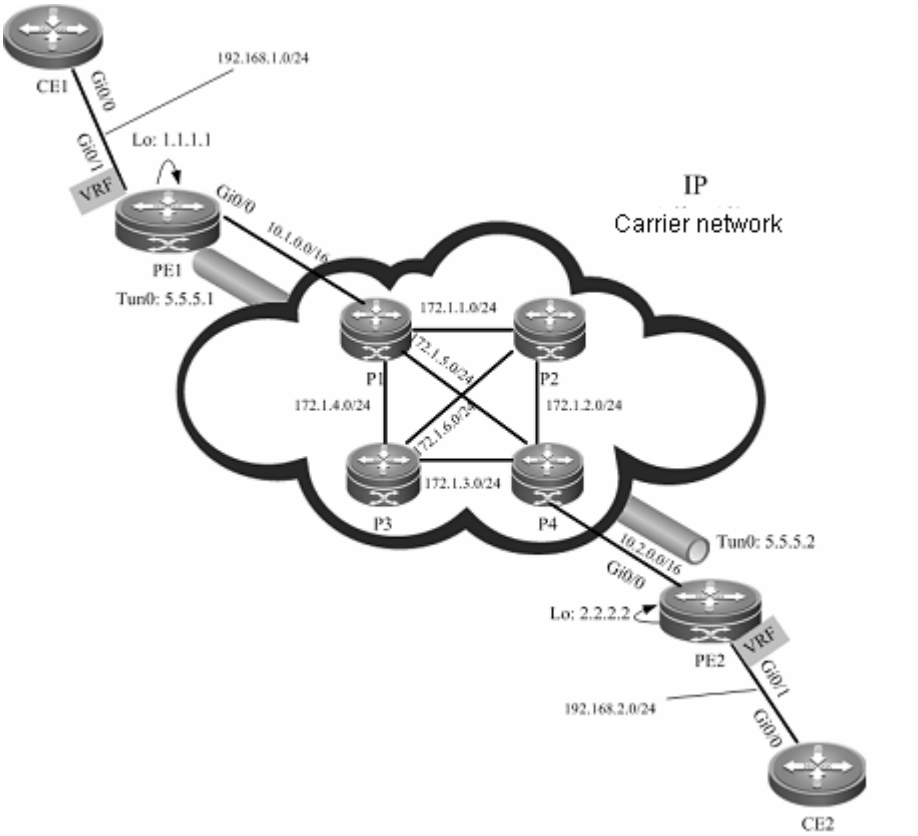


Fig 23 Network topology

2.5.12.3 Configuration tips

- Create GRE tunnel
- Configure IGP route

- Configure MPLS network
- Configure MPLS VPN

2.5.12.4 Configuration steps

Configure P device. Here we will take P1 as the example. The configurations of other devices are the same.

Configure interface and IP address

```
DES-7200(config)# interface gigabitEthernet 0/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 10.1.0.2 255.255.0.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet 0/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 172.1.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 172.1.5.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet 0/3
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 172.1.4.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
```

Configure IGP routing instance

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.1.1.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.1.5.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.1.4.0 0.0.0.255 area 0
DES-7200(config-router)# network 10.1.0.0 0.0.255.255 area 0
DES-7200(config-router)# exit
```

Configure PE device. Here we will take PE1 as the example. The configurations of other devices are the same.

Configure public-network interface and IP address

```
DES-7200(config)# interface Loopback 0
DES-7200(config-if)# ip address 1.1.1.1 255.255.255.255
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet 0/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 10.1.0.1 255.255.0.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
```

Create GRE tunnel

```
DES-7200(config)# interface tunnel 0
DES-7200(config-if)# ip address 5.5.5.1 255.255.255.0
DES-7200(config-if)# tunnel mode gre ip
DES-7200(config-if)# tunnel source 10.1.0.1
DES-7200(config-if)# tunnel destination 10.2.0.1
DES-7200(config-if)# exit
```

Configure IGP route

```
DES-7200(config)# router ospf 1
```

```
DES-7200(config-router)# network 10.1.0.0 0.0.255.255 area 0
DES-7200(config-router)# exit
DES-7200(config)# router ospf 2
DES-7200(config-router)# network 1.1.1.1 0.0.0.0 area 0
DES-7200(config-router)# network 5.5.5.0 0.0.0.255 area 0
DES-7200(config-router)# exit
```

Configure MPLS network

```
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface tunnel 0
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# mpls ip
DES-7200(config-if)# label-switching
DES-7200(config-if)# exit
```

Configure MPLS VPN

Configure VRF

```
DES-7200(config)# ip vrf vpn1
DES-7200(config-vrf)# rd 100:1
DES-7200(config-vrf)# route-target both 100:1
DES-7200(config-vrf)# exit
DES-7200(config)# interface gigabitEthernet 0/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip vrf forwarding vpn1
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
```

Configure MP-IBGP

```
DES-7200(config)# router bgp 100
DES-7200(config-router)# neighbor 2.2.2.2 remote-as 100
DES-7200(config-router)# neighbor 2.2.2.2 update-source Loopback 0
```

```
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 2.2.2.2 active
DES-7200(config-router-af)# neighbor 2.2.2.2 send-community both
DES-7200(config-router-af)# exit
DES-7200(config-router)# address-family ipv4 vrf vpn1
DES-7200(config-router-af)# redistribute ospf 10 vrf vpn1
DES-7200(config-router-af)# exit
DES-7200(config-router)# exit
```

Configure route exchanging between PE and CE

```
DES-7200(config)# router ospf 10 vrf vpn1
DES-7200(config-router)# network 192.168.1.0 0.0.0.255 area 0
DES-7200(config-router)# redistribute bgp 100 subnets
DES-7200(config-router)# exit
```

Configure CE. Here we will take CE1 as the example. The configurations of CE2 are the same.

```
DES-7200(config)# interface gigabitEthernet 0/0
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if)# ip ref
DES-7200(config-if)# ip address 192.168.1.2 255.255.255.0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# exit
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 192.168.1.0 0.0.0.255 area 0
DES-7200(config-router)# exit
```

2.5.12.5 Verification

On PE, check routing table entries. Here we will take PE1 as the example. The next-hop interface of route 2.2.2.2/32 is Tunnel 0.

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    10.1.0.0/16 is directly connected, gigabitEthernet 0/0
C    10.1.0.1/32 is local host.
```

```
C    1.0.0.0/8 is subnetted
C      1.1.1.1/32 is local host.
O    2.0.0.0/8 is subnetted
O      2.2.2.2/32 [110/11] via 5.5.5.2, 00:00:40, Tunnel 0
......
```

Verify VPN route on PE. Here we will take PE1 as the example.

```
DES-7200# show ip route vrf vpn1
Routing Table: vpn1

Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, gigabitEthernet 0/1
C    192.168.1.1/32 is local host.
B    192.168.2.0/24 [200/0] via 2.2.2.2, 00:00:41
......
```

Check MPLS forwarding table entries on PE. Here we will take PE1 as the example.

```
DES-7200# show mpls forwarding-table
Label Operation Code:
PH--PUSH label
PP--POP label
SW--SWAP label
SP—-SWAP topmost label and push new label
DP—-DROP packet
PC—-POP label and continue lookup( IP or Label )
PI--POP label and do ip lookup forward
PN--POP label and forward to nexthop
PM--POP label and do MAC lookup forward
PV--POP label and output to VC attach interface
IP--IP lookup forward
Local  Outgoing  OP  FEC        Outgoing      Next Hop
label  label                   interface
--     3         PH 2.2.2.2/32  Tunnel 0      5.5.5.2
--     21        PH 192.168.2.0/24(V) Tunnel 0  Point2point
```

```
......
```

Verify routing table on CE.

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default

Gateway of last resort is no set
C    192.168.1.0/24 is directly connected, gigabitEthernet 0/1
C    192.168.1.2/32 is local host.
O    192.168.2.0/24 [112/11] via 192.168.1.1, 00:00:41
......
```

Verify the intercommunication between CEs. On CE1:

```
DES-7200# ping 192.168.2.2
Sending 5, 100-byte ICMP Echoes to 192.168.2.2, timeout is 2 seconds:
  < press Ctrl+C to break >
!!!!!
```

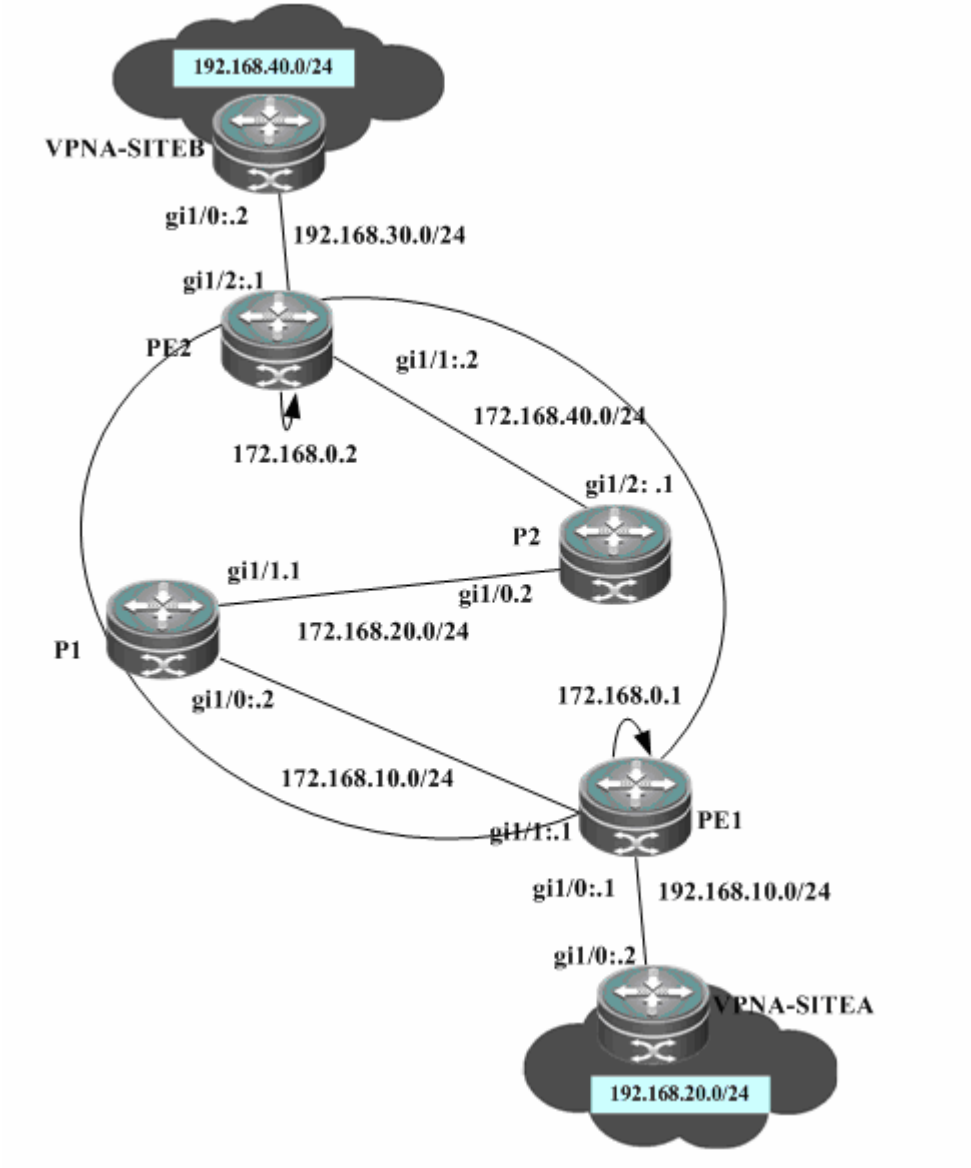
2.5.13 OSPF VPN configuration example

2.5.13.1 Domain-id configuration example

Networking requirements

Two different sites of the client exchange VPN routes via MPLS backbone network. Client sites are connected with PE via OSPF protocol. It is required that the client's OSPF routes can be restored to the OSPF routes of original site after being exchanged over MPLS backbone network.

Network topology



To meet such need, configure two VRF OSPF instances with same domain ID on two PEs, as shown below:

Configuration steps

SITEA:

Configure OSPF protocol between PE and CE

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
```

PE1:

Configure Loopback interface

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.1 255.255.255.255
```

Configure VRF

Create a VRF of " VPNA", define RD value and RT value, and associate VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# end
```

Associate the CE-connecting interface with VRF

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/0)# ip ref
DES-7200(config-if-GigabitEthernet 1/0)# ip vrf forwarding VPNA
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Configure BGP protocol to establish MP-IBGP session with PE2

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.2 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.2 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.2 activate
DES-7200(config-router-af)# end
```

Exchange routes with CE via OSPF protocol; configure the domain ID of OSPF instance to 10

```
DES-7200# configure terminal
```

```
DES-7200(config)# router ospf 10 VPNA
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# domain-id 10
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# redistribute ospf 10
DES-7200(config-router-af)# end
```

Configure MPLS signaling protocol for backbone network. Enable MPLS capability on WAN interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocol for the backbone network

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

P1:

P2:

The configuration steps are similar to that of P in the MPLS backbone network

SITEB:

Configure to run OSPF with PE2

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 192.168.30.0 255.255.255.0 area 0
```

PE2:

Configure Loopback interface

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.2 255.255.255.255
```

Configure VRF

Create a VRF of " VPNA", define RD value and RT value, and associate VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# exit
```

Associate the CE-connecting interface with VRF

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/2
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/2)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/2)# ip ref
DES-7200(config-if-GigabitEthernet 1/2)# ip vrf forwarding VPNA
DES-7200(config-if-GigabitEthernet 1/2)# ip address 192.168.30.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# exit
```

Configure BGP protocol to establish MP-IBGP session with PE2

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.1 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.1 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
```

```
DES-7200(config-router-af)# neighbor 172.168.0.1 activate
DES-7200(config-router-af)# end
```

Exchange VPN routes with CE via OSPF protocol; configure the domain ID to 10

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPNA
DES-7200(config-router)# network 192.168.30.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# domain-id 10
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# redistribute ospf 10
DES-7200(config-router-af)# exit
```

Configure MPLS signaling protocol for backbone network. Enable MPLS capability on WAN interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.40.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocol for the backbone network

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.40.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.2 0.0.0.0 area 0
DES-7200(config-router)# end
```

Verify configurations

VPNA-SITEB:

```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
C      192.168.30.0/24 is directly connected, Gi1/0
O      192.168.40.0/24 [110/101] via 192.168.24.2, 00:56:23, Gi1/1
O IA    192.168.20.0/24 [110/2] via 192.168.30.1, 00:00:36, Gi1/0
```

PE2:

```
DES-7200# show ip route vrf VPNA
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
C      192.168.30.0/24 is directly connected, Gi1/2
O      192.168.40.0/24 [110/101] via 192.168.30.2, 00:56:23, Gi1/2
B      192.168.20.0/24 [110/2] via 172.168.0.1, 00:00:36
```

PE1:

```
DES-7200# show ip route vrf VPNA
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
C      192.168.30.0/24 is directly connected, Gi1/2
B      192.168.40.0/24 [110/2] via 172.168.0.2, 00:00:36
```

```
O      192.168.20.0/24 [110/101] via 192.168.10.2, 00:56:23, Gi1/0
```

VPNA-SITEA:

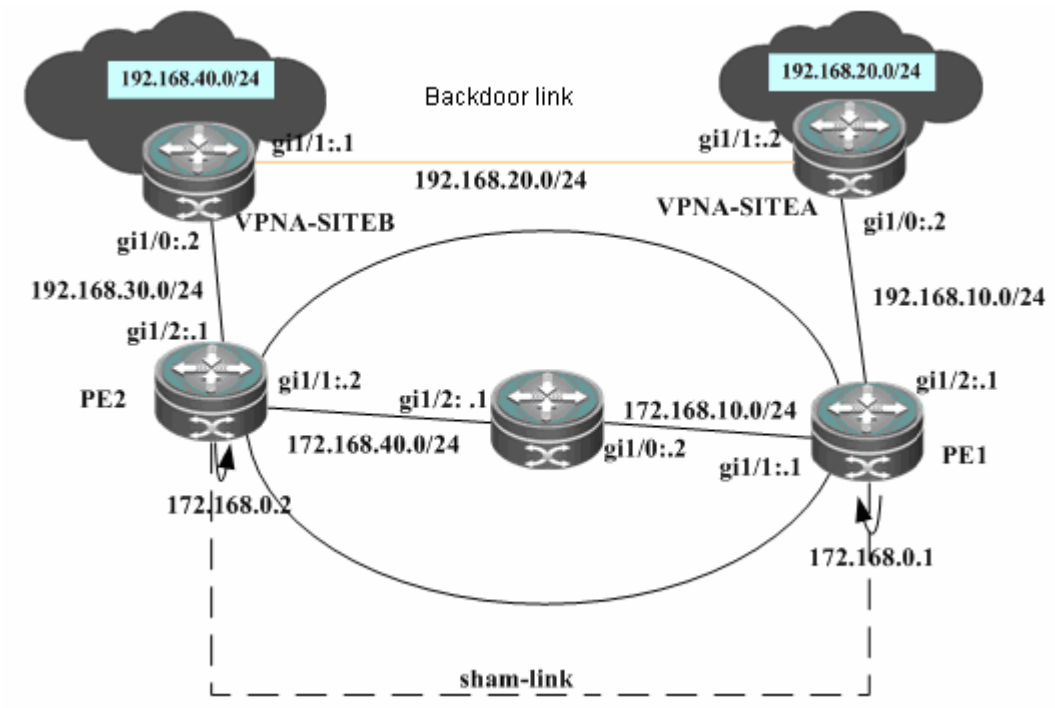
```
DES-7200# show ip route
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
C      192.168.10.0/24 is directly connected, Gi1/0
O      192.168.30.0/24 [110/101] via 192.168.23.2, 00:56:23, Gi1/1
O IA    192.168.40.0/24 [110/2] via 192.168.10.1, 00:00:36, Gi1/0
```

2.5.13.2 Sham-link configuration example

Networking requirements

Two different sites of the client exchange VPN routes via MPLS backbone network. At the same time, a "backdoor link" is also established between these two sites to ensure that information can still be exchanged between both sites through this backup link when the MPLS backbone network fails.

Network topology



Configuration steps

SITEA:

Configure to run OSPF protocol with PE1 and SITEB. The OSPF protocol runs over the backdoor link with SITEB.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
DES-7200(config-router)# network 192.168.20.0 255.255.255.0 area 0
```

Configure OSPF cost on interface

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/0)# ip ref
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.10.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# ip ospf cost 1
```

```
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 192.168.20.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# ip ospf cost 200
```

PE1:

Configure Loopback interface

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.1 255.255.255.255
```

Configure VRF

Create a VRF of " VPNA", define RD value and RT value, and associate VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# end
```

Associate the CE-connecting interface with VRF

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/2
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/2)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/2)# ip ref
DES-7200(config-if-GigabitEthernet 1/2)# ip vrf forwarding VPNA
DES-7200(config-if-GigabitEthernet 1/2)# ip address 192.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/2)# end
```

Configure VRF Loopback interface to establish sham-link

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 10
```

```
DES-7200(config-if-Loopback 10)# ip vrf forwarding VPNA
DES-7200(config-if-Loopback 10)# ip address 192.168.0.1 255.255.255.255
```

Configure BGP protocol to establish MP-IBGP session with PE2

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.2 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.2 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.2 activate
DES-7200(config-router-af)# end
```

Exchange routes with CE via OSPF protocol, and establish sham-link with the OSPF instance on PE2

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPNA
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# area 0 sham-link 192.168.0.1 192.168.0.2
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# redistribute ospf 10
DES-7200(config-router-af)# redistribute connected
DES-7200(config-router-af)# end
```

Configure MPLS signaling protocol for backbone network. Enable MPLS capability on WAN interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
```

```
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocol for the backbone network

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

P1:

The configuration steps are similar to that of P in the MPLS backbone network

SITEB:

Configure to run OSPF protocol with PE2 and SITEA. The OSPF protocol runs over the backup link with SITEA.

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10
DES-7200(config-router)# network 192.168.30.0 255.255.255.0 area 0
DES-7200(config-router)# network 192.168.20.0 255.255.255.0 area 0
```

Configure OSPF cost on interface

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/0)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/0)# ip ref
DES-7200(config-if-GigabitEthernet 1/0)# ip address 192.168.30.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/0)# ip ospf cost 1
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 192.168.20.2 255.255.255.0
```

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ospf cost 200
```

PE2:

Configure Loopback interface

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.2 255.255.255.255
```

Configure VRF

Create a VRF of " VPNA", define RD value and RT value, and associate VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPNA
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# exit
```

Associate the CE-connecting interface with VRF

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/2
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/2)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/2)# ip ref
DES-7200(config-if-GigabitEthernet 1/2)# ip vrf forwarding VPNA
DES-7200(config-if-GigabitEthernet 1/2)# ip address 192.168.30.1
255.255.255.0
DES-7200(config-if-GigabitEthernet 1/2)# exit
```

Configure VRF Loopback interface to establish sham-link

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 10
DES-7200(config-if-Loopback 10)# ip vrf forwarding VPNA
DES-7200(config-if-Loopback 10)# ip address 192.168.0.2 255.255.255.255
```

Configure BGP protocol to establish MP-IBGP session with PE2 and PE3

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.1 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.1 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.1 activate
DES-7200(config-router-af)# end
```

Exchange VPN routes with CE via OSPF protocol, and establish sham-link with PE1

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPNA
DES-7200(config-router)# network 192.168.30.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# area 0 sham-link  192.168.0.2 192.168.0.1
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# redistribute ospf 10
uijie(config-router-af)# redistribute connected
DES-7200(config-router-af)# exit
```

Configure MPLS signaling protocol for backbone network. Enable MPLS capability on WAN interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.40.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocol for the backbone network

```
DES-7200# configure terminal
```

```
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.40.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.2 0.0.0.0 area 0
DES-7200(config-router)# end
```

Verify configurations

PE1

```
DES-7200# show ip ospf 10 sham-links
Sham Link OSPF_SL0 to address 192.168.0.2 is up
Area 0 source address 192.168.0.1
  Run as demand circuit
  DoNotAge LSA allowed. Cost of using 1 State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Hello due in 00:00:06
    Adjacency State FULL (Hello suppressed)
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
DES-7200# show ip ospf 10 neighbor
Neighbor ID     Pri   State          Dead Time   Address         Interface
192.168.0.2       0   FULL/  -          -       192.168.0.2     OSPF_SL0
DES-7200# show ip route vrf VPNA
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
C       192.168.10.0/24 is directly connected, Gi1/2
O       192.168.20.0/24 [110/101] via 192.168.1.2, 00:56:23, Gi1/2
O       192.168.40.0/24 [110/2] via 172.168.0.2, 00:00:36
```

PE2

```
DES-7200# show ip ospf 10 sham-links
Sham Link OSPF_SL0 to address 192.168.0.1 is up
Area 0 source address 192.168.0.2
```

```
  Run as demand circuit
  DoNotAge LSA allowed. Cost of using 1 State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
    Hello due in 00:00:06
    Adjacency State FULL (Hello suppressed)
    Index 2/2, retransmission queue length 0, number of retransmission 0
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 0, maximum is 0
Last retransmission scan time is 0 msec, maximum is 0 msec
```

DES-7200# show ip ospf 10 neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.0.1	0	FULL/ -	-	192.168.0.1	OSPF_SL0

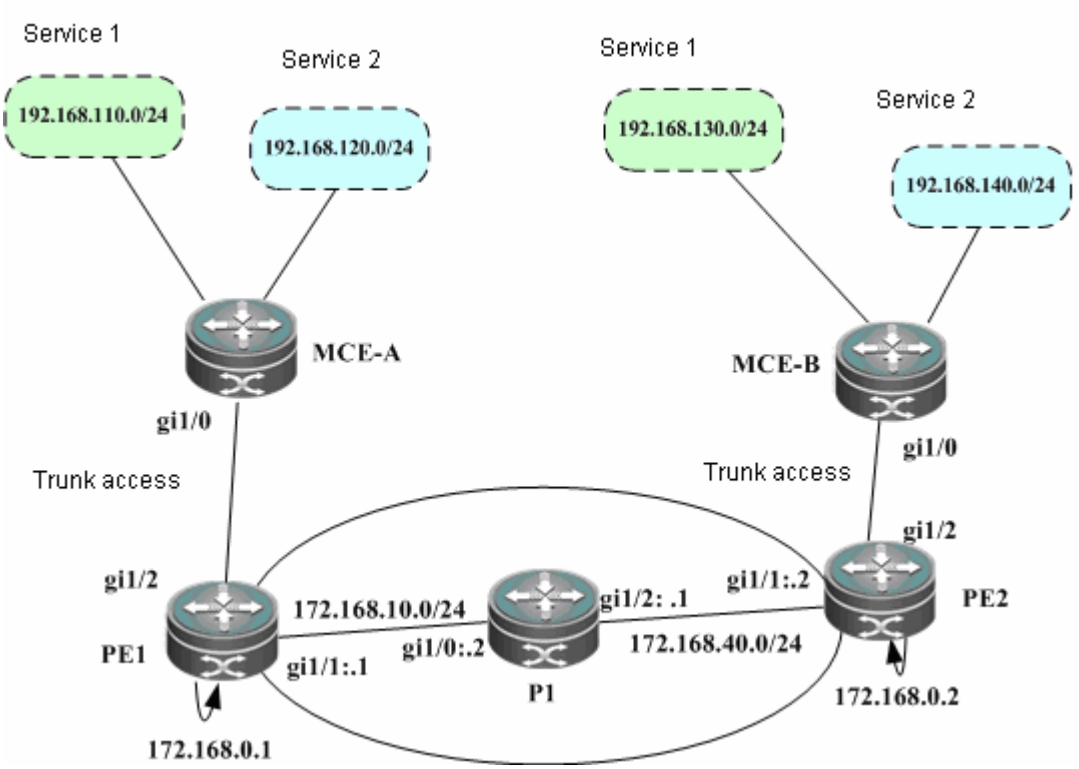
```
DES-7200# show ip route vrf VPNA
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
C       192.168.30.0/24 is directly connected, Gi1/2
O       192.168.40.0/24 [110/101] via 192.168.30.2, 00:56:23, Gi1/2
O       192.168.20.0/24 [110/2] via 172.168.0.1, 00:00:36
```

2.5.13.3 Configure multiple OSPF instances on MCE

Networking requirements

The client site involves multiple services, with same service communicating with each other over MPLS backbone network and different services isolated from each other.

Network topology



Configuration steps

MCE-A:

Configure Trunk link between PE and CE

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the routing interface to connect with PE.

```
DES-7200(config-if-GigabitEthernet 1/0)# switchport mode trunk
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Configure tow VRFs to represent different services and bind respective interfaces

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPN1
DES-7200(config-vrf)# exit
```

```
DES-7200(config)# VLAN 10
DES-7200(config)# interface vlan 10
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the subinterface to bind VRF.

```
DES-7200(config-if-vlan 10)# ip vrf forwarding VPN1
DES-7200(config-if-vlan 10)# ip address 192.168.10.2 255.255.255.0

DES-7200(config)# ip vrf VPN2
DES-7200(config-vrf)# exit
DES-7200(config)# VLAN 20
DES-7200(config)# interface vlan 20
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the sub-interface to bind VRF.

```
DES-7200(config-if-vlan 20)# ip vrf forwarding VPN2
DES-7200(config-if-vlan 20)# ip address 192.168.20.2 255.255.255.0
```

Configure to run OSPF protocol with PE for two VRFs

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPN1
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
DES-7200(config-router)# capability vrf-lite

DES-7200(config)# router ospf 10 VPN2
DES-7200(config-router)# network 192.168.20.0 255.255.255.0 area 0
DES-7200(config-router)# capability vrf-lite
```

PE1:

Configure Loopback interface

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.1 255.255.255.255
```

Configure Trunk link between PE and CE

```
DES-7200(config)# interface gigabitethernet 1/2
DES-7200(config-if-GigabitEthernet 1/2)# switchport mode trunk
DES-7200(config-if-GigabitEthernet 1/2)# end
```

Configure VRF

Create two VRFs of "VPN1" and "VPN2" to represent different services, and associate VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPN1
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# end
DES-7200# configure terminal
DES-7200(config)# ip vrf VPN2
DES-7200(config-vrf)# rd 1:200
DES-7200(config-vrf)# route-target both 1:200
DES-7200(config-vrf)# end
```

Associate the CE-connecting interface with VRF

```
DES-7200(config)# VLAN 10
DES-7200(config)# interface vlan 10
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the subinterface to bind VRF.

```
DES-7200(config-if-vlan 10)# ip vrf forwarding VPN1
DES-7200(config-if-vlan 10)# ip address 192.168.10.1 255.255.255.0
```

```
DES-7200(config)# VLAN 20
DES-7200(config)# interface vlan 20
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the sub-interface to bind VRF.

```
DES-7200(config-if-vlan 20)# ip vrf forwarding VPN1
DES-7200(config-if-vlan 20)# ip address 192.168.20.1 255.255.255.0
```

Configure BGP protocol to establish MP-IBGP session with PE2

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.2 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.2 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
```

```
DES-7200(config-router-af)# neighbor 172.168.0.2 activate
DES-7200(config-router-af)# end
```

Exchange routes with CE via OSPF protocol

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPN1
DES-7200(config-router)# network 192.168.10.0 255.255.255.0 area 0
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPNA
DES-7200(config-router-af)# redistribute ospf 10
DES-7200(config-router-af)# redistribute connected
DES-7200(config-router-af)# end

DES-7200# configure terminal
DES-7200(config)# router ospf 20 VPN2
DES-7200(config-router)# network 192.168.20.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPN2
DES-7200(config-router-af)# redistribute ospf 20
DES-7200(config-router-af)# redistribute connected
DES-7200(config-router-af)# end
```

Configure MPLS signaling protocol for backbone network. Enable MPLS capability on WAN interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.10.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
```

```
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocol for the backbone network

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.10.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.1 0.0.0.0 area 0
DES-7200(config-router)# end
```

P1:

The configuration steps are similar to that of P in the MPLS backbone network

SITEB:

Configure Trunk link between PE and CE

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitethernet 1/0
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the routing interface to connect with PE.

```
DES-7200(config-if-GigabitEthernet 1/0)# switchport mode trunk
DES-7200(config-if-GigabitEthernet 1/0)# end
```

Configure tow VRFs to represent different services and bind respective interfaces

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPN1
DES-7200(config-vrf)# exit
DES-7200(config)# VLAN 10
DES-7200(config)# interface vlan 30
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the subinterface to bind VRF.

```
DES-7200(config-if-vlan 10)# ip vrf forwarding VPN1
DES-7200(config-if-vlan 10)# ip address 192.168.30.2 255.255.255.0

DES-7200(config)# ip vrf VPN2
DES-7200(config-vrf)# exit
```

```
DES-7200(config)# VLAN 40
DES-7200(config)# interface vlan 40
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the sub-interface to bind VRF.

```
DES-7200(config-if-vlan 20)# ip vrf forwarding VPN2
DES-7200(config-if-vlan 20)# ip address 192.168.40.2 255.255.255.0
```

Configure to run OSPF protocol with PE for two VRFs

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPN1
DES-7200(config-router)# network 192.168.30.0 255.255.255.0 area 0
DES-7200(config-router)# capability vrf-lite

DES-7200(config)# router ospf 10 VPN2
DES-7200(config-router)# network 192.168.40.0 255.255.255.0 area 0
DES-7200(config-router)# capability vrf-lite
```

PE2:

Configure Loopback interface

```
DES-7200# configure terminal
DES-7200(config)# interface loopback 0
DES-7200(config-if-Loopback 0)# ip address 172.168.0.2 255.255.255.255
```

Configure Trunk link between PE and CE

```
DES-7200(config)# interface gigabitethernet 1/2
DES-7200(config-if-GigabitEthernet 1/2)# switchport mode trunk
DES-7200(config-if-GigabitEthernet 1/2)# end
```

Configure VRF

Create two VRFs of "VPN1" and "VPN2" to represent different services, and associate VRF with the corresponding interface.

```
DES-7200# configure terminal
DES-7200(config)# ip vrf VPN1
DES-7200(config-vrf)# rd 1:100
DES-7200(config-vrf)# route-target both 1:100
DES-7200(config-vrf)# end
DES-7200# configure terminal
```

```
DES-7200(config)# ip vrf VPN2
DES-7200(config-vrf)# rd 1:200
DES-7200(config-vrf)# route-target both 1:200
DES-7200(config-vrf)# end
```

Associate the CE-connecting interface with VRF

```
DES-7200(config)# VLAN 30
DES-7200(config)# interface vlan 30
```

VLAN is the configuration command used on switch products, and is not applicable to routers (except for the switching card interface). Routers can use the subinterface to bind VRF.

```
DES-7200(config-if-vlan 10)# ip vrf forwarding VPN1
DES-7200(config-if-vlan 10)# ip address 192.168.30.1 255.255.255.0
```

```
DES-7200(config)# VLAN 40
DES-7200(config)# interface vlan 40
```

VLAN is the configuration command used on switch products, and is not applicable to routers. Routers can use the sub-interface to bind VRF.

```
DES-7200(config-if-vlan 20)# ip vrf forwarding VPN2
DES-7200(config-if-vlan 20)# ip address 192.168.40.1 255.255.255.0
```

Configure BGP protocol to establish MP-IBGP session with PE2

```
DES-7200# configure terminal
DES-7200(config)# router bgp 1
DES-7200(config-router)# neighbor 172.168.0.1 remote-as 1
DES-7200(config-router)# neighbor 172.168.0.1 update-source loopback 0
DES-7200(config-router)# address-family vpnv4
DES-7200(config-router-af)# neighbor 172.168.0.1 activate
DES-7200(config-router-af)# end
```

Exchange routes with CE via OSPF protocol

```
DES-7200# configure terminal
DES-7200(config)# router ospf 10 VPN1
DES-7200(config-router)# network 192.168.30.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPN1
```

```
DES-7200(config-router-af)# redistribute ospf 10
DES-7200(config-router-af)# redistribute connected
DES-7200(config-router-af)# end

DES-7200# configure terminal
DES-7200(config)# router ospf 20 VPN2
DES-7200(config-router)# network 192.168.40.0 255.255.255.0 area 0
DES-7200(config-router)# redistribute bgp subnets
DES-7200(config-router)# exit
DES-7200(config)# router bgp 1
DES-7200(config-router)# address-family ipv4 vrf VPN2
DES-7200(config-router-af)# redistribute ospf 20
DES-7200(config-router-af)# redistribute connected
DES-7200(config-router-af)# end
```

Configure MPLS signaling protocol for backbone network. Enable MPLS capability on WAN interface.

```
DES-7200# configure terminal
DES-7200(config)# mpls ip
DES-7200(config)# mpls router ldp
DES-7200(config-mpls-router)# ldp router-id interface loopback 0 force
DES-7200(config-mpls-router)# exit
DES-7200(config)# interface gigabitethernet 1/1
```

In case of a switch, configure the interface to RoutedPort interface (not applicable to a router)

```
DES-7200(config-if-GigabitEthernet 1/1)# no switchport
```

In case of a router, enable fast forwarding on the interface (not applicable to a switch)

```
DES-7200(config-if-GigabitEthernet 1/1)# ip ref
DES-7200(config-if-GigabitEthernet 1/1)# ip address 172.168.40.2 255.255.255.0
DES-7200(config-if-GigabitEthernet 1/1)# label-switching
DES-7200(config-if-GigabitEthernet 1/1)# mpls ip
DES-7200(config-if-GigabitEthernet 1/1)# end
```

Configure routing protocol for the backbone network

```
DES-7200# configure terminal
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 172.168.40.0 0.0.0.255 area 0
DES-7200(config-router)# network 172.168.0.2 0.0.0.0 area 0
DES-7200(config-router)# end
```

Verify configurations

MCEA

```
DES-7200# show ip route vrf VPN1
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
C      192.168.10.0/24 is directly connected, VLAN 10
O      192.168.110.0/24 [110/101] via 192.168.21.2, 00:56:23, Gi1/1
O E2   192.168.130.0/24 [110/2] via 192.168.10.1, 00:00:36, VLAN 10

DES-7200# show ip route vrf VPN2
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
C      192.168.20.0/24 is directly connected, VLAN 20
O      192.168.120.0/24 [110/101] via 192.168.22.2, 00:56:23, Gi1/2
O E2   192.168.140.0/24 [110/2] via 192.168.20.1, 00:00:36, VLAN 20
```

MCEB

```
DES-7200# show ip route vrf VPN1
Codes:  C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default
C      192.168.30.0/24 is directly connected, VLAN 30
O      192.168.130.0/24 [110/101] via 192.168.23.2, 00:56:23, Gi1/1
O E2   192.168.110.0/24 [110/2] via 192.168.30.1, 00:00:36, VLAN 30

DES-7200# show ip route vrf VPN2
```

```
Codes:  C - connected, S - static, R - RIP, B - BGP
        O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default
C       192.168.40.0/24 is directly connected, VLAN 40
O       192.168.140.0/24 [110/101] via 192.168.24.2, 00:56:23, Gi1/2
O E2    192.168.140.0/24 [110/2] via 192.168.40.1, 00:00:36, VLAN 40
```

3 MPLS Reliability Configuration

3.1 MPLS GR Configuration

3.1.1 LDP GR Configuration

3.1.1.1 Introduction to LDP GR

Overview

IETF has expanded the MPLS signaling protocol of LDP. When the LDP protocol of certain device restarts, the neighboring devices can be advertised to retain MPLS forwarding data related to this device within a certain period and mark them as "stale". After restart of LDP protocol, the neighboring devices will help with message synchronization so that the device can restore to the state before restart within the shortest time. During the whole process of LDP restart, the packet forwarding path remains unchanged, and the entire system can forward data in a non-stop way, providing high reliability for various application services of MPLS.

Basic concepts of LDP GR

GR routers by capability

In terms of GR capability, there are GR-Capable router, GR-Aware router and GR-Unaware router.

GR-Capable router

The router with GR capability. Generally, such router has dual management boards (1+1 redundancy). During main-slave management board switchover, it can advertise its adjacent neighbors to keep its forwarding data and then rebuild the routing table after switchover without causing route oscillation. The packet forwarding path remains unchanged, and the entire system can forward data in a non-stop way.

GR-Aware router

The router with GR detection capability. Such router may not have dual management boards, but it can detect that its neighbor is experiencing GR and help its neighbor to complete GR.

GR-Unaware router

The router without GR detection capability. It cannot detect that the neighboring router is experiencing GR and cannot help the neighboring router to complete GR. This is generally because the no GR feature is provided by the system software or the GR feature is disabled.

GR routers by role

During the process of router restart, routers can be classified into GR-Restarter router and GR-Helper router according to router's role.

GR-Restarter router

GR-Restarter router must be a GR-Capable router, and the restart process is triggered by the administrator or fault.

GR-Helper router

Neighbor of GR-Restarter, at least a GR-Aware router.

Working principle

To establish a GR-Capable LDP session, LDP GR must be enabled at both ends of the session. During the process of establishing LDP session, if GR is not supported by any one end, then only ordinary LDP session can be established. If the session initiator supports and enables LDP GR, then FT Session TLV may be carried in the Initialization message.

When LDP session is established, if the acceptor receives Initialization message carrying FT Session TLV, it will determine whether or not to carry FT Session TLV in the Initialization message according to its own situation. If the acceptor supports and enables LDP GR, then it will carry FT Session TLV in the Initialization message in order to establish a GR-Capable LDP session. Otherwise, the acceptor will not carry FT Session TLV in the Initialization message in order to establish an ordinary LDP session without GR capability. If the Initialization message received by the acceptor doesn't carry FT Session TLV, then an ordinary LDP session without GR capability will be established no matter it carries FT Session TLV in the Initialization message or not. The following flowchart shows the process of establishing a session between two LDP GR-Capable LSRs.

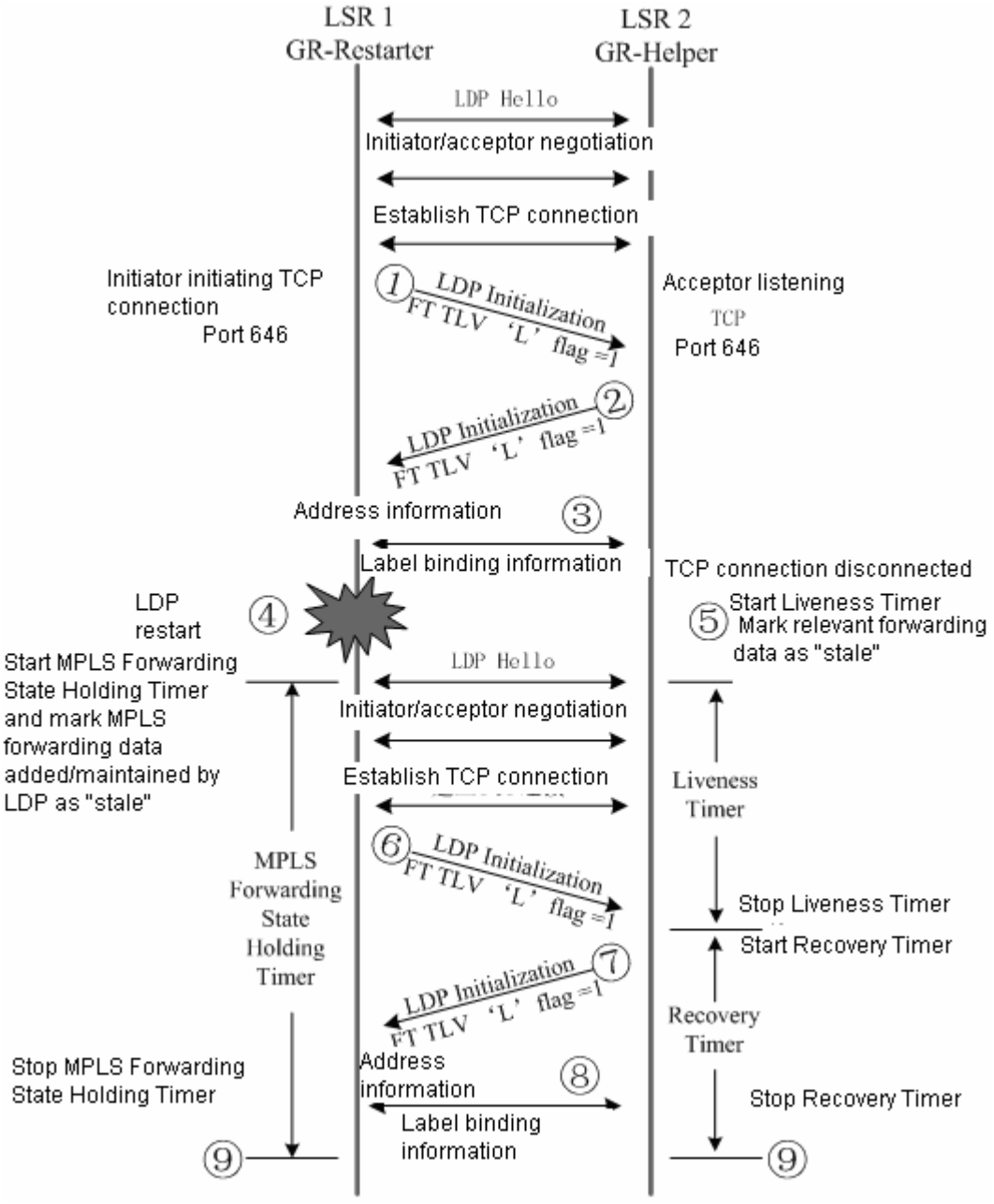


Fig 18 LDP GR flowchart

1) LSR 1 carries the optional parameter of FT Session TLV in the Initialization message to indicate its support to LDP GR.

2) LSR 2 receives the Initialization message carrying FT Session TLV. Since LSR 2 supports LDP GR, it will also carry the optional parameter of FT Session TLV in the Initialization message. After LSR 1 receives the Initialization message from LSR 2, a GR-Capable LDP session is established.

3) LSR1 and LSR2 exchanges address information and label mapping information.

4) For some reason, LDP on LSR1 is restarted. LSR1 retains all MPLS forwarding data added/maintained by LDP and mark them as "stale", and enables MPLS Forwarding State Holding Timer.

5) The LDP GR-Capable LSR 2 detects that its GR-Capable LDP session with LSR 1 is disconnected, and therefore retains the MPLS forwarding data related to this session and marks them as "stale". Meanwhile, it will use the lesser value of Liveness Timer configured and FT Reconnect Timeout in the FT Session TLV received to start the Liveness Timer, and retains these "stale" forwarding data before the timer is triggered.

6) When LSR 1 reestablishes session with LSR 2, it will set the Recovery Time in FT Session TLV carried by Initialization message to the residual value of MPLS Forwarding State Holding Timer.

7) LSR 2 receives the Initialization message carrying FT Session TLV sent by LSR 1 and detects that the Recovery Time is not 0. It will continue to retain the "stale" forwarding data and stop Liveness Timer at the same time. Meanwhile, it will use the lesser value of Recovery Timer configured and the Recovery Time in the FT Session TLV received to start the Recovery Timer, and retains these "stale" forwarding data before the timer is triggered.

8) LSR 1 and LSR 2 re-exchange address information and label mapping information, and remove or retain MPLS forwarding data marked as "stale" according to the information exchanged.

9) GR process ends. LSR 1 and LSR 2 will delete their own MPLS forwarding data marked as "stale".

Protocol specification

Related protocol specifications include:

- RFC3036: LDP Specification
- RFC3037: LDP Applicability
- RFC3215: LDP State Machine
- RFC3478: Graceful Restart Mechanism for Label Distribution Protocol
- RFC3479: Fault Tolerance for the Label Distribution Protocol (LDP)

3.1.1.2 Configure LDP GR

The following sections describe how to configure LDP GR:

Create configuration tasks

Default configurations

Enable LDP GR protocol

(Optional) Configure relevant parameters of LDP GR

- Display configurations

Create configuration tasks

- Application environment

In order to retain the adjacency and session information between routers while MPLS device fails and restore session connection and label information thereafter, MPLS LDP GR must be configured.

- Prerequisites

Before configuring MPLS LDP GR, the following configuration tasks must be completed:

- Configure IGP GR
- Configure MPLS LDP session

- Data preparation

Before configuring MPLS LDP GR, the following data must be prepared:

- LDP session reconnection timer
- LDP neighbor liveness timer
- LDP session recovery timer

Default configurations

The following table describes the default configurations of LDP GR.

Function	Default setting
LDP session reconnection timer	300 seconds
LDP neighbor liveness timer	120 seconds
LDP recovery time	120 seconds

Enable LDP GR protocol

By default, LDP GR capability is disabled on the device. To enable LDP GR capability of the device, enter privileged user mode and execute the following steps to enable LDP GR.

Command	Function
DES-7200#**configure teminal**	Enter global configuration mode.
DES-7200(config)#**mpls ip**	Enable global MPLS forwarding.
DES-7200(config)#**interface** type ID	Enter interface configuration mode.
DES-7200(config-if-type ID)#**no switchport**	Switch configuration. Configure to layer-3 interface.
DES-7200(config-if-type ID)#**mpls ip**	Enable LDP forwarding on the interface.
Or:	
DES-7200(config-if-type ID)#**mpls ip**	Router configuration. Enable LDP forwarding on the interface.
DES-7200(config-if-type ID)#**ip ref**	Enable fast forwarding on the interface.
DES-7200(config-if-type ID)#**label-switching**	Enable MPLS packet processing on the interface.
DES-7200(config)#**mpls router ldp**	Enter LDP configuration mode.
DES-7200(config-mpls-router)#**ldp router-id** *Loopback ID* **force**	Configure Route ID to Loopback ID (effective immediately).
DES-7200(config-mpls-router)#**graceful-restart**	Enable LDP GR. By default, LDP GR is disabled.
DES-7200(config-mpls-router)#**end**	Exit LDP configuration mode.
DES-7200#**show mpls ldp graceful-restart**	Display LDP GR session and session parameters.

To disable LDP GR, execute "**no graceful-restart**" command.

Note

The LDP session won't be affected by enabling LDP GR, namely it will cause the LDP session to restart. LDP GR will only come into effect after restarting LDP session.

(Optional) Configure relevant parameters of LDP GR

Enter LDP configuration mode on the device and configure relevant parameters of LDP GR:

Command	Function
DES-7200#**configure teminal**	Enter global configuration mode.
DES-7200(config)#**mpls router ldp**	Enable LDP protocol and enter LDP configuration mode.
DES-7200(config-mpls-router)#**graceful-restart timer reconnect** *seconds*	Configure LDP session reconnection timer. By default, the reconnection time is 300 seconds.
DES-7200(config-mpls-router)#**graceful-restart timer neighbor-liveness** *seconds*	Configure LDP neighbor liveness timer. By default, the LDP neighbor liveness time is 120 seconds.
DES-7200(config-mpls-router)#**graceful-restart timer recovery** *seconds*	Configure LDP recovery timer. By default, the LDP recovery time is 120 seconds.
DES-7200(config-mpls-router)#**end**	Exit LDP configuration mode.
DES-7200#**show mpls ldp graceful-restart**	Display LDP GR session and session parameters.

To reset relevant parameters of LDP GR, execute the following commands: no graceful-restart timer reconnect, no graceful-restart timer neighbor-liveness and no graceful-restart timer recovery.

Display configurations

The following commands are provided by LDP GR to display various configurations and status information. Their descriptions are given below:

Command	Function

show mpls ldp graceful-restart	Display LDP GR session and session parameters.
show mpls ldp bindings [**all | vrf** *vrf-name*] [*ip-address/mask*] [**label** *label*] [**remote | local**]	Display label-FEC bindings.
show mpls ldp neighbor [**all | vrf** *vrf-name*] [**graceful-restart** | **detail**]	Display LDP neighbor status.

3.1.1.3 Typical LDP GR configuration example

Networking requirements

1) A MPLS network is formed by PEs and P device.

2) Besides supporting LDP protocol, PEs and P device are GR-Capable.

3) PE1 and P device are hereby taken as the examples to describe LDP GR configurations on PE1 and P device. PE1 is a GR-Capable router playing the role of GR-Restarter; P device is a GR-Aware router playing the role of GR-Helper.

Network topology

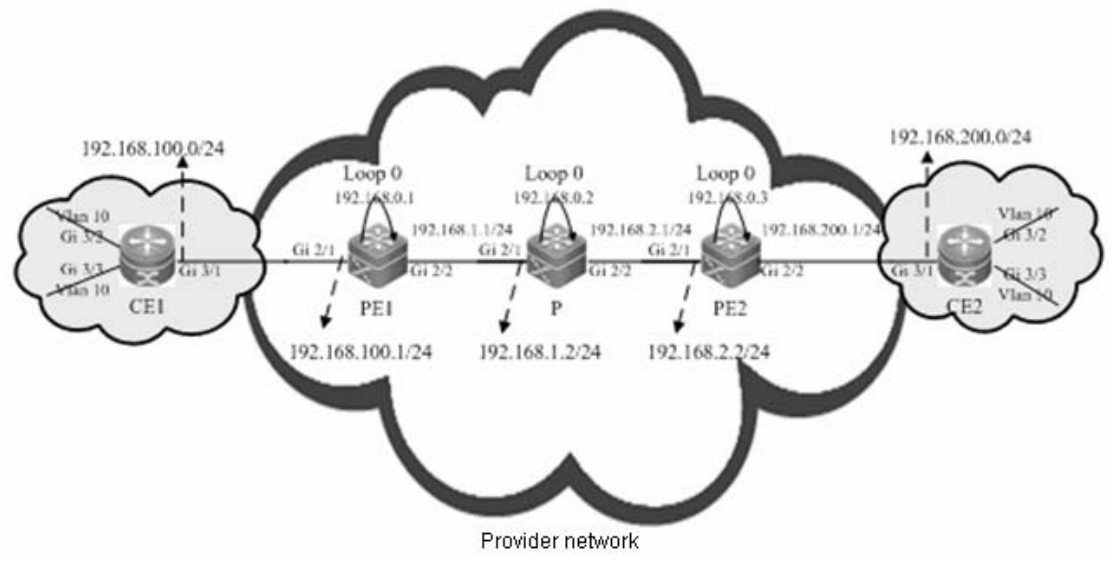


Fig 19 Network topology

Configuration tips

Configuration tips for PE1 and P device are shown below:

1) Configure IP address and OSPF protocol on the interface.
2) Configure global and interface MPLS capability.
3) Configure LDP protocol so that the network can forward MPLS traffic.
4) Enable LDP GR protocol
5) Configure relevant parameters of LDP GR protocol.
6) Restart LDP session to effect the configurations.

Configuration steps

1) Configure IP address and OSPF protocol on the interface.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 2/1
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 2/1)#no switchport
DES-7200(config-if-GigabitEthernet 2/1)#ip address 192.168.100.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 2/1)#exit
DES-7200(config)#interface gigabitEthernet 2/2
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 2/2)#no switchport
DES-7200(config-if-GigabitEthernet 2/2)#ip address 192.168.1.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 2/2)#exit
DES-7200(config)#interface loopback 0
DES-7200(config-Loopback 0)#ip address 192.168.0.1 255.255.255.255
DES-7200(config-Loopback 0)#exit
DES-7200(config)#router ospf 1
Router(config-router)#network 192.168.100.1 255.255.255.0 area 0
Router(config-router)#network 192.168.1.1 255.255.255.0 area 0
Router(config-router)#network 192.168.0.1 255.255.255.255 area 0
Router(config-router)#exit
```

Configure P. The configurations of P device are the same as that of PE1.

2) Configure global and interface MPLS capability.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 2/2
DES-7200(config-if-GigabitEthernet 2/2)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
Router(config-if-GigabitEthernet 2/2)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
DES-7200(config-if-GigabitEthernet 2/2)#ip ref
Router(config-if-GigabitEthernet 2/2)#exit
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 2/1
DES-7200(config-if-GigabitEthernet 2/1)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 2/1)#mpls ip
Router(config-if-GigabitEthernet 2/1)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 2/1)#mpls ip
DES-7200(config-if-GigabitEthernet 2/1)#ip ref
Router(config-if-GigabitEthernet 2/1)#exit
DES-7200(config)#interface gigabitEthernet 2/2
DES-7200(config-if-GigabitEthernet 2/2)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
Router(config-if-GigabitEthernet 2/2)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
DES-7200(config-if-GigabitEthernet 2/2)#ip ref
Router(config-if-GigabitEthernet 2/2)#exit
```

3) Configure LDP protocol so that the network can forward MPLS traffic.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
```

4) Enable LDP GR protocol

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#graceful-restart
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#graceful-restart
```

5) Configure relevant parameters of LDP GR protocol.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
```

Set reconnection timer to 300 seconds, LDP neighbor liveness timer to 120 seconds and LDP recovery timer to 120 seconds.

```
DES-7200(config-mpls-router)#graceful-restart timer reconnect 300
DES-7200(config-mpls-router)#graceful-restart timer neighbor-liveness 120
DES-7200(config-mpls-router)#graceful-restart timer recovery 120
DES-7200(config-mpls-router)#exit
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
```

Set reconnection timer to 300 seconds, LDP neighbor liveness timer to 120 seconds and LDP recovery timer to 120 seconds.

```
DES-7200(config-mpls-router)#graceful-restart timer reconnect 300
DES-7200(config-mpls-router)#graceful-restart timer neighbor-liveness 120
DES-7200(config-mpls-router)#graceful-restart timer recovery 120
DES-7200(config-mpls-router)#exit
```

6) Restart LDP session to effect the configurations.

Restart LDP session on PE1 device.

```
DES-7200#clear mpls ldp neighbor all
```

Restart LDP session on P device.

```
DES-7200#clear mpls ldp neighbor all
```

Verification

Verify PE1 configurations.

Display LDP GR configurations on PE1.

```
DES-7200#show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (1 records):
    Peer LDP Ident: 192.168.0.2:0; Local LDP Ident: 192.168.0.1:0
        Status: recovering (86 seconds left)
        Address list contains 3 addresses:
          192.168.1.2    192.168.2.1    192.168.0.2
  Graceful Restart-enabled Sessions:
```

```
   Peer LDP Ident: 192.168.0.2:0, State: estab
```

Display LDP neighbor GR configurations on PE1.

```
DES-7200#show mpls ldp neighbor graceful-restart
Default VRF:
   Peer LDP Ident: 192.168.0.2:0; Local LDP Ident: 192.168.0.1:0
      TCP connection: 192.168.0.2.15532 - 192.168.0.1.646
      State: OPERATIONAL; Msgs sent/recv: 23/27; UNSOLICITED
      Up time: 00:04:12
      Graceful Restart enabled; Peer reconnect time (msecs): 0
```

Display LDP bindings on PE1.

```
Router#show mpls ldp bindings
Default VRF:
   lib entry: 192.168.0.2/32
      local binding:  to lsr:  192.168.0.2:0, label: 1024
      remote binding: from lsr: 192.168.0.2:0, label: imp-null stale
lib entry: 192.168.1.2/24
      local binding:  to lsr:  192.168.0.2:0, label: 1025
      remote binding: from lsr: 192.168.0.2:0, label: imp-null stale
   lib entry: 192.168.2.1/24
      local binding:  to lsr:  192.168.0.2:0, label: 1026
      remote binding: from lsr: 192.168.0.2:0, label: imp-null stale
```

3.1.2 L3VPN GR configuration

Note

The router and switch icons involved in this section represent the general router and layer-3 switch running routing protocol.

3.1.2.1 Introduction to L3VPN GR

Overview

L3VPN GR (VPN GR for short) allows non-stop data forwarding of VPN service. When the control plane of device fails, data forwarding of VPN service can still be executed normally, so that the VPN service remains unaffected on the network. Preconditions to achieve VPN GR include:

- Management board 1+1 redundant backup.
- Supporting non-stop forwarding of routing protocol.
- Supporting BGP/MPLS GR protocol.
- Supporting LDP GR protocol.

Purpose of deploying VPN GR:

- Minimize routing protocol oscillation during main-slave management board switchover.
- Minimize the impacts on VPN service.
- Minimize the single point failure of access device and enhance the reliability of VPN network.
- Minimize the drop rate of VPN traffic.

Note

The non-stop forwarding of routing protocol means that the unicast route must support GR function, namely the device must support OSPF GR, IS-IS GR or BGP GR.

Basic concepts of L3VPN GR

GR routers by capability

In terms of GR capability, there are GR-Capable router, GR-Aware router and GR-Unaware router.

- GR-Capable router

The router with GR capability. Generally, such router has dual management boards (1+1 redundancy). During main-slave management board switchover, it can advertise its adjacent neighbors to keep its forwarding data and then rebuild the routing table after switchover without causing route oscillation. The packet forwarding path remains unchanged, and the entire system can forward data in a non-stop way.

- GR-Aware router

The router with GR-Aware capability. Such router may not have dual management boards, but it can detect that its neighbor is experiencing GR and help its neighbor to complete GR.

- GR-Unaware router

The router without GR detection capability. It cannot detect that the neighboring router is experiencing GR and cannot help the neighboring router to complete GR. This is generally because the no GR feature is provided by the system software or the GR feature is disabled.

GR routers by role

During the process of router restart, routers can be classified into GR-Restarter router and GR-Helper router according to router's role.

- GR-Restarter router

GR-Restarter router must be a GR-Capable router, and the restart process is triggered by the administrator or fault.

- GR-Helper router

Neighbor of GR-Restarter, at least a GR-Aware router.

Working principle

The control plane and forwarding plane of a traditional device are handled by the same processor, which maintains both the routing table and forwarding table. To enhance the forwarding performance and reliability performance of the device, multiprocessor architecture is employed on medium- and high-end devices. The processor handling control modules such as routing protocol is located on the main management board, while the processor responsible for data forwarding is located on the line card. The control plane and forwarding plane are separated in this way. When the control plane restarts, the data forwarding on the line card won't be affected. This technology provides a precondition for achieving GR. The GR-Capable router as mentioned herein has separated control plane and forwarding plane.

Assuming that the network topology of VPN is shown below. The network has the following characteristics:

- CE device represents the customer network running IGP or eBGP protocol.
- Provider network is formed between PEs and P device, running IGP protocol.
- PE1, P and PE2 establish a public-network tunnel and LSP path through LDP protocol.
- PE1 and PE2 establish a private-network tunnel through iBGP protocol.
- IGP protocol, BGP protocol and LDP protocol are GR-capable.
- PE devices are GR-Capable routers, while P device is a GR-Aware router.

Note

Please refer to "OSPF Routing Protocol Configuration", "BGP Protocol Configuration" and "LDP GR Configuration" for more information about IGP GR, BGP GR and LDP GR.

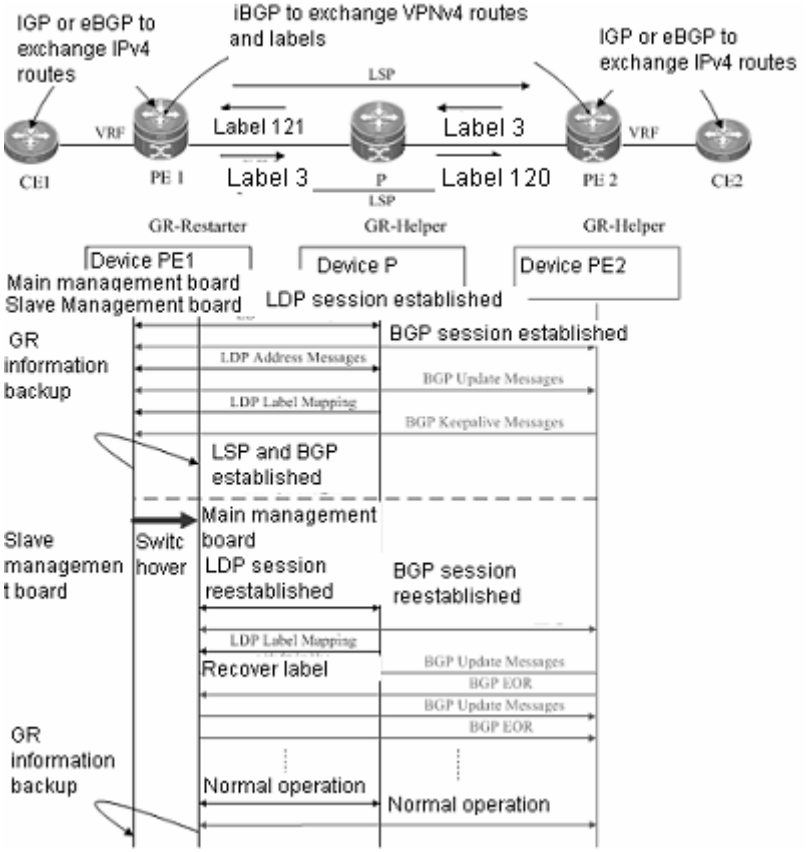


Fig 20 VPN network topology

The following example describes the GR process by taking provider network access point device PE1 as the example. When main-slave management board switchover takes place on PE1, PE1 plays the role of GR-Restarter, while P device and PE2 play the role of GR-Helper. The handling process can be divided into three phases:

- Before main-slave management board switchover

Device PE1 and the neighboring CE carry out IGP GR negotiation or eBGP GR negotiation. PE1 and P device carry out IGP or LDP GR negotiation. PE1 and PE2 carry out iBGP GR negotiation.

PE1 sends the Initialization message carrying the optional parameter of FT Session TLV to P device to establish GR-Capable LDP Session. After LDP Session is established, they exchange address information and label mapping information, and the GR-Capable LSP is established for data forwarding.

PE1 sends Open message carrying GR-Capable <AFI=IPv4, SAFI=Unicast> and <AFI=IPv4, SAFI=VPNv4> to PE2 in order to establish GR-Capable iBGP Session. When the main management board works normally, the main management board will need to backup GR information to the slave management board, so that these raw data can be read and used for protocol GR after main-slave management board switchover.

- During main-slave management board switchover

The GR information of PE1 has been backuped to the slave management board. Its main task at this phase is to carry out main-slave management board switchover.

P device detects that the corresponding TCP session has entered into "Down" state and then marks the corresponding LSP as "stale". Meanwhile, it will start forwarding table aging timer and keep forwarding packets before the timer runs out.

When PE2 detects that the TCP connection is disconnected, it will immediately mark the routes learned from PE1 as "stale" and start a restart timer against PE1. Before the restart timer runs out, if Open message is still not received, it will remove the "stable" route tag marked recently. If Open message is received, it will delete the restart timer. During this period, PE1 and PE2 will use the original route to forward traffic.

- After main-slave management board switchover

On PE1, the slave management board becomes the new main management board, and the main management board becomes the new slave management board. On the new main management board, the device will check the backuped GR information to see whether forwarding data before the restart is retained. After that, the device will begin CLI configuration initialization and GR. During the GR of IGP, BGP and LDP, they will advertise all IGP protocol neighbors, BGP neighbors and LDP neighbors to re-establish connection.

➢ IGP convergence

PE1 sends GR-Capable Initialization message to the neighboring P device and re-establish session to acquire topology and routing information after receiving response. PE1 will then recalculate the routing table and delete "stable" routes to complete protocol convergence.

➢ BGP processing

PE1 and CE will exchange routing information. After that, PE1 will update the routing table and forwarding data according to the new routes, replace void routing information and complete BGP protocol convergence.

PE1 and PE2 began to rebuild BGP session. Firstly, it sends Open message (carrying GR-Capable parameters) to PE2; secondly, it receives and handles the Update messages

(including IP prefix) from PE2 and will only start BGP best path selection after receiving EOR flag from PE2. Then, it will start sending prefix-carrying Update messages to PE2, after which it will further send EOR flag to PE2. After PE2 receives the EOR flag, it will also start best path selection. The network is converged in this way.

- LDP processing

PE1 sends GR-Capable Initialization message to the neighboring P device and establish a GR-Capable LDP session after receiving the Initialization message from neighbor. Two devices will begin to exchange address information and label mapping information, and remove or retain the "stale" mark of MPLS forwarding data according to the information exchanged. Upon completion of GR, both neighbors will delete their own MPLS forwarding data marked as "stale".

Note

The afore-cited IGP GR, BGP GR and LDP GR processing procedures are given in a random order. In terms of routing convergence, unicast routes will be converged first, and the converged routes will be advertised to LDP protocol for further use.

Caution

Before all protocols complete GR, only the RIB information of main management board will be updated; the FIB information of interface board won't be updated.

After all protocols complete GR, FIB information of the interface board will be updated at the same time.

Protocol specification

NA

3.1.2.2 Configure L3VPN GR

The following sections describe how to configure L3VPN GR:

Create configuration tasks

Configure L3VPN

Configure IGP GR

Configure BGP GR

Configure LDP GR

Create configuration tasks

Application environment

In MPLS network, L3VPN application needs to configure L3VPN GR on the service-carrying device, so that this device can ensure non-stop data forwarding during main-slave management board switchover, and the service traffic can maintain uninterrupted.

Note

When the neighboring devices experience main-slave management board switchover at the same time, GR capability cannot guarantee non-stop traffic.

Prerequisites

Before configuring L3VPN GR, the following configuration tasks must be completed:

- Build L3VPN environment and configure L3VPN.
- Support management board redundancy.
- Make sure IGP protocol is GR-Capable.
- Make sure BGP protocol is GR-Capable.
- Make sure LDP protocol is GR-Capable.

Data preparation

Before configuring L3VPN GR, the following data must be prepared:

- IGP GR parameters.
- BGP GR parameters.
- LDP GR parameters.

Configure L3VPN

Note

To configure L3VPN GR, you must configure L3VPN first. Please refer to "BGP/MPLS VPN Configuration" for L3VPN configuration.

Configure IGP GR

Note

To configure L3VPN GR, you must configure IGP GR. Please refer to "OSPF Routing Protocol Configuration" for IGP GR configuration.

Configure BGP GR

Note

To configure L3VPN GR, you must configure BGP GR. Please refer to "BGP Protocol Configuration" for BGP GR configuration.

Configure LDP GR

Note

To configure L3VPN GR, you must configure LDP GR. Please refer to "LDP GR Configuration" for LDP GR configuration.

Display configurations

The following commands are provided to display various configurations and status information. Their descriptions are given below:

Command	Function
show ip vrf [*vrf_name*]	Display VRF configurations.
show ip bgp vpnv4 {**all	rd** *route-distinguish*	**vrf** *vrf_name*} [*network-address*] [**summary**] [**neighbor**] [**label**]	Display VPN routing information.
show ip bgp summary	Display the status of all BGP connections.
show ip route vrf *vrf_name* [*A.B.C.D*	**bgp**	**connected**	**isis**	**ospf**	**rip**	**static**	*weight*]	Display relevant routing information of VRF.
show mpls ldp graceful-restart [**all**	**vrf** *vrf-name*]	Display LDP GR session and session parameters.

Note

The aforementioned display commands can be configured in any modes other than the user mode.

3.1.2.3 Typical L3VPN GR configuration example

Networking requirements

1) CE device represents the customer network running IGP or eBGP protocol.

2) Provider network is formed between PEs and P device, running IGP protocol.

3) PE1, P and PE2 establish a public-network tunnel and LSP path via LDP protocol.

4) PE1 and PE2 establish a private-network tunnel through iBGP protocol.

5) IGP protocol, BGP protocol and LDP protocol are GR-capable.

6) PE devices are GR-Capable routers, while P device is a GR-Aware router.

Network topology

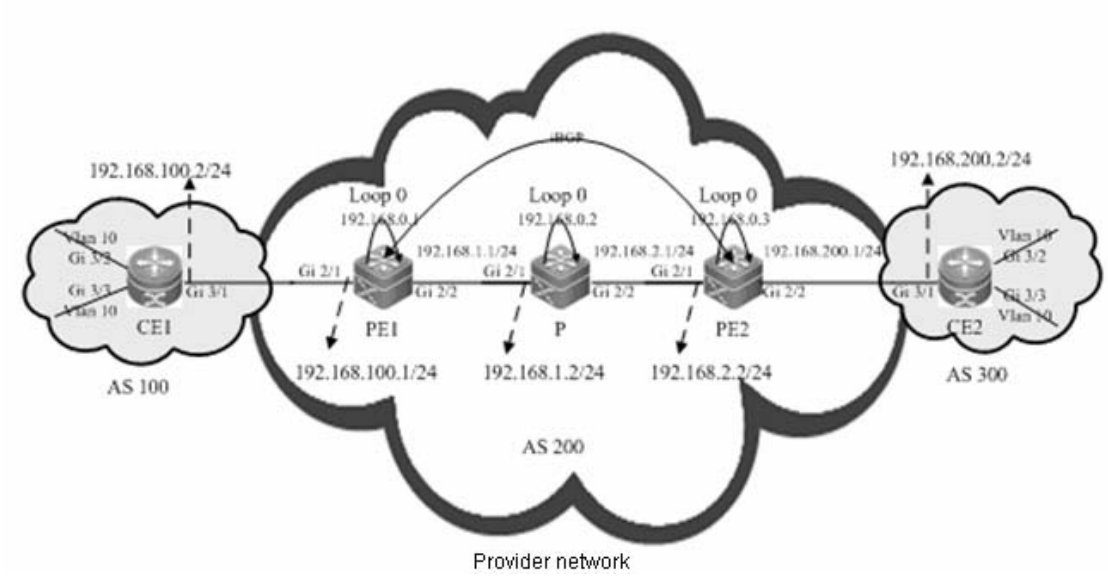


Fig 21 Network topology

Configuration tips

Configuration tips for PE1, P and PE2 are shown below:

1) Configure VRF.
2) Configure IP address and OSPF protocol on the interface of respective devices.
3) Configure global and interface MPLS capability on respective devices.
4) Configure LDP protocol so that the network can forward MPLS traffic.
5) Enable LDP GR protocol and configure relevant parameters of LDP GR protocol.
6) Configure L3VPN.
7) Enable BGP GR protocol.
8) Restart LDP session to effect the configurations.

Configuration steps

1) Configure VRF.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Configure VRF.

```
DES-7200(config)#ip vrf 10
DES-7200(config-vrf)#rd 1:100
DES-7200(config-vrf)#route-target both 1:100
DES-7200(config-vrf)#exit
```

Configure P. VRF configuration is not required.

Configure PE2. The configurations of PE2 are the same as that of PE1.

2) Configure IP address and OSPF protocol on the interface of respective devices.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Configure the IP address of interface (Gi 2/1) and associate VRF with the interface.

```
DES-7200(config)#interface gigabitEthernet 2/1
```

```
DES-7200(config-if-GigabitEthernet 2/1)#no switchport
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 2/1)#no switchport
DES-7200(config-if-GigabitEthernet 2/1)#ip vrf forwarding 10
DES-7200(config-if-GigabitEthernet 2/1)#ip address 192.168.100.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 2/1)#exit
```

Configure the loopback interface of Loopback 0

```
DES-7200(config)#interface loopback 0
DES-7200(config-Loopback 0)#ip address 192.168.0.1 255.255.255.255
DES-7200(config-Loopback 0)#exit
```

Configure the IP address of interface (Gi 2/2).

```
DES-7200(config)#interface gigabitEthernet 2/2
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 2/2)#no switchport
DES-7200(config-if-GigabitEthernet 2/2)#ip address 192.168.1.1 255.255.255.0
```

Activate OSPF protocol and enter OSPF mode.

```
DES-7200(config)#router ospf 10
DES-7200(config-router)#network 192.168.0.1 255.255.255.255 area 0
DES-7200(config-router)#network 192.168.1.0 255.255.255.0 area 0
DES-7200(config-router)#end
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Configure the loopback interface of Loopback 0.

```
DES-7200(config)#interface loopback 0
DES-7200(config-Loopback 0)#ip address 192.168.0.2 255.255.255.255
DES-7200(config-Loopback 0)#exit
```

Configure the IP address of interface (Gi 2/1).

```
DES-7200(config)#interface gigabitEthernet 2/1
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 2/1)#no switchport
DES-7200(config-if-GigabitEthernet 2/1)#ip address 192.168.1.2 255.255.255.0
```

Configure the IP address of interface (Gi 2/2).

```
DES-7200(config)#interface gigabitEthernet 2/2
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 2/2)#no switchport
DES-7200(config-if-GigabitEthernet 2/2)#ip address 192.168.2.1 255.255.255.0
```

Activate OSPF protocol and enter OSPF mode.

```
DES-7200(config)#router ospf 10
DES-7200(config-router)#network 192.168.1.0 255.255.255.0 area 0
DES-7200(config-router)#network 192.168.2.0 255.255.255.0 area 0
DES-7200(config-router)#network 192.168.0.2 255.255.255.255 area 0
DES-7200(config-router)#end
```

Configure PE2. The configurations of PE2 are the same as that of PE1.

3) Configure global and interface MPLS capability on respective devices.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 2/2
DES-7200(config-if-GigabitEthernet 2/2)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
Router(config-if-GigabitEthernet 2/2)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
DES-7200(config-if-GigabitEthernet 2/2)#ip ref
Router(config-if-GigabitEthernet 2/2)#exit
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 2/1
DES-7200(config-if-GigabitEthernet 2/1)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 2/1)#mpls ip
Router(config-if-GigabitEthernet 2/1)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 2/1)#mpls ip
DES-7200(config-if-GigabitEthernet 2/1)#ip ref
Router(config-if-GigabitEthernet 2/1)#exit
DES-7200(config)#interface gigabitEthernet 2/2
DES-7200(config-if-GigabitEthernet 2/2)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
Router(config-if-GigabitEthernet 2/2)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 2/2)#mpls ip
DES-7200(config-if-GigabitEthernet 2/2)#ip ref
Router(config-if-GigabitEthernet 2/2)#exit
```

Configure PE2. The configurations of PE2 are the same as that of PE1.

4) Configure LDP protocol so that the network can forward MPLS traffic.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
```

Configure PE2.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
```

5) Enable LDP GR protocol and configure relevant parameters of LDP GR protocol.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#graceful-restart
```

Set reconnection timer to 300 seconds, LDP neighbor liveness timer to 120 seconds and LDP recovery timer to 120 seconds.

```
DES-7200(config-mpls-router)#graceful-restart timer reconnect 300
DES-7200(config-mpls-router)#graceful-restart timer neighbor-liveness 120
DES-7200(config-mpls-router)#graceful-restart timer recovery 120
DES-7200(config-mpls-router)#exit
```

Configure P device.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#graceful-restart
```

Set reconnection timer to 300 seconds, LDP neighbor liveness timer to 120 seconds and LDP recovery timer to 120 seconds.

```
DES-7200(config-mpls-router)#graceful-restart timer reconnect 300
DES-7200(config-mpls-router)#graceful-restart timer neighbor-liveness 120
DES-7200(config-mpls-router)#graceful-restart timer recovery 120
DES-7200(config-mpls-router)#exit
```

Configure PE2. The configurations of PE2 are the same as that of PE1.

6) Configure L3VPN.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Configure eBGP peer CE

```
DES-7200(config-router)#address-family ipv4 vrf 10
DES-7200(config-router-af)#neighbor 192.168.100.2 remote-as 100
DES-7200(config-router-af)#exit-address-family
DES-7200(config-router)#exit
```

Configure iBGP peer PE2

```
DES-7200(config-router)#neighbor 192.168.0.3 remote-as 200
DES-7200(config-router)#neighbor 192.168.0.3 update-source loopback 0
DES-7200(config-router)#address-family vpnv4 unicast
DES-7200(config-router-af)#neighbor 192.168.0.3 activate
DES-7200(config-router-af)#exit-address-family
DES-7200(config-router)#exit
```

Configure P. L3VPN configuration is not required.

Configure PE2. The configurations of PE2 are the same as that of PE1.

7) Enable BGP GR protocol.

Configure PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

Enable BGP protocol and enter BGP configuration mode.

```
DES-7200(config)#router bgp 200
```

Enable BGP GR.

```
DES-7200(config-router)#bgp graceful-restart
```

Configure P. No need to enable BGP GR protocol.

Configure PE2. The configurations of PE2 are the same as that of PE1.

8) Restart LDP session to effect the configurations.

Restart LDP session on PE1 device.

```
DES-7200#clear mpls ldp neighbor all
```

Restart LDP session on P device.

```
DES-7200#clear mpls ldp neighbor all
```

Restart LDP session on PE1 device.

```
DES-7200#clear mpls ldp neighbor all
```

Verification

Verify PE1 configurations.

Display LDP GR configurations on PE1.

```
DES-7200#show mpls ldp graceful-restart
Default VRF:
  LDP Graceful Restart is enabled
  Neighbor Liveness Timer: 120 seconds
  Max Recovery Time: 120 seconds
  Forwarding State Holding Time: 300 seconds
  Down Neighbor Database (1 records):
    Peer LDP Ident: 192.168.0.2:0; Local LDP Ident: 192.168.0.1:0
        Status: recovering (86 seconds left)
        Address list contains 3 addresses:
          192.168.0.2    192.168.1.2    192.168.2.1
  Graceful Restart-enabled Sessions:
    Peer LDP Ident: 192.168.0.2:0, State: estab
```

Display BGP GR configurations on PE1.

```
DES-7200#show ip bgp vpnv4 all neighbor
BGP neighbor is 192.168.0.3, remote AS 200, internal link
BGP version 4, remote router ID 192.168.0.3
BGP state = Established, up for 02:49:47
Last read 00:00:47, hold time is 180, keepalive interval is 60 seconds
Neighbor capabilities:
Route refresh: advertised and received (new)
Address family VPNv4 Unicast: advertised and received
Graceful Restart Capability: advertised and received
Remote Restart timer is 120 seconds
Address families preserved by peer:
VPNv4 Unicast
```

3.2 MPLS BFD Configuration

3.2.1 Introduction to MPLS BFD

MPLS BFD is accomplished on the basis of the standard of "BFD For MPLS LSPs" defined by IETF. It describes a method to detect MPLS LSP, and constitutes a component of BFD application. Detailed introductions about BFD are given in "BFD Configuration Guideline".

3.2.1.1 Overview

In MPLS network, the following mechanisms are generally used to detect LSP faults:

- Adopting MPLS OAM mechanism. This mechanism can effectively detect, verify and locate defects or faults originating from the MPLS layer. However, the standardization of MPLS OAM mechanism is still underway, and various OAM mechanisms are merely at the preliminary stage in real network applications. OAM feature is not supported by all network devices.

- Hello packet mechanism using MPLS signaling protocol. This mechanism takes a longer time to detect faults (generally in seconds or more time). Therefore, this mechanism will result in the loss of substantial traffic.

MPLS BFD mechanism can address the aforementioned problems. It has the following features:

- Supporting intercommunication. Providing an unified detection mechanism for the entire network.

- Allowing fast detection. Capable of providing light-load fast detection, speeding up the activation of standby forwarding path, and improving MPLS network reliability.

- BFD can be used to detect faults in the data plane of MPLS LSP forwarding path. Meanwhile, BFD is also more suitable for being implemented in hardware or firmware due to its fixed packet format.

3.2.1.2 MPLS BFD feature

Introducing the mode to establish and detect MPLS BFD sessions.

BFD session establishment

BFD uses My Discriminator and Your Discriminator to identify multiple BFD sessions between the same pair of systems. The means of discriminator configuration can be divided into: 1) manual configuration; 2) automatic configuration.

Manual configuration will manually configure my discriminator and your discriminator of BFD. In this way, before BFD session is established, there is no need to negotiate and learn your discriminator through the discriminator carried in the LSP Ping echo packet. The BFD session will be established directly.

Automatic configuration uses the discriminator carried in the LSP Ping echo packet to negotiate and learn your discriminator before it can establish the BFD session.

The following paragraphs will describe the procedures of establishing BFD session. At the initial stage of BFD session, two ends sending packets play either the active role or the passive role. Whether the Ingress LSR or Egress LSR play an active role or passive is determined by the

application, but at least one LSR plays the active role. Therefore, the initialization phase can involve two scenarios.

- Both ends play the active role

In case both ends play the active role, since LSP is unidirectional, there may be the following two scenarios:

✧ From Ingress LSR to Egress LSR: BFD for LSP; from Egress LSR to Ingress LSR: BFD for another LSP.

The Ingress LSR will send LSP Ping echo request packet carrying my discriminator to the Egress LSR. When Egress LSR receives the echo request packet, it can then acquire your discriminator from the echo request packet. In this way, Egress LSR has both my discriminator (generated by Egress LSR) and your discriminator, and then starts to send BFD control packet to the Ingress LSR. When Ingress LSR receives the BFD control packet, it can acquire your discriminator from the BFD control packet received. Hence, the Ingress LSR also has my discriminator (generated by Ingress LSR) and your discriminator. After having the discriminators of both ends, it will start to send BFD control packet to Egress LSR, and thus the Ingress LSR and Egress LSR enter into the initial stage of BFD session establishment.

Here we shall point out that: when Egress LSR receives the echo request packet, it can reply with the echo reply packet (or choose not to reply). If Egress LSR does send the echo reply packet, then such packet must carry my discriminator (generated by Egress LSR). In this way, the Ingress LSR can acquire your discriminator from BFD control packet or from the echo reply packet.

For Egress LSR, the working process is same as that of Ingress LSR, and we will no give unnecessary details herein.

✧ From Ingress LSR to Egress LSR: BFD for LSP; from Egress LSR to Ingress LSR: BFD for IP (when there are multiple hops)

For Ingress LSR, the working process has been described before, and we will not give unnecessary details herein. For Egress LSR, before receiving the echo request packet sent by Ingress LSR or acquiring your discriminator, its BFD control packets sent to Ingress LSR will be discarded.

- One active end and one passive end

The active end will send LSP Ping echo request packet carrying my discriminator to the passive end. When the passive end receives the echo request packet, it can then acquire your discriminator from the echo request packet. In this way, the passive end has both my discriminator (generated by passive end) and your discriminator, and then starts to send BFD control packet to the active end. When active end receives the BFD control packet, it

can acquire your discriminator from the BFD control packet received. Hence, the active end also has my discriminator (generated by active end) and your discriminator. After having the discriminators of both ends, it will start to send BFD control packet to the passive end, and thus the active end and the passive end enter into the initial stage of BFD session establishment.

Here we shall point out that: when passive end receives the echo request packet, it can reply with the echo reply packet (or choose not to reply). If passive end does send the echo reply packet, then such packet must carry my discriminator (generated by passive end). In this way, the active end can acquire your discriminator from BFD control packet or from the echo reply packet.

For the passive end, before receiving the echo request packet sent from the active end, it will not send BFD control packet to the active end.

The following chart describes the process of BFD session establishment with both ends being active, BFD being used to detect the LSP from Ingress LSR to Egress LSR and BFD being used to detect another LSP from Egress LSR to Ingress LSR.

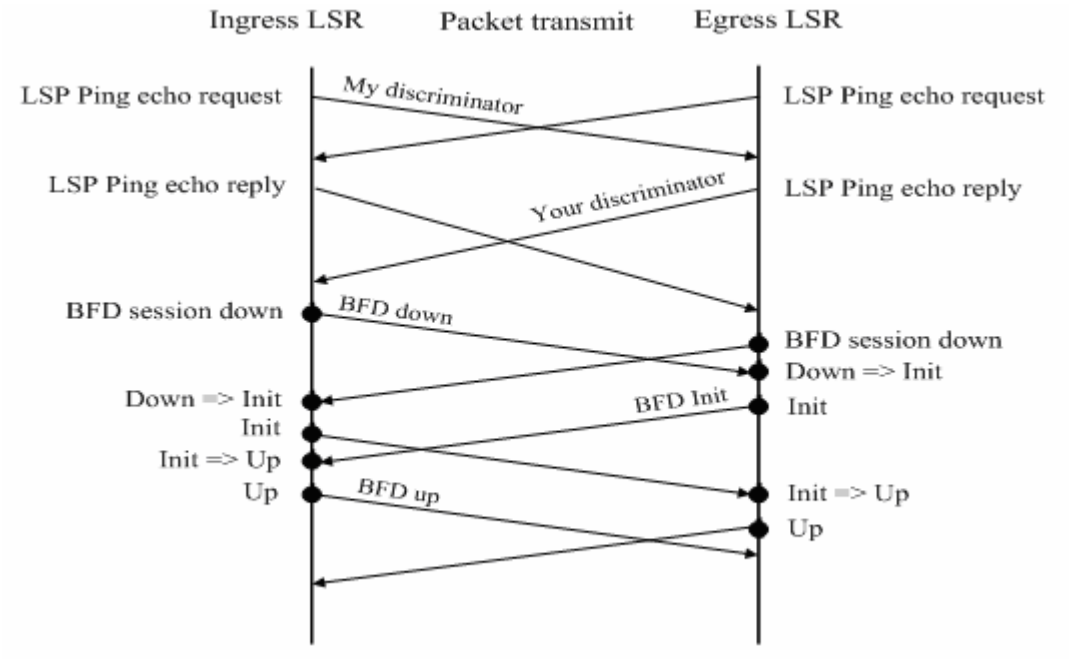


Fig 24

- Before initiating BFD, Ingress LSR and Egress LSR will first need to learn your discriminator and make sure the LSP state is "Up". As shown in Fig 2-1, Ingress LSR sends LSP Ping echo request packet carrying my discriminator to Egress LSR. After receiving the echo request packet, the Egress LSR will reply with echo reply packet carrying my discriminator

(generated by Egress LSR) to the Ingress LSR. This process is the same for Egress LSR, and we will not give unnecessary details herein. It shall be noted when no discriminator is defined at both ends, your discriminator must be learned through the LSP Ping echo packet. If both ends have defined my discriminator and your discriminator, then this step will be neglected during the process of establishing BFD session. Please refer to the section of "BFD for LSP" for discriminator configuration.

- Ingress LSR and Egress LSR initiate BFD, with initial state being "Down" and the BFD packet sent carrying "Down" state.
- Egress LSR receives the BFD packet with state being "Down". The local BFD switches state to "Init" and sends BFD packet carrying "Init" state.
- After Egress LSR switches local BFD state to "Init", it will no longer process BFD packets with state being "Down".
- The BFD state changing process of Ingress LSR is the same as above.
- Egress LSR receives the BFD packet with state being "Init". The local BFD switches state to "Up".
- The BFD state changing process of Ingress LSR is the same as above.
- Local BFD state changes to "Up", indicating that the BFD session is established successfully.

Detection mode

Before exchanging BFD control packets between two devices, a BFD session must be established, and the control plane and data plane must share the same path. There are two BFD operating modes:

- Asynchronous mode
- Demand mode

Besides these two modes, Echo feature is also defined in BFD. It can be applied in both asynchronous mode and demand mode.

Currently, BFD for LSP can only support asynchronous mode. It cannot support demand mode or Echo mode.

3.2.1.3 BFD for LSP

As described in the section of "BFD session establishment", we know that BFD session is discriminated through My Discriminator and Your Discriminator. According to the method of defining My Discriminator and Your Discriminator, BFD for LSP involves two configurations modes:

- Manual configuration

Manual configuration will manually configure my discriminator and your discriminator of BFD. In this way, before BFD session is established, there is no need to negotiate and learn your discriminator via the discriminator carried in the LSP Ping packet. The BFD session will be established directly.

- Automatic configuration

Automatic configuration uses the discriminator carried in the LSP Ping packet to negotiate and learn your discriminator before it can establish the BFD session.

According to the type of LSP, BFD for LSP currently supports the following types:

- BFD for static LSP
- BFD for LDP LSP

BFD for static LSP

BFD for static LSP supports both manual configuration mode and automatic configuration mode. Since LSP is an unidirectional link and BFD is a bidirectional detection mechanism, when using BFD to detect the unidirectional link of static LSP, the backward direction link can use any one of the following detection methods:

- Backward direction link with IP
- Backward direction link with static LSP

BFD for LDP LSP

BFD for static LSP supports both manual configuration mode and automatic configuration mode. Since LSP is an unidirectional link and BFD is a bidirectional detection mechanism, when using BFD to detect the unidirectional link of LDP LSP, the backward direction link detection can use any one of the following detection methods:

- Backward direction link with IP
- Backward direction link with LDP LSP

LDP LSP carries the basic services of VPN/PW public network. Therefore, BFD for LDP LSP will detect faults on the fundamental parts of VPN/PW public network. It can provide fast detection of various MPLS-based network applications such as VPN FRR, PW FRR and etc, thus protecting network services and enhancing the reliability of MPLS network.

3.2.1.4 Protocol specification

Related protocol specifications include:

- draft-ietf-bfd-base-09: Bidirectional Forwarding Detection
- draft-ietf-bfd-generic-05: Generic Application of BFD
- draft-ietf-bfd-mib-06: Bidirectional Forwarding Detection Management Information Base
- draft-ietf-bfd-v4v6-1hop-09: BFD for IPv4 and IPv6 (Single Hop)
- draft-ietf-bfd-multihop-07: BFD for IPv4 and IPv6 (Multihop)
- draft-ietf-bfd-mpls-07: BFD For MPLS LSPs

3.2.2 Default configurations

The following table describes the default configurations of BFD for static LSP.

Function	Default setting
BFD operating mode	Active mode. Currently only the active mode is supported.
BFD detection mode	Asynchronous mode. Currently only the asynchronous mode is supported. Echo mode is enabled by default.
BFD session parameters	No default values. The parameters must be configured manually.
BFD authentication mode	Disabled. No authentication mode is supported currently.

3.2.3 Configure BFD for static LSP

The following sections describe how to configure BFD for static LSP:

- Create configuration tasks
- Configure BFD on Ingress LSR
- Configure BFD on Egress LSR
- Display configurations

3.2.3.1 Create configuration tasks

- Application environment

Use BFD to detect the connectivity of static LSP. BFD for static LSP can avoid the case when the static LSP configured becomes "Down", the private-network route will not select this static LSP as the forwarding path.

- Prerequisites

Before configuring BFD for static LSP, the following configuration must be done:

- Enable MPLS
- Configure static LSP

- Data preparation

Before configuring BFD for static LSP, the following data must be prepared:

- My Discriminator and Your Discriminator of BFD session
- Backward direction link detection mode
- BFD session parameters: interval for transmitting BFD control packets, interval for receiving BFD control packets and BFD control packet detection time multiplier.

3.2.3.2 Configure BFD on Ingress LSR

By default, BFD for static LSP is disabled on the device. To enable BFD for static LSP, enter privileged user mode and execute the following steps to configure BFD for static LSP:

Command	Function
DES-7200# **configure teminal**	Enter global configuration mode.
DES-7200(config)# **interface** type ID	Enter interface configuration mode.

DES-7200(config-if-type ID)#**no bfd echo**	Disable Echo.
DES-7200(config-if-type ID)# **bfd interval** *50* **min_rx** *50* **multiplier** *3*	Configure BFD session parameters.
DES-7200(config-if-type ID)# **exit**	Exit interface configuration mode.
DES-7200(config)# **bfd bind static-lsp peer-ip** *10.10.10.10* **nexthop** *1.1.1.2* **interface** *gigabitEthernet 0/2* **local-discriminator** *1* **remote-discriminator** *2* **process-state**	Configure BFD for static LSP and handle BFD session state. The peer IP address of this LSP is 10.10.10.10; the next-hop address is 1.1.1.2; the egress interface is gigabitEthernet 0/2. For manual configuration mode: configure my discriminator as 1 and your discriminator as 2. If the Ingress LSR is manually configured, then the Egress LSR shall be manually configured as well, which means configurations at both ends shall be symmetrical.

To disable BFD for static LSP, execute "**no bfd bind static-lsp peer-ip** *10.10.10.10* **nexthop** *1.1.1.2* **interface** *gigabitEthernet 0/2*".

Caution

1、BFD for static LSP can only support the static LSP established by the host routing table.

2、For certain applications needing BFD to detect faults (such as BFD for LSP), the process-state parameter must be configured.

3、If the discriminators are configured manually, then My Discriminator and Your Discriminator configured on Ingress LSR must correspond to My Discriminator and Your Discriminator configured on Egress LSP.

3.2.3.3 Configure BFD on Egress LSR

By default, BFD for static LSP is disabled on the device. To enable BFD for static LSP, enter privileged user mode and execute the following steps to configure BFD for static LSP:

Command	Function
DES-7200# **configure teminal**	Enter global configuration mode.
DES-7200(config)# **interface** type ID	Enter interface configuration mode.
DES-7200(config-if-type ID)#**no bfd echo**	Disable Echo.

DES-7200(config-if-type ID)# **bfd interval** *50* **min_rx** *50* **multiplier** *3*	Configure BFD session parameters.
DES-7200(config-if- type ID)# **exit**	Exit interface configuration mode.
DES-7200(config)# **bfd bind static-lsp peer-ip** *20.20.20.20* **nexthop** *3.3.3.1* **interface** *gigabitEthernet 0/1* **local-discriminator** *2* **remote-discriminator** *1*	Configure BFD for static LSP without handling BFD session state. The peer IP address of this LSP is 20.20.20.20; the next-hop address is 3.3.3.1; the egress interface is gigabitEthernet 0/1. For manual configuration mode: configure my discriminator as 2 and your discriminator as 1. If the Ingress LSR is manually configured, then the Egress LSR shall be manually configured as well, which means configurations at both ends shall be symmetrical.
Or:	
DES-7200(config)#**bfd bind backward-lsp-with-ip peer-ip** *20.20.20.20* **interface** gigabitEthernet *0/1* **source-ip** *10.10.10.10* **local-discriminator** *2* **remote-discriminator** *1*	Configure BFD for backward direction LSP with IP. The source IP address of backward direction LSP is 10.10.10.10; the peer IP address is 20.20.20.20; the egress interface is gigabitEthernet 0/1. This step configures my discriminator as 2 and your discriminator as 1. When configuring BFD for LSP, if backward direction LSP adopts IP detection, then the positive direction LSP must be configured with my discriminator and your discriminator, which must be configured manually.
DES-7200(config)# **exit**	Exit global configuration mode.

To disable BFD for static LSP, execute "**no bfd bind static-lsp peer-ip** *20.20.20.20* **nexthop** *3.3.3.1* **interface** *gigabitEthernet 0/1*" or "**bfd bind backward-lsp-with-ip peer-ip** *20.20.20.20* **interface** gigabitEthernet *0/1*".

Caution

1. BFD for static LSP can only support the static LSP established by the host routing table.
2. BFD for backward direction LSP can adopt IP detection.
3. If the discriminators are configured manually, then My Discriminator and Your Discriminator configured on Egress LSR must correspond to My Discriminator and Your Discriminator configured on Ingress LSP.

3.2.3.4 Display configurations

The following commands are provided by BFD to display various configurations and status information. Their descriptions are given below:

Command	Function
show bfd neighbors [**vrf** *vrf-name*] [**ipv4** *ip-addess* [**details**] | **client** {**static-lsp | backward-lsp-with-ip**} **[ipv4** *ip-addess* [**details**] | [**details**]]	Display BFD session details.

3.2.4 Configure BFD for static LDP LSP

The following sections describe how to configure BFD for static LDP LSP:

- Create configuration tasks
- Configure BFD on Ingress LSR
- Configure BFD on Egress LSR
- Display configurations

3.2.4.1 Create configuration tasks

- Application environment

Use BFD to detect the connectivity of LDP LSP. BFD for LDP LSP can avoid the case when the LDP LSP becomes "Down", the private-network route will not select this LSP as the forwarding path.

- Prerequisites

Before configuring BFD for LDP LSP, the following configuration must be done:

- Enable MPLS
- Enable LDP

- Data preparation

Before configuring BFD for static LSP, the following data must be prepared:

- My Discriminator and Your Discriminator of BFD session

- Backward direction link detection mode
- BFD session parameters: interval for transmitting BFD control packets, interval for receiving BFD control packets and BFD control packet detection time multiplier.

3.2.4.2 Configure BFD on Ingress LSR

By default, BFD for LDP LSP is disabled on the device. To enable BFD for LDP LSP, enter privileged user mode and execute the following steps to configure BFD for LDP LSP:

Command	Function
DES-7200# **configure teminal**	Enter global configuration mode.
DES-7200(config)# **interface** type ID	Enter interface configuration mode.
DES-7200(config-if-type ID)#**no bfd echo**	Disable Echo.
DES-7200(config-if-type ID)# **bfd interval** *50* **min_rx** *50* **multiplier** *3*	Configure BFD session parameters.
DES-7200(config-if-type ID)# **exit**	Exit interface configuration mode.
DES-7200(config)#**mpls router ldp**	Enter LDP configuration mode.
DES-7200(config-mpls-router)# **bfd bind ldp-lsp peer-ip** *10.10.10.10* **nexthop** *1.1.1.2* **interface** *gigabitEthernet 0/2* **local-discriminator** *1* **remote-discriminator** *2* **process-state**	Configure BFD for LDP LSP and handle BFD session state. The peer IP address of this LSP is 10.10.10.10; the next-hop address is 1.1.1.2; the egress interface is gigabitEthernet 0/2. For manual configuration mode: configure my discriminator as 1 and your discriminator as 2. If the Ingress LSR is manually configured, then the Egress LSR shall be manually configured as well, which means configurations at both ends shall be symmetrical.

To disable BFD for LDP LSP, execute "**no bfd bind ldp-lsp peer-ip** *10.10.10.10* **nexthop** *1.1.1.2* **interface** *gigabitEthernet 0/2*".

Caution

1、BFD for LDP LSP can only support the LDP LSP triggered and established by the host routing table.

2、One LSP can only be bound with one BFD session.

3、BFD can only be bound on the Ingress of LDP LSP.

4、For certain applications needing BFD to detect faults (such as BFD for LSP based deployment), the process-state parameter must be configured.

5、If the discriminators are configured manually, then My Discriminator and Your Discriminator configured on Ingress LSR must correspond to My Discriminator and Your Discriminator configured on Egress LSP.

3.2.4.3 Configure BFD on Egress LSR

By default, BFD for LDP LSP is disabled on the device. To enable BFD for LDP LSP, enter privileged user mode and execute the following steps to configure BFD for LDP LSP:

Command	Function
DES-7200# **configure teminal**	Enter global configuration mode.
DES-7200(config)# **interface** type ID	Enter interface configuration mode.
DES-7200(config-if-type ID)#**no bfd echo**	Disable Echo.
DES-7200(config-if-type ID)# **bfd interval** *50* **min_rx** *50* **multiplier** *3*	Configure BFD session parameters.
DES-7200(config-if-type ID)# **exit**	Exit interface configuration mode.
DES-7200(config)#**bfd bind backward-lsp-with-ip peer-ip** *20.20.20.20* **interface** gigabitEthernet *0/1* **source-ip** *10.10.10.10* **local-discriminator** *2* **remote-discriminator** *1*	Configure BFD for backward direction LSP with IP. The source IP address of backward direction LSP is 10.10.10.10; the peer IP address is 20.20.20.20; the egress interface is gigabitEthernet 0/1. This step configures my discriminator as 2 and your discriminator as 1. When configuring BFD for LSP, if backward direction LSP adopts IP detection, then the positive direction LSP must be configured with my discriminator and your discriminator, which must be configured manually.
Or:	
DES-7200(config)#**mpls router ldp**	Enter LDP configuration mode.

DES-7200(config-mpls-router)# **bfd bind ldp-lsp peer-ip** *20.20.20.20* **nexthop** *3.3.3.1* **interface** *gigabitEthernet 0/1* **local-discriminator** *2* **remote-discriminator** *1*	Configure BFD for LDP LSP without handling BFD session state. The peer IP address of this LSP is 20.20.20.20; the next-hop address is 3.3.3.1; the egress interface is gigabitEthernet 0/1. For manual configuration mode: configure my discriminator as 2 and your discriminator as 1. If the Ingress LSR is manually configured, then the Egress LSR shall be manually configured as well, which means configurations at both ends shall be symmetrical.
DES-7200(config-bfd-router)# **exit**	Exit LDP configuration mode.

To disable BFD for LDP LSP, execute "bfd bind backward-lsp-with-ip peer-ip 20.20.20.20 interface gigabitEthernet 0/1" or "no bfd bind ldp-lsp peer-ip 20.20.20.20 nexthop 3.3.3.1 interface gigabitEthernet 0/1".

Caution

1、 BFD for backward direction LSP can adopt IP detection.

2、 Or configure BFD for another LSP

1) BFD for LDP LSP can only support the LDP LSP triggered and established by the host routing table.
2) One LSP can only be bound with one BFD session.
3) BFD can only be bound on the Ingress of LDP LSP.

3、 If the discriminators are configured manually, then My Discriminator and Your Discriminator configured on Egress LSR must correspond to My Discriminator and Your Discriminator configured on Ingress LSP.

3.2.4.4 Display configurations

The following commands are provided by BFD to display various configurations and status information. Their descriptions are given below:

Command	Function
show bfd neighbors [**vrf** *vrf-name*] [**ipv4** *ip-addess* [**details**] | **client** {**ldp-lsp** | **backward-lsp-with-ip**} **[ipv4** *ip-addess* [**details**] | [**details**]]	Display BFD session details.

3.2.5 Typical BFD for static LSP configuration example

3.2.5.1 Networking requirements

1) Configure BFD to detect the connectivity of static LSP. As shown in Fig 2, there are two links between PE1 and PE2.

2) Specifically:

3) PE1, PE2, P1 and P2 form the MPLS network.

4) There is a static LSP between PE1 -> P1 -> PE2 (static LSP1). Configure BFD for this static LSP.

5) There is a static LSP between PE2 -> P2 -> PE1 (static LSP2). Configure BFD for this static LSP, and advertise the fault detected to PE1 (backward direction link adopting LSP).

6) When static LSP1 fails, PE1 can quickly be notified of the fault and take the corresponding measure: delete MPLS static route.

3.2.5.2 Network topology

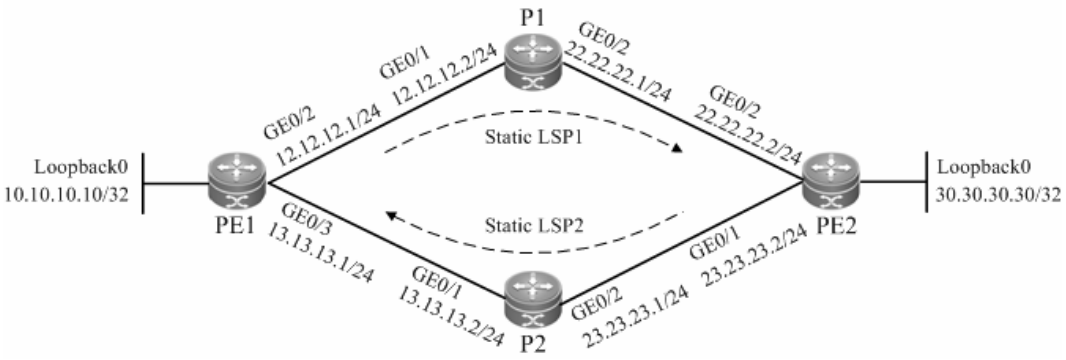


Fig 25 Network topology of BFD for static LSP configuration

3.2.5.3 Configuration tips

Configuration tips for respective nodes are shown below:

1) Configure IP address and OSPF protocol on the interface of respective nodes.
2) Configure global and interface MPLS capability on respective nodes.
3) Configure MPLS static route so that the network can forward MPLS traffic.
4) Configure BFD for static LSP1 on PE1.

5) Configure BFD for static LSP2 on PE2 (backward direction link adopting LSP).

3.2.5.4 Configuration steps

1) Configure IP address and OSPF protocol on the interface of respective nodes.

Configure PE1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/2
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
DES-7200(config-if-GigabitEthernet 0/2)#ip address 12.12.12.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#interface gigabitEthernet 0/3
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 0/3)#no switchport
DES-7200(config-if-GigabitEthernet 0/3)#ip address 13.13.13.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 0/3)#exit
DES-7200(config)#interface loopback 0
DES-7200(config-Loopback 0)#ip address 10.10.10.10 255.255.255.255
DES-7200(config-Loopback 0)#exit
DES-7200(config)#router ospf 1
Router(config-router)#network 12.12.12.1 255.255.255.0 area 0
Router(config-router)#network 13.13.13.1 255.255.255.0 area 0
Router(config-router)#network 10.10.10.10 255.255.255.255 area 0
Router(config-router)#exit
```

The configurations of other nodes are the same as that of PE1.

2) Configure global and interface MPLS capability on respective nodes.

Configure PE1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
Router(config-if-GigabitEthernet 0/2)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
DES-7200(config-if-GigabitEthernet 0/2)#ip ref
Router(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-if-GigabitEthernet 0/3)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 0/3)#mpls ip
Router(config-if-GigabitEthernet 0/3)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 0/3)#mpls ip
DES-7200(config-if-GigabitEthernet 0/3)#ip ref
Router(config-if-GigabitEthernet 0/3)#exit
```

The configurations of other nodes are the same as that of PE1.

3) Configure MPLS static route so that the network can forward MPLS traffic.

Configure static LSP1: PE1->P1->PE2

Configure PE1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls static ftn 30.30.30.30/32 out-label 16 nexthop gigabitEthernet 0/2
12.12.12.2
```

Configure P1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls static ilm in-label 16 forward-action swap-label 3 nexthop
gigabitEthernet 0/2 22.22.22.2 fec 30.30.30.30/32
```

Upon completion of configuration, execute "ping mpls 30.30.30.30" on PE1. Make sure you can ping the target node.

Configure static LSP2: PE2->P2->PE1

Configure PE2

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls static ftn 10.10.10.10/32 out-label 16 nexthop gigabitEthernet 0/1
23.23.23.1
```

Configure P2

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls static ilm in-label 16 forward-action swap-label 3 nexthop
gigabitEthernet 0/1 13.13.13.1 fec 10.10.10.10/32
```

Upon completion of configuration, execute "ping mpls 10.10.10.10" on PE2. Make sure you can ping the target node.

4) Configure BFD for static LSP1 on PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no bfd echo
DES-7200(config-if-GigabitEthernet 0/2)#bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#bfd bind static-lsp peer-ip 30.30.30.30 nexthop 12.12.12.2 interface
gigabitEthernet 0/2 local-discriminator 1 remote-discriminator 2 process-state
DES-7200(config)#exit
```

5) Configure BFD for static LSP2 on PE2 (backward direction link adopting LSP).

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#no bfd echo
DES-7200(config-if-GigabitEthernet 0/1)#bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if-GigabitEthernet 0/1)#exit
DES-7200(config)#bfd bind static-lsp peer-ip 10.10.10.10 nexthop 23.23.23.1 interface
gigabitEthernet 0/1 local-discriminator 2 remote-discriminator 1
DES-7200(config)#exit
```

3.2.5.5 Verification

Display BFD session establishment status.

Display BFD session establishment status on PE1

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr        LD/RD    RH  Holdown(mult)    State    Int
12.12.12.1      30.30.30.30  1/2      1       532 (3 )         Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: static-lsp
Uptime: 02:18:49
Last packet:     Version: 1               - Diagnostic: 0
I Hear You bit: 1        - Demand bit: 0
Poll bit: 0              - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2             - Your Discr.: 1
Min tx interval: 50000   - Min rx interval: 50000
Min Echo interval: 0
```

Display BFD session establishment status on PE2

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr        LD/RD    RH  Holdown(mult)    State    Int
23.23.23.2      10.10.10.10  1/2      1       532 (3 )         Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: static-lsp
Uptime: 02:18:49
Last packet:     Version: 1               - Diagnostic: 0
I Hear You bit: 1        - Demand bit: 0
Poll bit: 0              - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2             - Your Discr.: 1
Min tx interval: 50000   - Min rx interval: 50000
Min Echo interval: 0
```

3.2.6 Typical BFD for LDP LSP configuration example

3.2.6.1 Networking requirements

1) Configure BFD to detect the connectivity of LDP LSP. As shown in Fig 3, there are two links between PE1 and PE2.

2) Specifically:

3) PE1, PE2, P1 and P2 form the MPLS network.

4) There is a LDP LSP between PE1 -> P1 -> PE2 (LDP LSP1). Configure BFD for this LDP LSP.

5) There is a static LSP between PE2 -> P2 -> PE1 (LDP LSP2). Configure BFD for this LDP LSP, and advertise the fault detected to PE1 (backward direction link adopting LSP).

6) When LDP LSP1 fails, PE1 can quickly be notified of the fault and take the corresponding measure: delete MPLS route.

3.2.6.2 Network topology

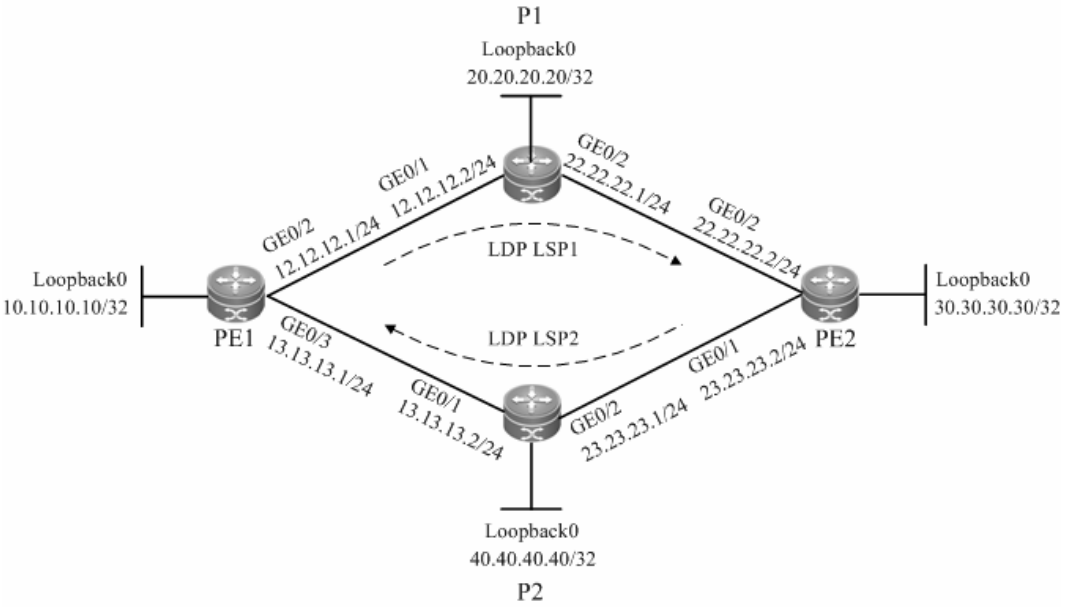


Fig 26 Network topology of BFD for LDP LSP

3.2.6.3 Configuration tips

Configuration tips for respective nodes are shown below:

1) Configure IP address and OSPF protocol on the interface of respective nodes.
2) Configure global and interface MPLS capability on respective nodes.
3) Configure LDP protocol so that the network can forward MPLS traffic.
4) Configure BFD for LDP LSP1 on PE1.
5) Configure BFD for LDP LSP2 on PE2 (backward direction link adopting LSP).

3.2.6.4 Configuration steps

1) Configure IP address and OSPF protocol on the interface of respective nodes.

Configure PE1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/2
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 0/2)#no switchport
DES-7200(config-if-GigabitEthernet 0/2)#ip address 12.12.12.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#interface gigabitEthernet 0/3
```

Execute the following command on the switch (not applicable to a router).

```
DES-7200(config-if-GigabitEthernet 0/3)#no switchport
DES-7200(config-if-GigabitEthernet 0/3)#ip address 13.13.13.1 255.255.255.0
DES-7200(config-if-GigabitEthernet 0/3)#exit
DES-7200(config)#interface loopback 0
DES-7200(config-Loopback 0)#ip address 10.10.10.10 255.255.255.255
DES-7200(config-Loopback 0)#exit
DES-7200(config)#router ospf 1
Router(config-router)#network 12.12.12.1 255.255.255.0 area 0
Router(config-router)#network 13.13.13.1 255.255.255.0 area 0
Router(config-router)#network 10.10.10.10 255.255.255.255 area 0
Router(config-router)#exit
```

The configurations of other nodes are the same as that of PE1.

2) Configure global and interface MPLS capability on respective nodes.

Configure PE1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
Router(config-if-GigabitEthernet 0/2)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
DES-7200(config-if-GigabitEthernet 0/2)#ip ref
Router(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-if-GigabitEthernet 0/3)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 0/3)#mpls ip
Router(config-if-GigabitEthernet 0/3)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 0/3)#mpls ip
DES-7200(config-if-GigabitEthernet 0/3)#ip ref
Router(config-if-GigabitEthernet 0/3)#exit
```

Configure P1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls ip
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 0/1)#mpls ip
Router(config-if-GigabitEthernet 0/1)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 0/1)#mpls ip
DES-7200(config-if-GigabitEthernet 0/1)#ip ref
Router(config-if-GigabitEthernet 0/1)#exit
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#label-switching
```

Configurations on the switch.

```
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
Router(config-if-GigabitEthernet 0/2)#exit
```

Configurations on the router. You need to execute one more command: enable fast forwarding.

```
DES-7200(config-if-GigabitEthernet 0/2)#mpls ip
DES-7200(config-if-GigabitEthernet 0/2)#ip ref
Router(config-if-GigabitEthernet 0/2)#exit
```

The configurations of other nodes are the same as that of PE1.

3) Configure LDP protocol so that the network can forward MPLS traffic.

Configure PE1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
```

Configure P1

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#ldp router-id interface loopback 0 force
```

The configurations of other nodes are the same as that of PE1.

4) Configure BFD for LDP LSP1 on PE1.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/2
DES-7200(config-if-GigabitEthernet 0/2)#no bfd echo
```

```
DES-7200(config-if-GigabitEthernet 0/2)#bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if-GigabitEthernet 0/2)#exit
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#bfd bind ldp-lsp peer-ip 30.30.30.30 nexthop 12.12.12.2
interface gigabitEthernet 0/2 local-discriminator 1 remote-discriminator 2 process-state
DES-7200(config-mpls-router)#exit
```

5) Configure BFD for LDP LSP2 on PE2 (backward direction link adopting LSP).

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#no bfd echo
DES-7200(config-if-GigabitEthernet 0/1)#bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if-GigabitEthernet 0/1)#exit
DES-7200(config)#mpls router ldp
DES-7200(config-mpls-router)#bfd bind ldp-lsp peer-ip 10.10.10.10 nexthop 23.23.23.1
interface gigabitEthernet 0/1 local-discriminator 2 remote-discriminator 1
DES-7200(config-mpls-router)#exit
```

3.2.6.5 Verification

Display BFD session establishment status.

Display BFD session establishment status on PE1

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr        LD/RD    RH  Holdown(mult)    State    Int
12.12.12.1      30.30.30.30  1/2      1        532 (3 )         Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: ldp-lsp
Uptime: 02:18:49
Last packet:     Version: 1               - Diagnostic: 0
I Hear You bit: 1        - Demand bit: 0
Poll bit: 0              - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2             - Your Discr.: 1
Min tx interval: 50000   - Min rx interval: 50000
```

```
Min Echo interval: 0
```

Display BFD session establishment status on PE2

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr        LD/RD    RH  Holdown(mult)    State    Int
23.23.23.2      10.10.10.10  1/2      1       532 (3 )         Up       Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 3
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: ldp-lsp
Uptime: 02:18:49
Last packet:     Version: 1               - Diagnostic: 0
I Hear You bit: 1        - Demand bit: 0
Poll bit: 0              - Final bit: 0
Multiplier: 3                - Length: 24
My Discr.: 2             - Your Discr.: 1
Min tx interval: 50000   - Min rx interval: 50000
Min Echo interval: 0
```

DES-7200

Security Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

Note

The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products.

The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 AAA Configuration

The access control is used to control which people can access the network server and which services can be accessed by the users on the network. The authentication, authorization and accounting (AAA) is a key security mechanism for access control.

1.1 Basic AAA Principles

Authentication, Authorization and Accounting (shortened as AAA) provide a consistence framework for configuring the authentication, authorization and accounting functions, which are supported by DES-7200 products.

The AAA provides the following services in a modular manner:

- Authentication: It verifies whether a user can access, where the Radius protocol or Local can be used. The authentication is the method to identify a user before his/her access to the network and network services. The AAA is configured by the definition of a naming list for authentication method and application of it on every interface. The method list defines the authentication type and execution order. Before a defined authentication is executed, the method list must be applied on a specific interface. The default method list is exceptional. If no other method list is defined, the default method list will automatically apply on all interfaces. The defined method list overwrites the default method list. All authentication methods other than the local, line password and allowing authentication must be defined with AAA.
- Authorization: This means authorizing the user with services. The AAA authorization is implemented through the definition of series attributes that describe the operations on the user by the authorization. These attributes can be stored on the network device or the RADIUS security server remotely. All authorization methods must be defined with AAA. When the AAA authorization is enabled, it is automatically applied on all interfaces of the network device.
- Accounting: This means recording the user's usage of network resources. When the AAA accounting is enabled, the network access server starts to send the user's network resource usages to the Radius security server through statistics records. Every accounting record is composed of attribute pairs and stored in the security server. These records can be read for analysis by special software to implement the accounting, statistics and tracing for the user's network resource usage. All accounting methods must be defined with AAA. When the AAA accounting is enabled, it is automatically applied on all interfaces of the network device.

Note

The AAA of some products only provides the authentication function. For all problems with product specifications, contact the market or technical support personnel.

Although the AAA is the primary access control method, our product also provides simple control accesses out of the range of AAA, such as the local username authentication, line password authentication and more. The difference lies in the degree of their network protection, and the AAA provides the security protection of a higher level.

The AAA has the following advantages:

- Powerful flexibility and controllability
- Expandability
- Standardized authentication
- Multiple backup systems

1.1.1 Basic AAA Principles

The AAA can configure dynamically authentication, authorization and accounting for a single user (line) or server. It defines the authentication, authorization and accounting by means of creating method lists and then applies them on specific services or interfaces.

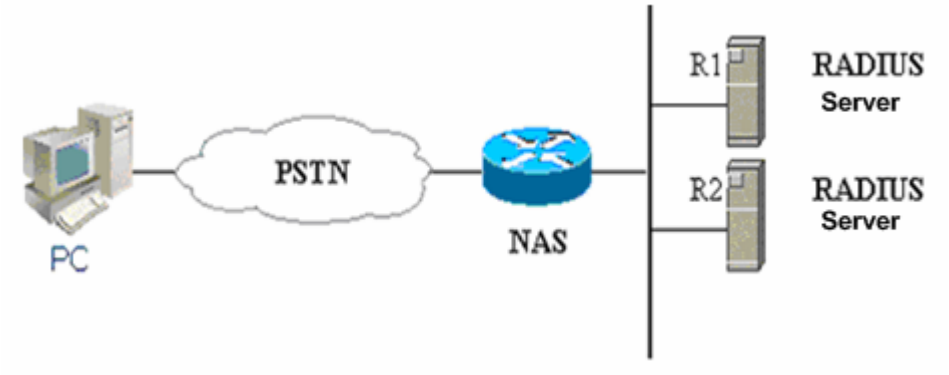
1.1.2 Method List

Since the authentication for users can be implemented in a variety of ways, you need to use the method list to define the sequence of using different method to perform authentication for the users. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of the failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method listed successfully allows communication or all methods listed are used up. If all methods listed are used up but the communication is not allowed, it declares failure of authentication.

Caution

Only when there is no reply from a method, our product will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

A typical AAA network configuration



The figure above illustrates a typical AAA network configuration, including two security servers: R1 and R2 are both RADIUS servers.

Supposed the system administrator has defined a method list, R1 is used first to capture the identity information, then R2, and finally the local username database on the NAS. If a remote PC user attempts to access the network via dialup, the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a SUCCESS reply to the NAS, and thus the user's access to the network is allowed. If R1 returns FAIL reply, the user's access is refused and the disconnected. If R1 has no reply, the NAS regards it as ERROR and queries authentication information from R2. This process continues for the remaining methods till the user passes the authentication, is refused or the session is terminated. If ERROR is returned for all methods, the authentication fails and the user is disconnected.

Caution

The REJECT response is not the same as the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request will be refused. TIMEOUT means there is no reply from the security server to the authentication. When an ERROR is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

Note

In this chapter, take RADIUS for example of the configuration of the related authentication, authorization and accouting of the AAA security server. For the TACACS+, refer to TACACS+ Configuration.

1.2 Basic AAA Configuration Steps

First you shall decide to choose which security solution, evaluate the potential security risks in

the specific network and select the proper measures to prevent unauthorized accesses. For the security risk evaluation and the possible security solutions, see Chapter 2, Security Overview. We recommend the use of AAA as much as possible to guarantee the network security.

1.2.1 Overview of AAA Configuration Steps

The AAA configuration may become simple when the basic operation process of AAA is understood. On the network devices, the AAA is configured through the following steps:

1. Enable AAA by using the global configuration command **aaa new-model**.
2. Configure the security protocol parameters if you decide to use the security server, such as RADIUS.
3. Define the authentication method list by using the **aaa authentication** command.
4. Apply the method list on specific interface or line, if necessary.

Caution

When the specific method list is applied, if no named method list is clearly specified, the default authentication method list will apply.

As a result, if you do not want to use the default authentication method list, you shall specify a specific method list.

For complete descriptions of the commands mentioned in this chapter, see the related chapters in the *Security Configuration Command Reference*.

1.2.2 Enabling AAA

It is required to enable AAA first to be able to use the AAA security features.

To enable AAA, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **aaa new-model**	Enable AAA

1.2.3 Disabling AAA

To disable AAA, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **no aaa new-model**	Disable AAA

1.2.4 Sequential Configuration Steps

After the AAA is enabled, it is time to configure the other parts related with the selected security solutions. Following table lists the possible configuration tasks and their description chapters.

Methods of AAA access control security solution

Configuration task	Step	Chapter
Configuring Local Login Authentication	3	Configuring Authentication
Defining AAA Authentication Method List	3	Configuring Authentication
Applying Method List on Specific Interface or Line	4	Configuring Authentication
Configuring Radius Security Protocol Parameters	2	Configuring Radius
Enabling Radius Authorization	5	Configuring Authorization

If you are using AAA for authentication, see Configuring Authentication.

1.3 Configuring Authentication

The authentication allows the user's identity verification before the user of network resources. In most cases, the authentication is implemented with the AAA security features. We recommend the use of AAA as much as possible.

1.3.1 Defining AAA Authentication Method List

To configure the AAA authentication, the first step is to define a named list of the authentication method, and then the applications use the defined list for authentication. The method list defines the authentication type and execution order. The defined authentication methods must be applied on specific interfaces before they can be executed. The default method list is exceptional.When not configured, all applications will use the default method list.

The method list is just a list to define the authentication method to be queried in turn to verify the user identity. The method list can define one or more security protocols for authentication, so that there are backup systems available for the authentication in case of the failure of the first method. Our product works with the first method in the method list for user authentication, and then selects the next method in the method list in case of no reply from that method. This process goes on till an authentication method listed successfully allows communication or all methods listed are used up. If all methods listed are used up but the communication is not allowed, it declares failure of authentication.

Caution Only when there is no reply from a method, our product will attempt the next method. During the authentication, if the user access is refused by a method, the authentication process ends and no other methods will be attempted.

1.3.2 Example of Method List

In a typical AAA network configuration, there are two servers: R1 and R2 are both RADIUS servers. Suppose the network administrator has chosen a security solution, and the NAS authentication uses an authentication method to authenticate the Telnet connection: First, R1 is used for the user authentication. In case of no reply, R2 will be used. In case there is no reply from both R1 and R2, the local database of the access server will perform the authentication. To configure the above authentication list, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa authentication login default group radius local	Configure a default authentication method list, where "default" is the name of the method list. The protocols included in this method list are listed behind the name in the order by which they will be queried. The default method list is applied on all applications.

If the system administrator hopes to apply this method list on a specific Login connection, he/she must create a named method list and then apply it on the specific connection. The example below shows how to apply the authentication method list on line 2 only.

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication login test group radius local	Define a method list named "test" in the global configuration mode.
line vty *2*	Enter the configuration layer of line 2
login authentication *test*	In the line configuration mode, apply the method list named “test” on the line.

If a remote PC user attempts to Telnet the network access server(NAS), the NAS first queries the authentication information from R1. If the user passes the authentication on R1, R1 sends a ACCEPT reply to the NAS, and thus the user's access to the network is allowed. If R1 returns the REJECT reply, the user's access is refused and then disconnected.If R1 does not respond, NAS considers TIMEOUT and queries the authentication information to R2. This process continues for the remaining methods till the user passes the authentication, is refused

or the session is terminated. If all servers (R1 and R2) returns TIMEOUT, the authentication will be performed by the NAS local database.

Caution

The REJECT response is not the same as the TIMEOUT response. REJECT means the user fails to comply with the standard in the available authentication database and does not pass the authentication, thus the access request will be refused. TIMEOUT means there is no reply from the security server to the authentication. When an TIMEOUT is detected, the AAA selects the next authentication method in the method list to continue the authentication process.

1.3.3 Authentication Type

DES-7200 products support the following authentication types:

- Login Authentication -- the authentication of the user terminal logging in the NAS CLI.
- Enable Authentication -- the authentication of improving the CLI authority after the user terminal loggs in the NAS CLI.
- PPP Authentication -- the authentication of PPP dial user.
- DOT1X(IEEE802.1x) Authentication -- the authentication of the IEEE802.1x access user.

1.3.4 General Steps in Configuring AAA Authentication

The following tasks are common for the configuration of AAA authentication.

- Enable AAA by using the global configuration command **aaa new-model**.
- Configure the security protocol parameters if you decide to use the security server, such as RADIUS. See Configuring Radius for details.
- Define the authentication method list by using the **aaa authentication** command.
- Applying method list on a specific interface or line, if possible.

Caution

TACACS+ is not supported by the DOT1X authentication.

1.3.5 Configuring the AAA Login Authentication

This section deals with how to configure the AAA Login authentication methods supported by our product:

Caution

Only after the AAA is enabled through the command **aaa new-model** in the global configuration mode, the AAA security features are available for your configuration. For the details, see *AAA Overview*.

In many cases, the user needs to Telnet the network access server (NAS). Once such a connection is set up, it is possible to configure NAS remotely. To prevent unauthorized accesses to the network, it is required to perform authentication on the user identity.

The AAA security services make it easy for the network devices to perform line-based authentication. No matter which line authentication method you decide to use, you just need to execute the aaa authentication login command to define one or more authentication method list and apply it on the specific line that need the line authentication.

To configure the AAA PPP authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication login {**default** |*list-name} method1 [method2...]*	Define an accounting method list, or repeat this command to define more.
line vty *line-num*	Enter the line that needs to apply the AAA authentication.
login authentication {**default**|*list-name*}	Apply the method list on the line.

The keyword "list-name" is used to name the created authentication method list, which can be any string. The keyword "method" means the actual algorithm for authentication. Only when the current method returns ERROR (no reply), the next authentication method will be attempted. If the current method returns FAIL, no authentication method will be used any more. To make the authentication return successfully, even if no specified methods reply, it is possible to specific "none" as the last authentication method.

In the example below, it is possible to pass the identity authentication even if the Radius server returns TIMEOUT. aaa authentication login default group radius none

Caution

Since the keyword "none" enables any dialup user can pass the authentication even if the security server has no reply, it is only used as the backup authentication method. We suggest not using the "none" identity authentication in general cases. In special case when all possible dialup users are trustful, and no delay due to system fault is allowed for the user's work, it is possible to use "none" as the last identity authentication method in case the security server has no reply. And we recommend adding the local authentication method before the “none” authentication method.

Keyword	Description
local	Use the local username database for authentication
none	Do not perform authentication
group radius	Use Radius for authentication

The table above lists the AAA login authentication methods supported by our product.

1.3.5.1 Using the local database for Login authentication

To configure the login authentication with local database, it is required to configure the local database first. Our product supports authentication based on the local database. To establish the username authentication, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
username *name* [**password** *password*] or **username** *name* [**access-class** *number*]	Establish the username authentication using the password, or the access list.
username *name* [**privilege** *level*]	(Optional) Set the privilege level for the user.
username *name* [**autocommand** *command*]	(Optional) Set the command auto-executed after the user login.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

To define the local login authentication method list and apply it, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.

Command	Function
aaa authentication login {**default** | *list-name*} **local**	Define the local method list.
end	Return to the privileged mode.
show aaa *method-list*	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode
login authentication {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

1.3.5.2 Using Radius for Login authentication

To configure the use of RADIUS authentication server for login authentication, it is required to first configure the RADIUS server. Our product supports the authentication based on the RADIUS server. To configure the RADIUS server, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
end	Return to the privileged mode.
show radius server	Show the RADIUS server.

After the RADIUS server is configured, make sure of successful communication with the RADIUS server before configuring the RADIUS for authentication. For details of the RADIUS server configurations, see Configuring RADIUS.

Now it is possible to configure the RADIUS server based method list. Run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication login {**default** | *list-name*} **group radius**	Define the local method list.

Command	Function
end	Return to the privileged mode.
show aaa *method-list*	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode
login authentication {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

1.3.6 Configuring the AAA Enable Authentication

This section deals with how to configure the AAA Enable authentication methods supported by our product:

In many cases, the user needs to Telnet the network access server (NAS). After passing the authentication, the user enters the Command Line Interface (CLI) and is assigned an initial command execution privilege (0-15 level). You can execute different commans in different levels and use the show privilege command to display the current level. For the details, see using the CLI.

After logging in the CLI, you can use the enable command to improve the privilege level if you fail to execute some commands due to low initial privilege level. To prevent the unauthorized access to the network, the identity authentication, named Enable authentication, is necessary when improving the privilege level.

To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication enable default *method1 [method2...]*	Define an enable authentication method list, for example RADIUS.
line vty *line-num*	Enter the line that needs to apply the AAA authentication.
login authentication {**default**|*list-name*}	Apply the method list on the line.

It can only define one enable authentication method list globally, so it is no need to define the name of the method list. The keyword "method" means the actual algorithm for authentication.

Only when the current method returns ERROR(no reply), the next authentication method will be attempted. If the current method returns FAIL, no authentication method will be used any more. To make the authentication return successfully, even if no specified methods reply, it is possible to specify none as the last authentication method.

Once configured, the enable authentication method takes effect. When executing enable command in the privileged mode, it prompts to authenticate if you want to switchover a higher privilege level. It is no need to authenticate if the privilege level to be set is lower than or equal to the current one.

Caution

The current username will be recorded if the Login authentication(except for none method) is done when entering the CLI. At this time, if the Enable authencation processes, it will not prompt to input the username and you can use the same username of Login authentication. Note that the password input must be consistent.

The username information will not be recorded if there is no Login authentication when entering the CLI, or the none method is used. At this time, if the Enable authentication processes, you shall input the username again. This username will not be recorded, so you shall input it every time when the Enable authentication processes.

Some authentication methods can bind the security level. Then in the process of authentication, except for the returned response according to the security protocol, it is necessary to verify the binded security level. If the service protocol can bind the security level, the level shall be verified while authenticating. If the binded level is more than or equal to the level to be configured, the enable authentication and level switchover succeed. But if the binded level is less than the level to be configured, the enable authentication fails, prompting the error message and keeping the current level. If the service protocol fails to bind the security level, you can configure the level without verification of the binded level.

Caution

Now only RADIUS and Local authentication support to bind the securiy level. To this end, only the security levels of these two methods are checked.

1.3.6.1 Using the local username database for Enable authentication

When processing the enable authentication with local database, you can configure the user privilege level while configuring the local user. By default, the privilege level is 1. To configure the enable authentication with local database, it is required to configure the local database first and configure the privilege level. To establish the username authentication, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
username *name* [**password** *password*]	Establish the local username and set the password.
username *name* [**privilege** *level*]	Set the user privilege level. (Optional)
end	Return to the privileged mode.
show running-config	Confirm the configuration.

To define the local Enable authentication method list, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication enable default local	Define the local method list.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
show running-config	Confirm the configuration.

1.3.6.2 Using Radius for Enable authentication

The standard RADIUS server can pass the privilege level binded with the Service-Type attribute(the standard attribute number is 6), can specify the privilege with 1 or 15 level. The extened RADIUS server can configure the privilege level of the administrator(the private attribute number is 42), can specify 0-15 privilege level. For the details of the RADIUS server, see Specifying the RADIUS Private Attribute Type in Configuring RADIUS.

To configure the use of RADIUS authentication server for enable authentication, it is required to first configure the RADIUS server, then the RADIUS server-based enable authentication method list. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication enable default group radius	Define RADIUS authentication method.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.

Command	Function
show running-config	Confirm the configuration.

1.3.7 Configuring the AAA Authentication for PPP User

PPP is a link-layer protocol of carrying the network-layer datagram in the point-to-point link. In many circumstances, the user accesses to the NAS(Network Access Server) by asynchronous or ISDN dail. Once the connection has been set up, the PPP negotiation will be enabled. To prevent the unauthorized access to the network, the identity authentication is required for the dailed user in the process of PPP negotiation.

This section deals with how to configure the AAA Enable authentication methods supported by DES-7200 product. To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication ppp {default | *list-name***}** *method1 [method2...]*	Define a PPP authentication method list. RADIUS, TACACS+ remote authentication and using the local database are the supported authentication methods.
interface *interface-type interface-number*	Enter the asynchronous or ISDN interface that needs to apply the AAA authentication.
ppp authentication {**chap** | **pap**} {**default** | *list-name*}	Apply the method list on the asynchronous or ISDN interface.

For the detailed configuration method for the PPP, see the related chapter in *Configuring PPP, MP*.

1.3.8 Configuring the AAA Authentication for 802.1x User

IEEE802.1x is a standard of Port-Based Network Access Control, providing the point-to-point secure access for the LAN, and a means of the authentication of the user connecting to the LAN device.

This section deals with how to configure the 802.1x authentication methods supported by DES-7200 product. To configure the AAA Enable authentication, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable AAA.
aaa authentication dot1x {default | *list-name***}** *method1 [method2...]*	Define an IEEE802.1x authentication method list. RADIUS remote authentication and using the local database are the supported authentication methods.
dot1x authentication *list-name*	Apply the method list to 802.1x.

For the detailed configuration method for the IEEE802.1x, see the related chapter in Configuring 802.1x.

1.3.9 Example of Authentication Configuration

The example below illustrates show to configure the network device to use “Radius + local” for authentication.

```
DES-7200(config)# aaa new-model
DES-7200(config)# username DES-7200 password starnet
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# aaa authentication login test group radius local
DES-7200(config)# line vty 0
DES-7200(config-line)# login authentication test
DES-7200(config-line)# end
DES-7200# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
username DES-7200 password 0 starnet
!
radius-server host 192.168.217.64
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
!
```

In the example above, the access server uses the Radius server (IP 192.168.217.64) to perform authentication for the login users. If the Radius server has no reply, the local database will be used for the identity authentication.

1.3.10 Example of Terminal Service Application Configuration

In the environment of the terminal service application, the terminal first connects to the asynchronous console, then offers the service accessing the network network server. However, if AAA is enabled, the Login authentication is necessary in all lines. To access the server, the terminal must pass the Login authentication and it influences the terminal service. You can separate two lines by configuration that makes the line using the terminal service directly connecting the server without the Login authentication, and ensures the device security by the Login authentication of the line connecting the device. That is to say, you can configure a login authentication list specific for the terminal service but the authentication method as none. Then apply the configured list to the line with terminal service enabled, while other lines connecting the local device is unchanged. Thereof the terminal can skip the local login authentication.

The example below illustrates the configuration steps:

```
DES-7200(config)# aaa new-model
DES-7200(config)# username DES-7200 password starnet
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# radius-server key test
DES-7200(config)# aaa authentication login test group radius local
DES-7200(config)# aaa authentication login terms none
DES-7200(config)# line tty 1 4
DES-7200(config-line)# login authentication terms
DES-7200(config-line)# exit
DES-7200(config)# line tty 5 16
DES-7200(config-line)# login authentication test
DES-7200(config-line)# exit
DES-7200(config)# line vty 0 4
DES-7200(config-line)# login authentication test
DES-7200(config-line)# end
DES-7200(config)# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius local
aaa authentication login terms none
username DES-7200 password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line aux 0
line tty 1 4
login authentication terms
line tty 5 16
login authentication test
```

```
line vty 0 4
login authentication test
!
!
```

In the example above, the access server uses the Radius server (IP 192.168.217.64) to perform authentication for the login users. If the Radius server has no reply, the local database will be used for the identity authentication. Login authentication is unnecessary for tty 1-4 is the used line of the terminal service, while using other tty and vty lines needs the login authentication.

1.4 Configuring Authorization

The AAA authorization enables the administrator to control the user's use of the services or the rights. After the AAA authorization service is enabled, the network device configures the user sessions by using the user configuration file stored locally or in the server. After the authorization is completed, the user can only use the services allowed in the profile or has the allowed rights.

1.4.1 Authorization Types

Our product supports the following AAA authorization methods:

- Exec authorization method – the user terminal loggs in the NAS CLI and is granted the privilege level (0-15 level).
- Command authorization method – after the user terminal loggs in the NAS CLI, the specific commands are authorized.
- Network authorization method – grant the available service to the user session in the network.

Note

Only TACACS+ supports the command authorization method. For the detailed information, please refer to *TACACS+ Configuration*.

1.4.2 Preparations for Authorization

The following tasks must be completed before the AAA authorization is configured:

- Enable the AAA server. For the details, see *AAA Overview*.
- (Optional) Configure the AAA authentication. The authorization is done after the user passes the authentication. But sole authorization can also be done without authentication. For details of the AAA authentication, see *Configuring Authentication*.
- (Optional) Configure security protocol parameters. If the security protocol is required for authorization, it is required to configure the security protocol parameters. The network

authorization only supports RADIUS; the Exec authorization supports RADIUS and TACACS+. For details of the RADIUS, see *Configuring RADIUS*. For details of the TACACS+, see *Configuri*ng *TACACS+*.

- (Optional) If the local authorization is required, it is required to use the **username** command to define the user rights.

1.4.3 Configuring Authorization List

To enable AAA authorization, execute the following command in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization exec network{default | *list-name} method1 [method2*|…]	Define the AAA Exec authorization method.
aaa authorization network network{default | *list-name} method1 [method2*|…]	Define the AAA Command authorization method.

1.4.4 Configuring AAA Exec Authorization

The Exec authorization grants the privilege level of command execution for the user terminal loggs in the network access server (NAS). You can use the show privilege command to display the specific level after the user loggs in the NAS CLI successfully (by telnet, for example).

No matter which Exec authorization method you decide to use, you just need to execute the aaa authorization exec command to define one or more authorization method list and apply it to the specific line that need the Exec authorization.

To configure the AAA Exec authorization, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization exec network{default | *list-name} method1 [method2*|…]	Define the AAA Exec authorization method. If you need to define multiple methods, execute this command repeatedly.

Command	Function
line vty *line-num*	Enter the line to which the AAA Exec authorization method is applied.
authorization exec {**default** | *list-name*}	Apply the method to the line.

The keyword "list-name" is used to name the created authorization method list, which can be any string. The keyword "method" means the actual algorithm for authorization. Only when the current method returns ERROR (no reply), the next authorization method will be attempted. If the current method returns FAIL, no authorization method will be used any more. To make the authorization return successfully, even if no specified methods reply, it is possible to specific "none" as the last authorization method.

In the example below, it is possible to pass the Exec authorication even if the Radius server returns TIMEOUT：

aaa authorization exec default group radius none

Keyword	Description
local	Use the local username database for Exec authorization.
none	Do not perform Exec authorization.
group radius	Use Radius for Exec authorization.
group tacacs+	Use Tacacs+ for Exec authorization.

The table above lists the AAA Exec authorization methods supported by our product.

Caution

The exec authorization is always used together with the login authentication, and they can be applied to the same line at the same time. But note that it is possible to have different results of the authentication and the authorization towards the same user because they can use different methods and servers. If the exec authorization fails, even though the login authentication has passed, the user can not access the CLI.

1.4.4.1 Using the local username database for exec authorization

To configure the Exec authorization with local database, it is required to configure the local database first. You can configure the user privilege level while configuring the local user. By default, the privilege level is 1. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.

Command	Function
username *name* [**password** *password*]	Establish the local username and set the password.
username *name* [**privilege** *level*]	Set the user privilege level. (Optional)
end	Return to the privileged mode.
show running-config	Confirm the configuration.

To define the local Exec authorization method list, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization exec {**default** | *list-name*} **local**	Define the local method list.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode.
authorization exec {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

1.4.4.2 Using Radius for exec authorization

To configure the use of RADIUS server for Exec authorization, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see Configuring RADIUS.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authentication enable {**default** | *list-name*} **group radius**	Define RADIUS authentication method.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.

Command	Function
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode.
authorization exec {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

1.4.4.3 Example of Configuring Exec Authorization

The example below illustrates how to configure exec authorization. The local login authentication and the "Radius+local" exec authorization are used when the user on the vty line 0-4 loggs in. The access server uses the Radius server with IP address 192.168.217.64 and shared keyword test. The local username and password are DES-7200, and the privilege level is 6.

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# radius-server key test
DES-7200(config)# username DES-7200 password DES-7200
DES-7200(config)# username DES-7200 privilege 6
DES-7200(config)# aaa authentication login mlist1 local
DES-7200(config)# aaa authentication exec mlist2 group radius local
DES-7200(config)# line vty 0 4
DES-7200(config-line)# login authentication mlist1
DES-7200(config-line)# authorization exec mlist2
DES-7200(config-line)# end
DES-7200(config)# show running-config
!
aaa new-model
!
aaa authorization lexec mlist2 group radius local
aaa authentication login mlist1 local
!
username DES-7200 password DES-7200
username DES-7200 privilege 6
!
Radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
authorization exec mliat2
login authentication mlist1
!
end
```

1.4.5 Configuring AAA Network Authorization

Our product support the network authorization over the network connection including PPP, SLIP. The network authorization makes the network connection obtain the service like traffic, bandwidth, timeout, ect. The network authorization only support the RADIUS. The authorization information assigned from the server are encapsulated in the RADIUS attribute. For different network connection application, it is possible that these authorization information are different.

Caution

Now the configuration does not support the 802.1X AAA authorization, while the 802.1X is implemented by using other commands. For the details of the 802.1X authorization, see *Configuring 802.1X*.

To configure the AAA network authorization, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa authorization network{default | *list-name} method1 [method2*|…]	Define the AAA network authorization method. If you need to define multiple methods, execute this command repeatedly.

The keyword "list-name" is used to name the created authorization method list, which can be any string. The keyword "method" means the actual algorithm for authorization. Only when the current method returns ERROR (no reply), the next authorization method will be attempted. If the current method returns FAIL, no authorization method will be used any more. To make the authorization return successfully, even if no specified methods reply, it is possible to specific "none" as the last authorization method.

1.4.5.1 Using Radius for network authorization

To configure the use of RADIUS server for network authorization, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see Configuring RADIUS.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.

Command	Function
aaa authentication network {**default** | *list-name*} **group radius**	Define RADIUS authentication method.

1.4.5.2 Example of Configuring Network Authorization

The example below illustrates how to configure network authorization.

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# radius-server key test
DES-7200(config)# aaa authorization network test group radius local
DES-7200(config-line)# end
DES-7200(config)# show running-config
!
aaa new-model
!
aaa authorization network test group radius none
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

1.5 Configuring Accounting

The AAA accounting function enables you to trace the services and network resources used by the user. After the accounting function is enabled, the network access server or router sends the user's network accesses to the Radius security server by means of attribute pair. You may use some analysis software to analyze these data to implement the billing, audition and tracing function for the user's activities.

1.5.1 Accounting Types

Our product currently supports the following accounting types:

- Exec Accounting -- record the accounting information of entering to and exiting from the CLI of the user terminal logged in the NAS CLI.
- Command Accounting – record the specific command execution information after the user terminal loggs in the NAS CLI.
- Network Accounting – records the related information on the user session in the network.

Note

Only TACACS+ supports the command accounting function. For the detailed information, please refer to *TACACS+ Configuration*.

1.5.2 Preparations for Accounting

The following tasks must be completed before the AAA accouting is configured:

- Enable the AAA server. For the details, see *AAA Overview*.
- Define the security protocol parameters. It is required to configure the security protocol parameters for accouting. The network accounting only supports RADIUS; the Exec accounting supports RADIUS and TACACS+; the Command accounting supports TACACS+ only. For details of the RADIUS, see *Configuring RADIUS*. For details of the TACACS+, see *Configuri*ng *TACACS+*.
- (Optional) Configure the AAA authentication. The accounting is done after the user passes the authentication(for example, Exec accounting). In some circumstances, the accouting can also be done without authentication. For details of the AAA authentication, see *Configuring Authentication*.

1.5.3 Configuring AAA Exec Accounting

The exec accounting records the information of entering to and exiting from the CLI of the user terminal logged in the NAS. When the user terminal loggs in and enters to the NAS CLI, it sends the accounting start information to the security server. When the user terminal exits from the CLI, it sends the accounting stop information to the server.

Caution

Only after the user terminal logged in the NAS has passed the login authentication, the exec accounting starts. If no login authentication or **none** authentication method has been configured, no exec accounting processes. For the same user terminal, if it sends no accounting start information to the security server when logging in, no accounting stop information will be sent when logging out.

To configure the AAA Exec accounting, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa accounting exec network{**default** | *list-name}* **start-stop** *method1 [method2*|*…*]	Define the AAA Exec accounting method list. If you need to define multiple method lists, execute this command repeatedly.
line vty *line-num*	Enter the line to which the AAA Exec accounting is applied.
accounting exec {**default** | *list-name*}	Apply the method list to the line.

The keyword "list-name" is used to name the created accounting method list, which can be any string. The keyword "method" means the actual algorithm for accounting. Only when the current method returns ERROR (no reply), the next accounting method will be attempted. If the current method returns FAIL, no accounting method will be used any more. To make the accounting return successfully, even if no specified methods reply, it is possible to specific "none" as the last accounting method.

Note The keyword "start-stop" is used for the network access server to send the accounting information at the start and end of the network service to the security server.

1.5.3.1 Using the Radius for exec accounting

To configure the use of RADIUS server for Exec acounting, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see Configuring RADIUS.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa accounting exec {**default** | *list-name*} **start-stop group radius**	Define RADIUS accounting method.
end	Return to the privileged mode.
show aaa method-list	Confirm the configured method list.
configure terminal	Enter the global configuration mode.
line vty *line-num*	Enter the line configuration mode.
accounting exec {**default** | *list-name*}	Apply the method list.
end	Return to the privileged mode.
show running-config	Confirm the configuration.

1.5.3.2 Example of Configuring Exec Accounting

The example below illustrates how to configure exec accounting. The local login authentication and the Radius exec authorization are used when the user on the vty line 0-4 loggs in. The access server uses the Radius server with IP address 192.168.217.64 and shared keyword test. The local username and password are DES-7200

```
DES-7200# configure terminal
```

```
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# radius-server key test
DES-7200(config)# username DES-7200 password DES-7200
DES-7200(config)# aaa authentication login auth local
DES-7200(config)# aaa accouting exec acct start-stop group radius
DES-7200(config)# line vty 0 4
DES-7200(config-line)# login authentication auth
DES-7200(config-line)# accounting exec acct
DES-7200(config-line)# end
DES-7200(config)# show running-config
!
aaa new-model
!
aaa accounting exec acct start-stop group radius
aaa authentication login auth local
!
username DES-7200 password DES-7200
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
line con 0
line vty 0 4
accounting exec acct
login authentication auth
!
end
```

1.5.4 Configuring AAA Network Accounting

The network accounting provides the accounting information about user session, including the packet number, bytes, IP address and username. Now the network accounting only support RADIUS.

Note The format of Radius accounting information varies with the Radius security server. The contents of the account records may also vary with our product version.

To configure the AAA network accounting, run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa accounting network{**default** | *list-name}* **start-stop** *method1 [method2*|…]	Define the AAA network accounting method list. If you need to define multiple method lists, execute this command repeatedly.

The keyword "list-name" is used to name the created accounting method list, which can be any string. The keyword "method" means the actual algorithm for accounting. Only when the current method returns ERROR (no reply), the next accounting method will be attempted. If the current method returns FAIL, no accounting method will be used any more. To make the accounting return successfully, even if no specified methods reply, it is possible to specific "none" as the last accounting method.

1.5.4.1 Using Radius for network accounting

To configure the use of RADIUS server for network acounting, it is required to first configure the RADIUS server. For the details of the RADIUS server configuration, see Configuring RADIUS.

After configuring the RADIUS server, the RADIUS server-based method list can be configured. Run the following commands in the global configuration mode:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa accounting network {**default** | *list-name*} **start-stop group radius**	Define RADIUS accounting method.

1.5.4.2 Example of Configuring Network Accounting

The example below illustrates how to configure network authorization using RADIUS.

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
DES-7200(config)# radius-server key test
DES-7200(config)# aaa accounting network acct start-stop group radius
DES-7200(config-line)# end
DES-7200(config)# show running-config
!
aaa new-model
!
aaa accounting network acct start-stop group radius
!
radius-server host 192.168.217.64
radius-server key 7 093b100133
!
```

1.6 Monitoring AAA user

To view the information of the current login users, run the following commands in the privileged

user mode:

Command	Function
show aaa user { *id* | **all** }	View the information of the current AAA user.

1.7 Configuring VRF-supported AAA Group

Virtual Private Networks (VPNs) provides a secure method for bandwidth share on the ISP backbone network. One VPN is the collection of the sharing routes. The user station is linked with the service vendor network via one to multiple interfaces. The VPN routing table is also called VPN routing//forwarding(VRF) table. AAA can specify the VRF for each self-defined server group.

In the global configuration mode, use the following command to configure VRF for the AAA group:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa group server radius *gs_name*	Configure the RADIUS server group and enter the server group configuration mode.
ip vrf forwarding *vrf_name*	Specify the vrf for the group.

Note It is valid for the product supporting VRF function.

1.8 Configuring Failed Authentication Lockout of Login User

To prevent login user from decoding password, use command to limit the attempt times. If you has attempted more than the limited times, you will not login during the lockout.

In the global configuration mode, use the following command to configure login parameters:

Command	Function
configure terminal	Enter the global configuration mode.

Command	Function
aaa new-model	Turn on the AAA switch.
aaa local authentication attempts *<1-2147483647>*	Configure attempt times of login user.
aaa local authentication lockout-time*<1-2147483647>*	Configure lockout-time(hour) when the user has attempted more than the limited times.
show aaa user lockout {**all** | **user-name** <*word*>}	Display current lockout user list.
clear aaa local user lockout {**all** | **user-name** <*word*>}	Clear lockout user list.

Note By default, login attempt times are 3 and the lockout time is restricted to be 15 hours.

1.9 Configuring Domain-name-based AAA Service

The domain-name-based AAA service configurations include:

- Overview
- Domain-name-based AAA service configuration tasks
- Domain-name-based AAA service configuration note
- Domain-name-based AAA service configuration example

Caution The domain-name-based AAA service is applied to the IEEE802.1x authentication service. For the detailed IEEE802.1x protocol configurations, please refer to the chapter of *802.1x Configuration*.

1.9.1 Overview

In the multi-domain environment, one NAS(Network Access Switch) can provide the AAA service for the users in different domains. Due to the different user attributes(such as the username, password, service type, privilege, ect) in each domain, it needs to tell them apart by setting the domain method and set the attribute collection for each domain, including the AAA service method list.

Note

DES-7200 product supports the following types of username:

1. userid@domain-name
2. domain-name\userid
3. userid.domain-name
4. userid

For the type4 username, i.e., userid, without the domain-name, its domain-name is default.

The followings are the basic principles for the domain-name-based AAA service:

- Resoluting the domain-name carried by the user
- Searching for the user domain according to the domain-name
- Searching for the AAA service method list-name according to the domain configurations
- Searching the corresponding method list according to the method list-name in the system
- Providing the AAA service using the method list

Note

One of the abovementioned steps fails, the AAA service cannot be used.

The following is the typical topology in the multi-domain environment:

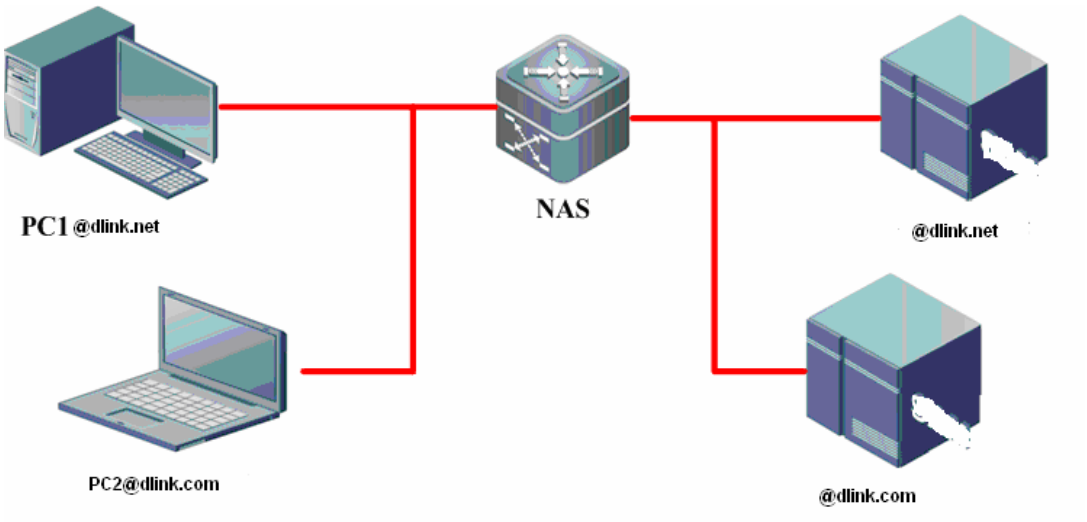


Figure-2 Typical topology for the multi-domain network

1.9.2 Domain-name-based AAA Service Configuration Tasks

Note The system supports up to 32 domains.

1.9.2.1 Enabling AAA

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.

For the detailed command descriptions, please refer to the chapter of *Enabling AAA*.

1.9.2.2 Defining the AAA Service Method list

Command	Function
configure terminal	Enter the global configuration mode.
aaa authentication dot1x {**default** | *list-name*} *method1* [*method2*...]	Define the IEEE802.1x authentication method list.
aaa accounting network {**default** | *list-name*} **start-stop** *method1* [*method2*...]	Define the Network accounting method list.
aaa authorization network {**default** | *list-name*} *method1* [*method2*...]	Define the Network authorization method list.

For the detailed command descriptions, please refer to the chapter of *Configuring authentication, Configuring accounting and Configuring authorization.*.

1.9.2.3 Enabling the Domain-name-based AAA Service Switch

Command	Function
configure terminal	Enter the global configuration mode.
aaa domain enable	Enable the domain-name-based AAA service switch.

1.9.2.4 Creating the Domain

You shall follow the following rules when searching for the domain-name matched the

username:

1. Support to use the single character, such as ".", "\", "@" to tell the username and the domain-name apart.

2. The single "@" character is followed by the character string "domain-name". With multiple "@" characters in the username, use the character string following the last "@" characeter as the domain-name. For example, if the username is a@b@c@d, use the a@b@c as the username and use the d as the domain-name.

3. The single "\" character follows the character string "domain-name". With multiple "\" characters in the username, use the character string followed by the first "\" characeter as the domain-name. For example, if the username is a\b\c\d, use the b\c\d as the username and use the a as the domain-name.

4. The single "." character is followed by the character string "domain-name". With multiple "." characters in the username, according to the pre-settings, use the character string following the last "." characeter as the domain-name. For example, if the username is a.b.c.d, use the a.b.c as the username and use the d as the domain-name.

5. If all characters of ".", "\" and "@" exist in the username, when matching the domain-name, use the rules in sequence of the "@", "\" and "." characters.

Command	Function
configure terminal	Enter the global configuration mode.
aaa domain *domain-name*	Create the domain and enter the domain configuration mode.

Note The domain-name-based AAA service supports the domain name in the length of up to 64 characters, which is not case-sensitive.

1.9.2.5 Configuring the Domain Attribute Collection

Use the following commands to select the AAA service method list in the domain configuration mode:

Command	Function
authentication dot1x {**default** | *list-name*}	In the domain configuration mode, select the authentication method list.
accounting network {**default** | *list-name*}	In the domain configuration mode, select the accounting method list.

Command	Function
authorization network {**default** | *list-name*}	In the domain configuration mode, select the authorization method list.

Use this command to configure the domain state:

Command	Function
state {**block** | **active**}	In the domain configuration mode, set the domain state.

Use this command to check whether the username carries with the domain-name information:

Command	Function
username-format {**without-domain** | **with-domain**}	In the domain configuration mode, check whether the username carries with the domain-name information when the NAS is interacting with the server.

Use this command to set the maximum user number supported in the domain:

Command	Function
access-limit *num*	In the domain configuration mode, set the maximum user limit in the domain. By default, no user limit has been configured(only valid for the 802.1x user).

Note

1. To select the AAA service method list in the domain configuration mode, the AAA service method list is defined before entering the domain configuration mode. Or the configurations are inexistent when selecting the AAA method list-name.

2. With the domain-name-based AAA service enabled, if there is no domain information carried by the username, use the default domain; if there is no configurations for the user domain in the system, the user is determined to be illegal and provides no AAA service.

3. In the domain configuration mode, without the method list configured, use the default method list in the system.

1.9.2.6 Showing the domain configuration

Use the following commands to show the domain-name-based AAA service information.

Command	Function
show aaa domain [*domain-name*]	Show the current domain-name-based AAA service information

1.9.3 Domain-name-based AAA Service Configuration Notes

The followings are the domain-name-based AAA service configuration notes:

1. With the domain-name-based AAA service enabled, use the method list in the domain. Without the service enabled, use the method list selected according to the access protocol(such as 802.1x, ect) for the AAA service. For example, without the service enabled, use the **dot1x authentication** *authen-list-name,* **dot1x accounting** *acct-list-name authen-list-name* and **dot1x accounting** *acct-list-name acct-list-name* command to provide the AAA service for the authentication and accouting method list name.

2. With the domain-name-based AAA service enabled, by default, there is no default domain, and you shall manually set the default domain-name as “default”. After the configuration, user that not carries with the domain information provides the AAA service using the default domain. Without the default domain configured, the user that not carries with the domain information fails to use the AAA service.

3. If the domain information is carried by the auth-user but the domain is not configured on the device, it fails to provide the AAA service for the user.

4. The AAA service method list selected by the domain must be consistent with the one defined by the AAA service. Or it fails to provide the AAA service for the users in the domain.

5. The domain name carried by the user shall be accurately matched with the one configured on the device. For example, the domain.com and the domain.com.cn have been configured on the device, and the request message carried by the user is aaa@domain.com, the device determines that the user belongs to the domain.com but not the domain.com.cn.

1.9.4 Domain-name-based AAA Service Configuration Example

The following is an example of configuring the domain-name-based AAA service:

```
DES-7200(config)# aaa new-model
```

```
DES-7200(config)# radius-server host 192.168.197.154

DES-7200(config)# radius-server key test

DES-7200(config)# aaa authentication dot1x default group radius

DES-7200(config)# aaa domain domain.com

DES-7200(config-aaa-domain)# authentication dot1x default

DES-7200(config-aaa-domain)# username-format without-domain
```

After the configuration, with the user a1 in the radius server, use the 802.1x client to login the server for authentication by keying in the username a1@domain.com and the correct password. The following shows the related domain-name information:

```
DES-7200#show aaa domain domain.com


=============Domain domain.com=============

State: Active

Username format: Without-domain

Access limit: No limit

802.1X Access statistic: 0


Selected method list:

 authentication dot1x default
```

1.10 Typical AAA Configuration Example

1.10.1 Typical AAA Aplication

1.10.1.1 Network Topology

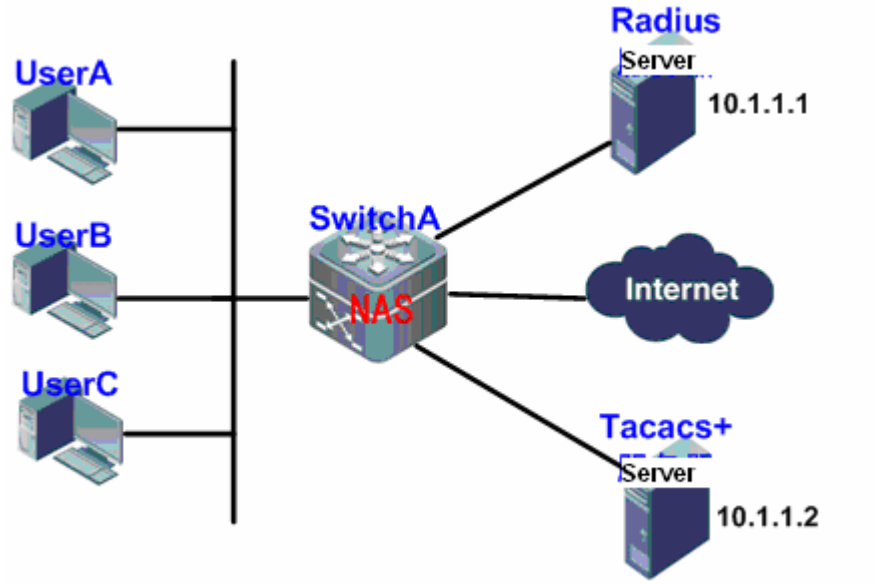


Figure 3 Typical AAA Application Topology

1.10.1.2 Network Requirements

For better security management for the SwitchA in the Figure-3, the followings are the network requirements:

1. The administrators shall have the individual username and password for the convenience of the account management.

2. The user authentication methods are divided into local authentication and collection authentication. The method of combining the collection-authentication with the local-authentication shall be adopted, with the collection-authentication mainly-used and the local-authentication as backup. In the process of the collection-authentication, the Radius server authentication shall be passed first, if there is no reply, it will switch to the local authentication.

3. Different users can be configured to access to the specified network device during the authentication.

4. User management priority: divide the network management users into the super users and ordinary users, wherein the super users own the priority of reading and writing while the

ordinary users own the reading priority only.

5. The user authentication information, the authorization information and the network information are recorded in the server for the display and audit later(This example uses the TACACS+ for the accounting.)

1.10.1.3 Configuration Key-points

From the analysis of the part of "*Network Requirements*", deploying the AAA function can address the above requirements, which is to dynamically configure the ID authentication, authorization and accounting type for the user(line) or the server. Define the ID authentication, authorization and accounting type by creating the method list, and apply the method list to the specified service or interface. For the details, see the following "*Configuration Steps*".

1.10.1.4 Configuration Steps

#Enable AAA:

！Enable the AAA function on the device

```
DES-7200#configure terminal

DES-7200(config)#aaa new-model
```

 # Configure the security server:

The network security server takes the responsibilty for the authentication, the authorization and the accounting. The user information are stored in the server and the software of the server can record, calculate and analyze the various information via the syslogs.

！ Configure the Radius server information (the shared key for the communication between the device and the Radius server is DES-7200)

```
DES-7200(config)#radius-server host 10.1.1.1

DES-7200(config)#radius-server key DES-7200
```

！ Configure Tacacs+ server information (the shared key for the communication between the device and the Tacacs+ server is redgiant)

```
DES-7200(config)#tacacs-server host 10.1.1.2

DES-7200(config)#tacacs-server key redgiant
```

 # Configure the local user:

！ Configure the password encryption (the key information for the local password and the security server are saved and shown in the simply-encrypted format)

```
DES-7200(config)#service password-encryption
```

！ Configure the local user database (Configure the username and the password, and set the user privilege level)

```
DES-7200(config)#username bank privilege 10 password yinhang

DES-7200(config)#username super privilege 15 password star

DES-7200(config)#username normal privilege 2 password normal

DES-7200(config)#username test privilege 1 password test
```

！ Configure the local enable password for the local enable authentication

```
DES-7200(config)#enable secret w
```

！ Configure the line login password (with the AAA function enabled, the login password of the terminal line takes no effect. So the line login password configuration is to prevent the login failure with the AAA function disabled)

```
DES-7200(config)#line vty 0 15

DES-7200(config-line)#password w
```

！ Configure the line user privilege level (with the Exec authorization disabled, or no Exec authorization method list is applied in the line and no default Exec authorization method list, the configure line user privilege level should be used)

```
DES-7200(config)#line vty 0 15

DES-7200(config-line)#privilege level 10
```

 # Configure the authentication

1. Login authentication

The Login authentication is used to control the user access. There are two methods to define the authentication method list: 1) Radius; 2) Local.

！ Configure login authentication method list and apply it to the corresponding line

```
DES-7200(config)# aaa authentication login hello group radius local

DES-7200(config)# line vty 0 15

DES-7200(config-line)# login authentication hello
```

To prevent the user from using the exhaust algorithm to crack the password during the Login authentication, AAA is used to limit the user Login attempts. When the authentication attempts reached the configured limit, the user would fail to log in for the lockout time(by default, the login authentication attempt is 3 times and the lockout time is 15 hours.)

！Configure the authentication attempt 2 times and the authentication lockout-time 10 hours

```
DES-7200(config)#aaa local authentication attempts 2

DES-7200(config)#aaa local authentication lockout-time 10
```

2. Enable authentication

The Enable authentication is used to switch the user privilege level. An authentication process is needed before the user switches the privilege level to the superuser using the **enable** command. There are two methods to define the authentication method list: 1) Radius; 2) Local. The Enable authentication can only set the default method list, which will be auto-applied after the configuration.

！Configure the enable authentication method list

```
DES-7200(config)#aaa authentication enable default group radius local
```

 # Configure the authorization

1. Exec authorization

The Exec authorization is used to control the user command privilege level. For example, level 15 is the superuser, level 14 is the configuration user, level 2 is the ordinary user. The remote Exec authorization takes precedence over the local one.

！ Configure the exec authorization method list and apply it to the line

```
DES-7200(config)#aaa authorization exec shouquan group tacacs+ local

DES-7200(config)#line vty 0 15

DES-7200(config-line)#authorization exec shouquan
```

！ Configure the exec authorization for the console (by default, the exec authorization is not for the console)

```
DES-7200(config)#aaa authorization console
```

2. Command authorization

The Command authorization is used to offer the execution privilege of the key commands only to the administrators. The Command authorization authorizes the level of the command but not of the current user. The Radius protocol is not supported.

！Configure the Command authorization method list and apply it to the line.

```
DES-7200(config)#aaa authorization commands 2 abc group tacacs+ local

DES-7200(config)#line vty 0 15
```

```
DES-7200(config-line)#authorization commands 2 abc
```

 # Configure the accounting

1. Exec accounting

The Exec accouting is used to send the messages of the user login and logout to the server for the displaying, statistics and the auditing.

！ Configure the exec accouting method list and apply it to the line

```
DES-7200(config)#aaa accounting exec default start-stop group tacacs+
```

2. Command accounting

The Command accouting is used to send the commands of a specific level executed by the user to the server for the displaying, statistics and the auditing.

！Configure the command accounting method list and apply it to all lines

```
DES-7200(config)#aaa accounting commands 2 default start-stop group tacacs+
```

1.10.1.5 Configuration verification

Step 1: Use the **show running-config** command to show the current configurations:

```
DES-7200(config)#show run


Building configuration...

Current configuration : 2337 bytes


!

!

aaa new-model

aaa local authentication attempts 2

aaa local authentication lockout-time 10

!

!

!

aaa authorization exec shouquan group tacacs+ local
```

```
aaa authorization commands 2 abc group tacacs+
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 2 default start-stop group tacacs+
aaa authentication login hello group radius local
aaa authentication enable default group radius local
!
!
vlan 1
!
!
username bank password 7 09361c1c2f041c4d
username bank privilege 10
username super password 7 093c011335
username super privilege 15
username normal password 7 09211a002a041e
username normal privilege 2
username test password 7 093b100133
service password-encryption
!
!
!
!
tacacs-server key 7 072c062b121b260b06
tacacs-server host 10.1.1.2
radius-server host 10.1.1.1
radius-server key 7 072c16261f1b22
enable secret 5 $1$2MjW$xr1t0s1Euvt76xs2
!
!
```

```
!
!
!
line con 0
line vty 0 4
 authorization exec shouquan
 authorization commands 2 abc
 privilege level 10
 login authentication hello
 password 7 0938
line vty 5 15
 authorization exec shouquan
 authorization commands 2 abc
 privilege level 10
 login authentication hello
 password 7 005d
!
!
end
```

Step 2: In the actual application, use the **show aaa user {** *id* **| all }** command to show the current AAA user information.

1.10.2 AAA Multi-domain Authentication Application

1.10.2.1 Network Topology

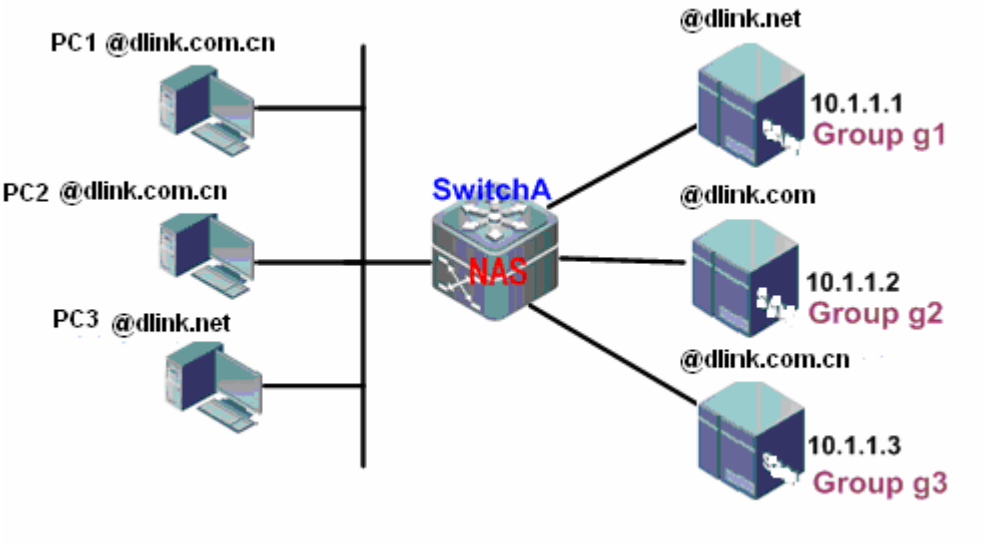


Figure-4 AAA multi-domain authentication application topology

1.10.2.2 Network Requirements

Configure the NAS device (SwitchA) to enable the domain-name-based AAA service, including the authentication, authorization and the accounting:

- Use the 802.1x client for the login authentication with the username PC1@DES-7200.com or PC2@DES-7200.com.cn or PC3@DES-7200,.net and the password.
- User network management: classify the users into the superusers and the ordinary users, wherein the superusers are able to read and write while the ordinary users are able to read only.
- The user authentication, authorization and network action messages are saved in the authentication server for the displaying and the auditing.

1.10.2.3 Configuration Key-points

Configure the domain-name-based AAA service to address the above network requirements.

1.10.2.4 Configuration Steps

#Enable AAA:

! Enable the AAA function on the device

```
DES-7200#configure terminal

DES-7200(config)#aaa new-model
```

 # Configure the security server:

The network security server takes the responsibilty for the authentication, the authorization and the accounting. The user information are stored in the server and the software of the server can record, calculate and analyze the various information via the syslogs.

！ Configure the Radius server information (the shared key for the communication between the device and the Radius server is DES-7200)

```
DES-7200(config)#aaa group server radius g1

DES-7200(config-gs-radius)#server 10.1.1.1

DES-7200(config-gs-radius)#exit

DES-7200(config)#aaa group server radius g2

DES-7200(config-gs-radius)#server 10.1.1.2

DES-7200(config-gs-radius)#exit

DES-7200(config)#aaa group server radius g3

DES-7200(config-gs-radius)#server 10.1.1.3

DES-7200(config-gs-radius)#exit

DES-7200(config)#radius-server key DES-7200
```

 # Configure the local user:

！Configure the password encryption (the key information for the local password and the security server are saved and shown in the simply-encrypted format)

```
DES-7200(config)#service password-encryption
```

！Configure the local user database (Configure the username and the password, and set the user privilege level)

```
DES-7200(config)#username bank privilege 10 password yinhang

DES-7200(config)#username super privilege 15 password star

DES-7200(config)#username normal privilege 2 password normal

DES-7200(config)#username test privilege 1 password test
```

！ Configure the local enable password for the local enable authentication

```
DES-7200(config)#enable secret w
```

 # Define the AAA service method list

! Configure dot1x authentication

```
DES-7200(config)#aaa authentication dot1x renzheng group radius local
```

! Configure network authorization

```
DES-7200(config)#aaa authorization network shouquan group radius
```

! Configure network accounting

```
DES-7200(config)#aaa accounting network jizhang start-stop group radius
```

 # Enable the domain-based AAA service switch

```
DES-7200(config)#aaa domain enable
```

 # Create the domain and configure the domain attribute collection

! Create the domain

```
DES-7200(config)#aaa domain DES-7200.com
```

! Associate the AAA service method list

```
DES-7200(config-aaa-domain)#authentication dot1x renzheng
DES-7200(config-aaa-domain)#authorization network shouquan
DES-7200(config-aaa-domain)#accounting network jizhang
```

! Configure the domain state

```
DES-7200(config-aaa-domain)#state active
```

! Configure the username without the domain

```
DES-7200(config-aaa-domain)#username-format without-domain
!
DES-7200(config)#aaa authentication dot1x renzheng group g2
DES-7200(config)#aaa authorization network shouquan group g2

DES-7200(config)#aaa accounting network jizhang start-stop group g2
```

The configurations of the DES-7200.com.cn and the DES-7200.net are similar.

1.10.2.5 Configuration verification

Step 1: Use the **show running-config** command to show the current configurations (take the domain name DES-7200.com for example):

```
DES-7200#show run


Building configuration...

Current configuration : 2013 bytes


!

aaa new-model

aaa domain enable

!

aaa domain DES-7200.com

 authentication dot1x renzheng

 accounting network jizhang

 authorization network shouquan

 username-format without-domain

!

!

aaa group server radius g1

 server 10.1.1.1

!

aaa group server radius g2

 server 10.1.1.2

!

aaa group server radius g3

 server 10.1.1.3
```

```
!
!
aaa accounting network jizhang start-stop group g2
aaa authorization network shouquan group g2
aaa authentication dot1x renzheng group g2
!
!vlan 1
!
!
no service password-encryption
!
!
radius-server key DES-7200
!
!
!
```

Step 2: Show the domain-based AAA service domain information:

```
DES-7200#show aaa domain

=============Domain DES-7200.com=============
State: Active
Username format: Without-domain
Access limit: No limit
802.1X Access statistic: 0

Selected method list:
 authentication dot1x renzheng
 authorization network shouquan
```

```
accounting network jizhang
```

2 RADIUS Configuration

2.1 Radius Overview

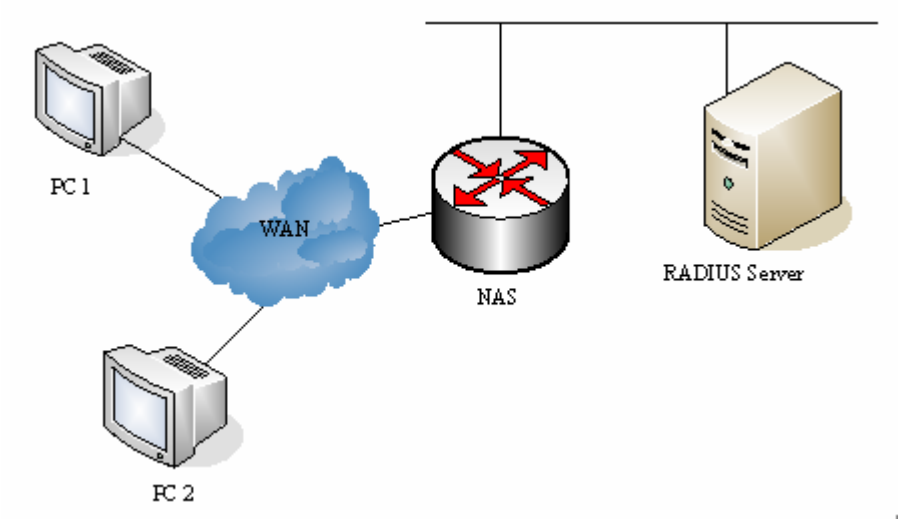
The Remote Authentication Dial-In User Service (Radius) is a distributed client/server system that works with the AAA to perform authentication for the users who are attempting to make connection and prevent unauthorized access. In the implementation of our product, the RADIUS client runs on the router or the network access server (NAS) to send the authentication requests to the central RADIUS server. The central center includes all information of user authentication and network services.

Since the RADIUS is a completely-open protocol, it has become a component and been installed in such systems as UNIX and WINDOWS 2000, so it is the security server most widely used for the time being.

The running process of the RADIUS is as follows:

- Prompt the user to enter username and password.
- The username and the encrypted password are sent to the RADIUS server via the network.
- The RADIUS returns one of the following responses:
- The user authentication passes.
- The user authentication fails and it prompts to reenter the username and password.
- The RADIUS server sends the challenge request to gather more authentication information from the user.
- The user authorization information is included in the ACCEPT response.

Here is a typical RADIUS topology:



Typical RADIUS network configuration

2.2 RADIUS Configuration Tasks

To configure Radius on the network device, perform the following tasks first:

- Enable AAA. For the details, see *AAA Overview*.
- Define the RADIUS authentication method list by using the **aaa authentication** command. For details about how to use "aaa authentication" to define the authentication method list, see *Configuring Authentication*.
- Apply the defined authentication list on the specific line; otherwise the default authentication list will be used for authentication. For more details, see *Configuring Authentication.*

After the configuration is completed, you may start to configure the RADIUS. The configuration of the RADIUS consists of the following parts:

- Configuring Radius Protocol Parameters
- Specify the RADIUS authentication.

2.2.1 Configuring Radius Protocol Parameters

Before configuring the Radius on the network device, the network communication shall operate perfectly on the Radius server. To configure RADIUS protocol parameters, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the IP address or hostname of the remote Radius security server and specify the authentication port and accounting port.
radius-server key *string*	Configure the sharing password for the communication between the device and Radius server
radius-server retransmit *retries*	Specify the times of sending requests before the router confirms Radius invalid (3 by default)
radius-server timeout *seconds*	Specify the waiting time before the router resend request (2 s by default)
radius-server deadtime *minutes*	Specify the waiting time before the server is considered dead in case of no response to the request sent by the device (5 minutes by default).

Caution To configure the RADIUS, it is necessary to configure the RADIUS Key. The sharing password on the network device and the sharing password on the Radius server must be the same.

2.2.2 Specifying the Radius Authentication

This means defining the authentication method list for the Radius after the Radius server is specified and the Radius authentication sharing password is defined. Since the RADIUS authentication is done via AAA, it is required to execute the **aaa authentication** command to define the authentication method list and specify the authentication method as RADIUS. For more details, see AAA Configurations.

2.2.3 Specifying the Radius Standard Attribute Type

This chapter introduces configuration of Radius standard attribute type. Now the RADIUS Calling-Station-ID attribute(the attribute type is 31) is supported.

2.2.3.1 Configuring Calling-Station-ID Format

RADIUS Calling-Station-ID attribute is used to identify the NAS when the NAS is sending the request packets to the RADIUS server. The contents of the RADIUS Calling-Station-ID are character strings, which can be in multiple formats. The MAC address for the NAS is usually used as the content of the Calling-Station-ID to solely identify the NAS. The table blow lists the

formats of the MAC address:

Format	Description
ietf	The standard format specified by the IETF （RFC3580）. ‘-’ is used as the seperator, for example: 00-D0-F8-33-22-AC.
normal	Normal format representing the MAC address. ‘.’ is used as the seperator. For example: 00d0.f833.22ac.
unformatted	No format and seperator. By default, unformatted is used. For example: 00d0f83322ac.

To configure the RADIUS Calling-Station-ID MAC-based attribute format, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
radius-server attribute 31 mac format {ietf | normal | unformatted}	Configure the RADIUS Calling-Station-ID MAC-based attribute format. The default format is **unformatted**.

2.2.4 Specify Radius Private Attribute Type

The contents in this section enable configuring freely the type of private attributes. The default configurations are as follows:

Default configurations of our product private attribute recognition:

ID	Function	Type
1	max down-rate	1
2	qos	2
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-diractory	9

ID	Function	Type
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15
16	max up-rate	16
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilige	22
23	login privilige	42
24	limit to user number	50

Extended manufacturer ID default configuration:

ID	Function	TYPE
1	max down-rate	76
2	qos	77
3	user ip	3
4	vlan id	4
5	version to client	5
6	net ip	6
7	user name	7
8	password	8
9	file-diractory	9
10	file-count	10
11	file-name-0	11
12	file-name-1	12
13	file-name-2	13
14	file-name-3	14
15	file-name-4	15

ID	Function	TYPE
16	max up-rate	75
17	version to server	17
18	flux-max-high32	18
19	flux-max-low32	19
20	proxy-avoid	20
21	dailup-avoid	21
22	ip privilige	22
23	login privilige	42
24	limit to user number	50

Note

Two functions cannot be configured with the same type number.

Here is an example on how to configure the private type for network device:

```
DES-7200# show radius vendor-specific
id   vendor-specific      type-value
---- -------------------- ----------
1    max down-rate        76
2    qos                  77
3    user ip              3
4    vlan id              4
5    version to client    5
6    net ip               6
7    user name            7
8    password             8
9    file-diractory       9
10   file-count           10
11   file-name-0          11
12   file-name-1          12
13   file-name-2          13
14   file-name-3          14
15   file-name-4          15
16   max up-rate          75
17   version to server    17
18   flux-max-high32      18
19   flux-max-low32       19
20   proxy-avoid          20
21   dailup-avoid         21
22   ip privilige         22
23   login privilige      42
24   limit to user number 50
DES-7200# configure
DES-7200(config)# radius attribute 24 vendor-type 67
```

```
DES-7200(config)# show radius vendor-specific
id   vendor-specific      type-value
---- -------------------- ----------
1    max down-rate        76
2    qos                  77
3    user ip              3
4    vlan id              4
5    version to client    5
6    net ip               6
7    user name            7
8    password             8
9    file-diractory       9
10   file-count           10
11   file-name-0          11
12   file-name-1          12
13   file-name-2          13
14   file-name-3          14
15   file-name-4          15
16   max up-rate          75
17   version to server    17
18   flux-max-high32      18
19   flux-max-low32       19
20   proxy-avoid          20
21   dailup-avoid         21
22   ip privilige         22
23   login privilige      42
24   limit to user number 50
DES-7200(config)#
DES-7200(config)#
```

2.2.5 Configuring the Reachability Detection for RADIUS server

The device maintains the reachability state of each RADIUS server configured: reachable or unreachable. The device won't send the authentication, authorization and accounting requests of the access user to an unreachable RADIUS server, unless all RADIUS servers in the RADIUS server group are all unreachable.

The device can carry out active detection of the specified RADIUS server, and this feature is disabled by default. If you enable active detection of the specified RADIUS server, the device will periodically send detection requests (authentication requests or accounting requests) to the RADIUS server. The corresponding interval will be:

- RADIUS server in reachable state: the default interval for active detection is 60 minutes.
- RADIUS server in unreachable state: fixed to 1 minute.

To enable active detection of the specified RADIUS server, the following conditions must be met:

1. Testing user name for this RADIUS server has been configured on the device.
2. At least one tested port of this RADIUS server (authentication port or accounting port) has been configured on the device.

For a RADIUS server in reachable state, the device will considered this RADIUS server unreachable if the following two conditions are met:

1. The time configured by "**radius-server dead-criteria time** *seconds*" is exceeded after correct response is last received from this RADIUS server.
2. After correct response is last received from this RADIUS server, the number of tries to send requests to this RADIUS server when no correct response is received has exceeded the number set by "**radius-server dead-criteria tries** *number*".

Note

For a RADIUS server in unreachable state, the device will considered this RADIUS server reachable if any of the following conditions is met:

1. Correct response is received from this RADIUS server.
2. The duration that this RADIUS server remains unreachable exceeds the time set by "**radius-server deadtime**", and active detection of this RADIUS server is not enabled.
3. The authentication port or accounting port of this RADIUS server is updated on the device.

RADIUS server reachability detection allows the user to configure the dead-criteria conditions for a RADIUS server and active detection.

To configure RADIUS dead-server detection, execute the following commands in global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.

Command	Function
DES-7200(config)# **radius-server dead-criteria time** *seconds* **tries** *number*	Globally configure the dead-criteria conditions for a RADIUS server to be marked as dead. The default value of "seconds" is 60, and the default value of "number" is 10.
DES-7200(config)# **radius-server deadtime** *minutes*	Configure the duration for the device to stop sending request packets to the RADIUS server in unreachable state (default: 0 minute).
DES-7200(config)# **radius-server host** *ip-address* [**auth-port** *port*] [**acct-port** *port*] [**test username** *name* [**idle-time** *time*] [**ignore-auth-port**] [**ignore-acct-port**]]	Configure the IP address of remote RADIUS server, specify the authentication port and accounting port, and specify relevant parameters of active detection (testing user name, interval for active detection of RADIUS server in reachable state, and whether the authentication port or the accounting port shall be neglected).

Caution

The dedicated testing user name shall be used. This user name must not be used by other valid access users, so as not to affect the authentication, authorization or accounting of other valid users.

2.3 Monitoring RADIUS

To monitor the RADIUS, execute the following commands in the privileged user mode:

Command	Function
debug radius event	Turn on the Radius debug switch to view the Radius debug information

2.4 Radius Configuration Example

In a typical Radius network configuration diagram, the RADIUS server performs authentication for the visiting users, enables the accounting function for the visiting users and records the network usage of the users.

Note

The RADIUS server can be a component that comes with the Windows 2000/2003 server (IAS) or the UNIX system, or the special server software of some manufacturers.

Here is an example on how to configure the Radius for network device:

```
DES-7200# configure terminal
```

```
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.12.219
auth-port 1645 acct-port 1646
DES-7200(config)# radius-server key aaa
DES-7200(config)# aaa authentication login test group radius
DES-7200(config)# end
DES-7200# show radius server
Server IP:      192.168.12.219
Accounting Port: 1646
Authen  Port:    1645
Server State:    Ready
DES-7200#configure terminal
DES-7200(config)#line vty 0
DES-7200(config-line)#login authentication test
DES-7200(config-line)#end
DES-7200#show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
username DES-7200 password 0 starnet
!
radius-server host 192.168.12.219 auth-port 1645 acct-port 1646
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

2.5 Radius IPv6 Configuration Example

In the typical RADIUS network configuration diagram, RADIUS server authenticates the access users, enables accounting of access users and records the network service usage by users.

Note

RADIUS server shall be running Windows 2008 Server or other dedicated IPv6 server software recognized by the manufacturer.

The following example shows how to configure RADIUS on the network device:

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 3000::100 auth-port 1645 acct-port 1646
DES-7200(config)# radius-server key aaa
DES-7200(config)# aaa authentication login test group radius
```

```
DES-7200(config)# end
DES-7200# show radius server
Server IP:       3000::100
Accounting Port: 1646
Authen  Port:    1645
Test Username:    <Not Configured>
Test Idle Time:   60 Minutes
Test Ports:      Authen and Accounting
Server State:    Active
     Current duration 765s, previous duration 0s
    Dead: total time 0s, count 0
    Statistics:
       Authen: request 15, timeouts 1
       Author: request 0, timeouts 0
       Account: request 0, timeouts 0

DES-7200# configure terminal
DES-7200(config)# line vty 0
DES-7200(config-line)# login authentication test
DES-7200(config-line)# end
DES-7200# show running-config
!
aaa new-model
!
!
aaa authentication login test group radius
!
!
!
radius-server host 3000::100 auth-port 1645 acct-port 1646
radius-server key aaa
!
line con 0
line vty 0
login authentication test
line vty 1 4
!
```

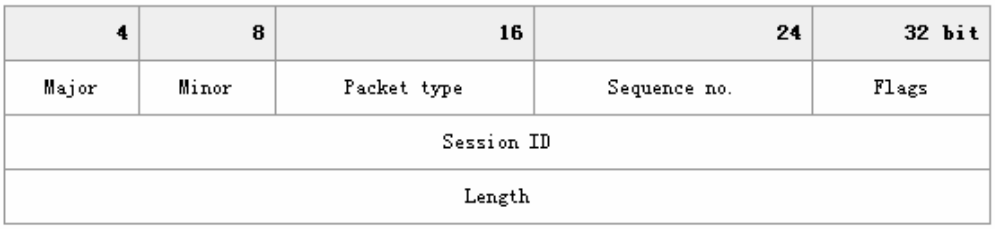
3 TACACS+ Configuration

3.1 TACACS+ Overview

TACACS+ is a security protocol with more powerful function on the basis of TACACS (RFC 1492 Terminal Access Controller Access Control System). It implements AAA function of multi-users by Client-Server mode and TACACS server communication. It needs to configure the related contents of TACACS+ server before using TACACS+ server.

TACACS+ supports user authentication, authorization and accounting analysis. That is, we can use one server to authenticate, another one to authorize and the third one to account at the same time. Each server has its own user data information, being antagonistic to authenticate, authorize and account.

The table below shows TACACS+ packet format:



4	8	16	24	32 bit
Major	Minor	Packet type	Sequence no.	Flags
Session ID				
Length				

Figure 1

- Major Version — Major TACACS+ Version number;
- Minor Version — Minor TACACS+ Version number;
- Packet Type — the value may include:

TAC_PLUS_AUTHEN: = 0x01 (Authentication);
TAC_PLUS_AUTHOR:= 0x02 (Authorization);
TAC_PLUS_ACCT:= 0x03 (Accounting).

- Sequence Number — packet sequence number in current session. The first TACACS+ packet sequence number in the session must be 1 and every packet sequence number followed is added by 1 gradually. Therefore, the client only sends the packet with odd sequence number, while TACACS+ Daemon only sends the packet with even sequence number.
- Flags — this field includes flag with various bitmap format. The Flag value

indicates whether the packet is encrypted or not.

- Session ID — ID in the TACACS+ session.
- Length —body length of TACACS+ packet (excluding head). All the packets are transmitted in the network in the encrypted form.

3.2 TACACS+ Application

The typical application of TACACS+ is the login management control of terminal users. TACACS+ client sends user name and password to TACACS+ server for authentication. After authentication and authorization, you can login to the switch for operation, which is shown as figure 2:

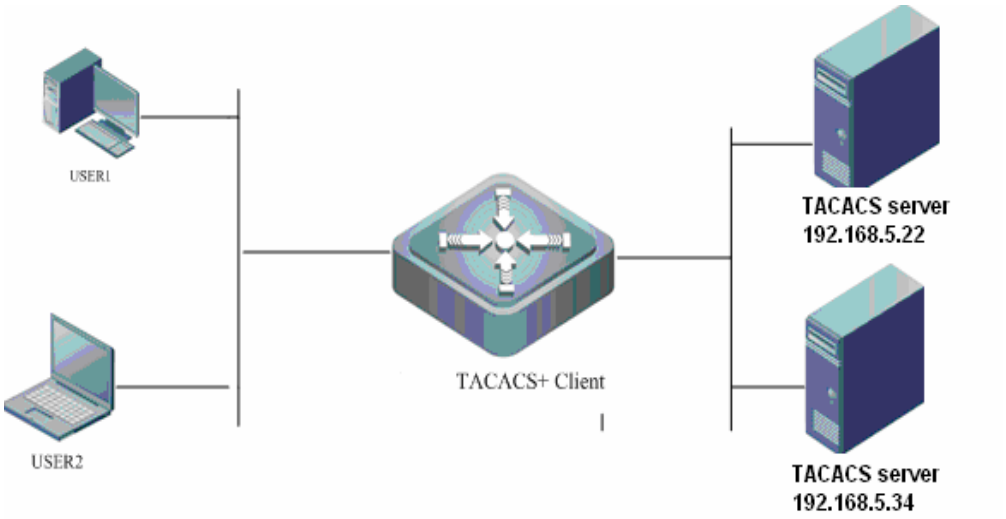


Figure 2

Figure 3 describes the interaction of the packets running in TACACS+ by login AAA:

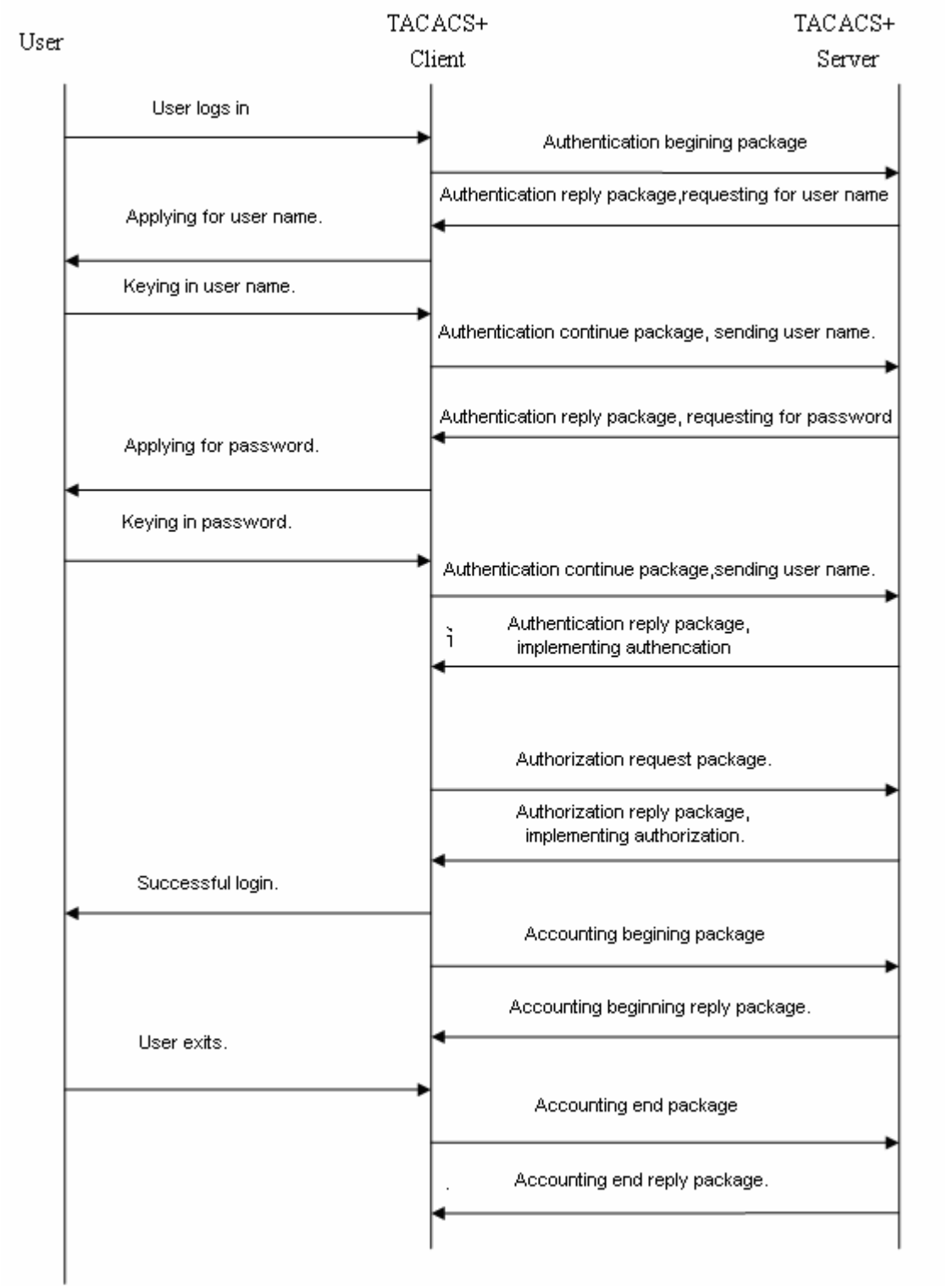


Figure 3

The whole process of basic information interaction is divided into three parts:

1. Authentication process includes:

a) User requests for logging in to the switch;

b) After receiving the request, TACACS+ Client sends the authentication beginning message to TACACS+ server;

c) TACACS+ server sends the authentication reply message, requesting for the user name;

d) TACACS+ Client asks user for user name.

e) The user keys in the login user name;

f) After receiving the user name, TACACS+ Client sends the authentication continue message including user name to TACACS+ server;

g) TACACS+ server sends authentication reply message, requesting for login password;

h) TACACS+ Client receives the login password;

i) The user keys in the login password;

j) After receiving the login password, TACACS+ Client sends authentication continue message including login password to TACACS+ server;

k) TACACS+ server sends authentication reply message, indicating that user has been authenticated.

2. Authorization process includes:

a) TACACS+ Client sends authorization request message to TACACS+ server.

b) TACACS+ server sends authorization reply message, indicating that user has been authenticated;

c) TACACS+ Client receives successful authorization reply message, outputting the configuration interface of switch to the user.

3. **Accounting process includes:**

a) TACACS+ Client sends the accounting beginning message to TACACS+ server;

b) TACACS+ server sends accounting beginning reply message, indicating that it has received the accounting beginning message;

c) The user exits;

d) TACACS+ Client sends the accounting end message to TACACS+ server;

e) TACACS+ server sends accounting end reply message, indicating that it has received the accounting end message.

3.3 TACACS+ Configuration Task

The following tasks must be executed before configuring TACACS+ on the network device:

- Use **aaa new-mode** to enable AAA. AAA must be enabled before using TACACS+; for the information how to enable **aaa new-mode**, please refer to AAA Overview.
- Use **tacacs-server host** to configure one or multiple tacacs+ servers.
- Use **tacacs-server key** to specify server and NAS shared key.
- Use **tacacs-server timeout** to specify timeout time waiting for the server reply;
- Use tacacs-server directed-request to enable the function of supporting the user to specify authentication server.
- If you need to authenticate, use **aaa authentication** to define using TACACS+ identity authentication method list. For the detailed information, please refer to authentication configuration.
- If you need to authorize, use **aaa authorization** to define using TACACS+ authorization method list. For the detailed information, please refer to authorization configuration.
- If you need to account, use **aaa accounting** to define using TACACS+ accounting method list. For the detailed information, please refer to accounting configuration.
- You shall use the defined authentication list in the specified line, or you use the list by default.

3.3.1 Configuring TACACS+ Protocol Parameter

You need to ensure that the network communication of TACACS+ server runs well before configuring TACACS+ on the network device. Use the following commands to configure TACACS+ protocol parameters:

Command	Function
configure terminal	Enter the global configuration mode.
aaa group server tacacs+ *group-name*	Configure TACACS+ group server, dividing different TACACS+ server into different groups.

server *ip-address*	Configure the server addresses in TACACS+ group server.
ip vrf forwarding *vrf-name*	Configure vrf name used in TACACS+ group server (this command exits on the device supporting VRF.)
tacacs-server host *ip-address* [**port** *integer*] [**timeout** *integer*] **key** [0 | 7] *string*	Configure IP address of remote TACACS+ security server; configures different parameters on this server by different parameter combination: ● *ip-address* :configures server address; ● **port** *intege* [optional] :determines the port used by the server; By default , the port number is 49 with the range from 1 to 65535. ● **timeout** *integer* [optional] :configures server timeout time; By default, the timeout time is 5s with the range from 1 to 1000s. ● **key** *string* [optional]:configures the key shared with the server of corresponding ip.
tacacs-server key [0 | 7] *string*	Configure the shared key used to communicate between the device and TACACS+ server. If the corresponding host does not set key by itself, you should set it globally.
tacacs-server timeout *seconds*	Specify the waiting time before the device resends request. By default, it is 5s. if the specified host does not set the specified timeout time, you should set the time globally.
tacacs-server directed-request [**restricted**] [**no-truncate**]	Configure the function of supporting the user specified authentication server. The default configuration is enabled.
Ip tacacs source-interface *interface*	Specify to send tacacs+ request to the source IP used by the server. By default, it does not specify.

Caution

You must configure TACACS+ Key before configuring TACACS+. The shared passwords on the network device and TACACS+ server must be consistent.

3.4 Using TACACS+ to Authenticate, Authorize and Account

In the typical TACACS+ network configuration figure, TACACS+ server authenticates, authorizes and accounts the access users. The following shows the examples of how to configure TACACS+ to authenticate, authorize and account by login authentication, authorization and accounting.

3.4.1 Using TACACS+ by Login Authentication

- Enables aaa first:

```
DES-7200# configure terminal

DES-7200(config)# aaa new-model
```

- Then configures tacacs+ server information:

```
DES-7200(config)# tacacs-server host 192.168.12.219

DES-7200(config)# tacacs-server key aaa
```

- Configures authentication method of using tacacs+:

```
DES-7200(config)# aaa authentication login test group tacacs+
```

- Applies the authentication method on the interface:

```
DES-7200(config)# line vty 0 4

DES-7200 (config-line)# login authentication test
```

Through the above configuration, you implement to configure login tacacs+ authentication. The configuration is shown as follows;

```
DES-7200#show running-config

!

aaa new-model

!

aaa authentication login test group tacacs+

!

tacacs-server host 192.168.12.219
```

```
tacacs-server key aaa

!

line con 0

line vty 0 4

login authentication test

!
```

3.4.2 Using TACACS+ by Enable Authentication

1. Enables aaa first:

```
DES-7200# configure terminal

DES-7200(config)# aaa new-model
```

2. Then configures tacacs+ server information:

```
DES-7200(config)# tacacs-server host 192.168.12.219

DES-7200(config)# tacacs-server host 192.168.12.218

DES-7200(config)# tacacs-server host 192.168.12.217

DES-7200(config)# tacacs-server key aaa
```

Configures tacacs+ server group using a part of the servers in the server list:

```
DES-7200(config)# aaa group server tacacs+ tacgroup1

DES-7200(config-gs-tacacs)# server 192.168.12.219

DES-7200(config-gs-tacacs)# server 192.168.12.218
```

3. Configures authentication method of using tacgroup1:

```
DES-7200(config)# aaa authentication enable default group tacgroup1
```

Through the above configuration, you implement to configure enable authentication of some tacacs+ servers. The configuration is shown as follows;

```
DES-7200#show running-config

!

aaa new-model

!

!

aaa group server tacacs+ tacgroup1
```

```
server 192.168.12.219

server 192.168.12.218

!

aaa authentication enable default group tacgroup1

!

!

tacacs-server host 192.168.12.219

tacacs-server host 192.168.12.218

tacacs-server host 192.168.12.217

tacacs-server key aaa

!

line con 0

line vty 0 4

!
```

3.4.3 Using TACACS+ by Login Authorization

1. Enables aaa first:

```
DES-7200# configure terminal

DES-7200(config)# aaa new-model
```

2. Then configures tacacs+ server information:

```
DES-7200(config)# tacacs-server host 192.168.12.219

DES-7200(config)# tacacs-server key aaa
```

3. Configures the authorization method of using tacacs+:

```
DES-7200(config)# aaa authorization exec test group tacacs+
```

4. Applies the authorization on the interface:

```
DES-7200(config)# line vty 0 4

DES-7200 (config-line)# authorization exec test
```

Through the above configuration, you implement to configure to use tacacs+ by login authorization. The configuration is shown as follows:

```
DES-7200#show running-config
```

```
!
aaa new-model
!
!
aaa authorization exec test group tacacs+
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
authorization exec test
!
```

3.4.4 Using TACACS+ by Level 15 Command Audit

- Enables aaa first:

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
```

- Then configures tacacs+ server information:

```
DES-7200(config)# tacacs-server host 192.168.12.219
DES-7200(config)# tacacs-server key aaa
```

- Configures command audit method of using tacacs+:

```
DES-7200(config)# aaa accounting commands 15 test start-stop group tacacs+
```

- Applies the authorization on the interface:

```
DES-7200(config)# line vty 0 4
DES-7200 (config-line)# accounting commands 15 test
```

Through the above configuration, you implement to configure enable authentication of some tacacs+ servers. The configuration is shown as follows;

```
DES-7200# show running-config
!
```

```
aaa new-model
!
!
aaa accounting commands 15 default group tacacs+
!
!
tacacs-server host 192.168.12.219
tacacs-server key aaa
!
line con 0
line vty 0 4
accounting commands 15 test
!
```

4 802.1x Configuration

This chapter describes the contents related to the AAA service configurations. The 802.1x is used to control the authentication over network access of users, and provide authorization and accounting functions for users.

This chapter includes:

- Overview
- Configuring 802.1x
- Viewing the Configuration and Current Statistics of the 802.1x
- Other Precautions for Configuring 802.1x

Note

For details about usage and descriptions of the CLI commands used in this section, please refer to *Configuring 802.1X command*.

4.1 Overview

In an IEEE 802 LAN, users can access the network device without authorization and authorization as long as they are connected to the network device. Therefore, an unauthorized user can access the network unobstructed by connecting the LAN. As the wide application of LAN technology , particularly the appearance of the operating network, it is necessary to address the safety authentication needs of the network. It has become the focus of concerns in the industry that how to provide user with the authentication on the legality of network or device access on the basis of simple and cheap Ethernet technologies. The IEEE 802.1x protocol is developed under such a context.

As a Port-Based Network Access Control standard, **the IEEE802.1x** provides LAN access point-to-point security access. Specially designed by the IEEE Standardization Commission to tackle the safety defects of Ethernet, this standard can provide a means to authenticate the devices and users connected to the LAN by utilizing the advantages of IEEE 802 LAN.

The IEEE 802.1x defines a mode based on Client-Server to restrict unauthorized users from accessing the network. Before a client can access the network, it must first pass the authentication of the authentication server.

Before the client passes the authentication, only the EAPOL (Extensible Authentication Protocol over LAN) packets can be transmitted over the network. After successful authentication, normal data streams can be transmitted over the network.

By using 802.1x, our switches provide Authentication, Authorization, and Accounting (AAA).

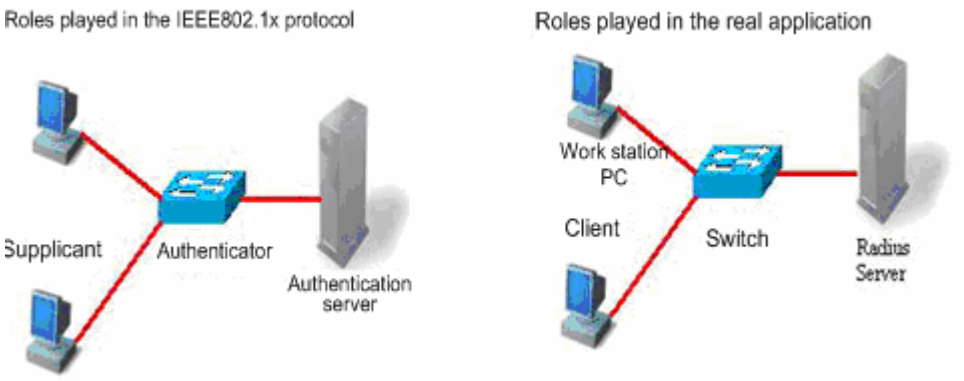
- Authentication: It is used to determine whether a user has the access, restricting illegal users.
- Authorization: It authorizes the services available to users, controlling the rights of valid users.
- Accounting: It records users' use of network resources, providing the supporting data for charging.

The 802.1x is described in the following aspects as below:

- Device Roles
- Authentication Initiation and Packet Interaction During Authentication
- States of Authorized Users and Unauthorized Users
- Topologies of Typical Applications

4.1.1 Device Roles

In the IEEE802.1x standard, there are three roles: **supplicant, authenticator, and authentication server.** In practice, they are the Client, network access server (NAS) and Radius-Server.



- Supplicant:

The **supplicant** is a role played by the end user, usually a PC. It requests for the access to network services and acknowledges the request packets from the authenticator. The supplicant must run the IEEE 802.1x client. Currently, the most popular one is the IEEE802.1x client carried by Windows XP. In addition, we have also launched the STAR Supplicant software compliant of this standard.

- Authenticator:

The **authenticator** is usually an access device like the switch. The responsibility of the device is to control the connection status between client and the network according to the current

authentication status of that client. Between the client and server, this device plays the role of a mediator, which requests the client for username, verifies the authentication information from the server, and forwards it to the client. Therefore, the switch acts as both the IEEE802.1x authenticator and the RADIUS Client, so it is referred to as the network access server (NAS). It encapsulates the acknowledgement received from the client into the RADIUS format packets and forwards them to the RADIUS Server, while resolving the information received from the RADIUS Server and forwards the information to the client.

The device acting as the authenticator has two types of ports: controlled Port and uncontrolled Port. The users connected to a controlled port can only access network resources after passing the authentication, while those connected to a uncontrolled port can directly access network resources without authentication. We can control users by simply connecting them to an controlled port. On the other hand, the uncontrolled port is used to connect the authentication server, for ensuring normal communication between the server and switch.

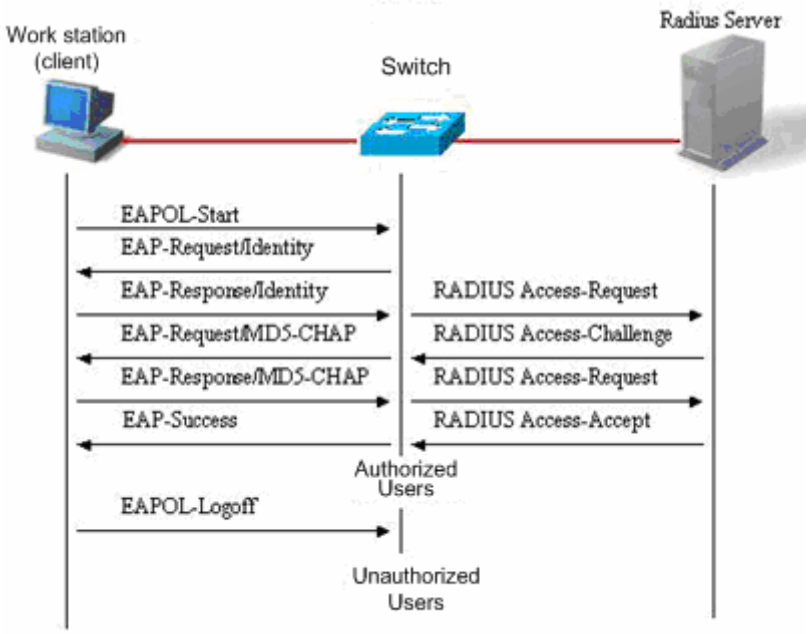
- Authentication server:

The **authentication server** is usually an **RADIUS** server, which works with the authenticator to provide users with authentication services. The authentication server saves the user name and password and related authorization information. One server can provide authentication services for multiple authenticators, thus allowing centralized management of users. The authentication server also manages the accounting data from the authenticator. Our 802.1x device is fully compatible with the standard Radius Server, for example, the Radius Server carried on Microsoft Win2000 Server and the Free Radius Server on Linux.

4.1.2 Authentication Initiation and Packet Interaction During Authentication

The supplicant and the authenticator exchange information by EAPOL protocol, while the authenticator and authentication server exchange information by RADIUS protocol, completing the authentication process with such a conversion. The EAPOL protocol is encapsulated on the MAC layer, with the type number of 0x888E. In addition, the standard has required for an MAC address (01-80-C2-00-00-03) for the protocol for packet exchange during the initial authentication process.

The following diagram shows a typical authentication process, during which the three role devices exchange packets with one another.



This is a typical authentication process initiated by users (in some special cases, the switch can actively initiate authentication request, whose process is the same as that shown in the diagram, except that it does not contain the step where the user actively initiates the request).

4.1.3 States of Authorized Users and Unauthorized Users

The 802.1x determines whether the users on the port are allowed to access the network according to the authentication status of the port. Since we expand the 802.1X based on users, we determine whether a user is allowed to access network resources according to the authentication status of that user under a port. All users under an uncontrolled port can use network resources, while those under a controlled port can access network resources only if they are authorized. When a user just initiates an authentication request, its status is unauthorized, in which case it cannot access the network. When the authentication is passed, its status changes to be authorized, in which case it can use the network resources.

If the workstation does not support 802.1x while the machine is connected with the controlled port, when the equipment requests the username of the user, the workstation will not respond to the request due to no support. This means that the user is still unauthorized and cannot access the network resources.

On the contrary, if the client supports 802.1x, while the connected switch does not: The EAPOL-START frames from the user are not responded, and the user deems it connected port as an uncontrolled port and directly uses network resources, when the user fails to receive any response after it sends the specified number of EAPOL-START frames.

On a 802.1x-enabled device, all ports are uncontrolled ports by default. We can set a port as a controlled port, to impose authentication over all the users under that port.

When a user has passed authentication (the switch has received success packets from the

RADIUS Server), the user is authorized and therefore can freely use network resources.If the user fails in the authentication and remains in the unauthenticated status, it is possible to initiate authentication once again. If the communication between the switch and the RADIUS server is faulty, the user is still unauthorized and therefore still cannot use the network.

When the user sends the EAPOL-LOGOFF packets, its status changes from authorized to unauthorized.

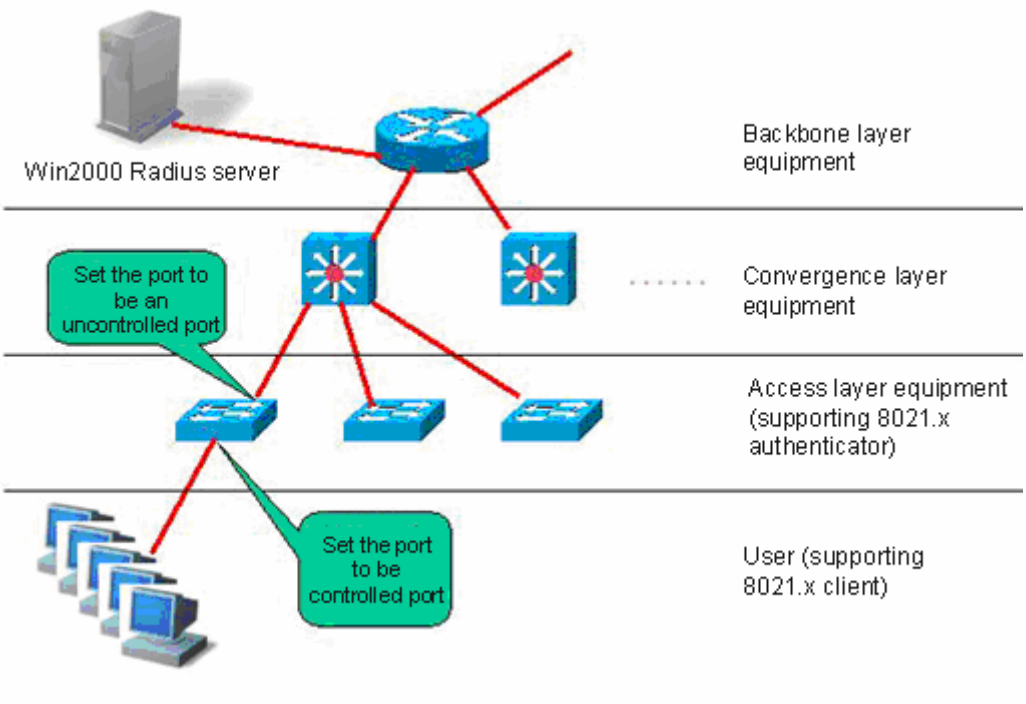
When a port of the switch changes to the LINK-DOWN status, all the users on the port change to the unauthorized status.

When the device restarts, all users on the device turn into the unauthorized status.

To force a user to pass the authentication, you can add a static MAC address.

4.1.4 Topologies of Typical Applications

A. The 802.1x-enabled device is used as the access layer device



This solution is described as below:

- Requirements of this solution:

The user supports 802.1x. That is, it is installed with the 802.1x client (Windows XP carried, Star-supplicant or other IEEE802.1x compliant client software).

The access layer device supports IEEE 802.1x.

One or multiple RADIUS compliant servers are available as the authentication server.

■ Key points for configuration of this solution:

The ports connected to the Radius Server and the uplink ports are configured as uncontrolled ports, so that the switch can normally communicate with the server and the authorized users can access network resources through the uplink interface.

The ports connected to the user must be set as controlled ports to control the accessed users, and the users cannot access network resources unless they first pass the authentication.

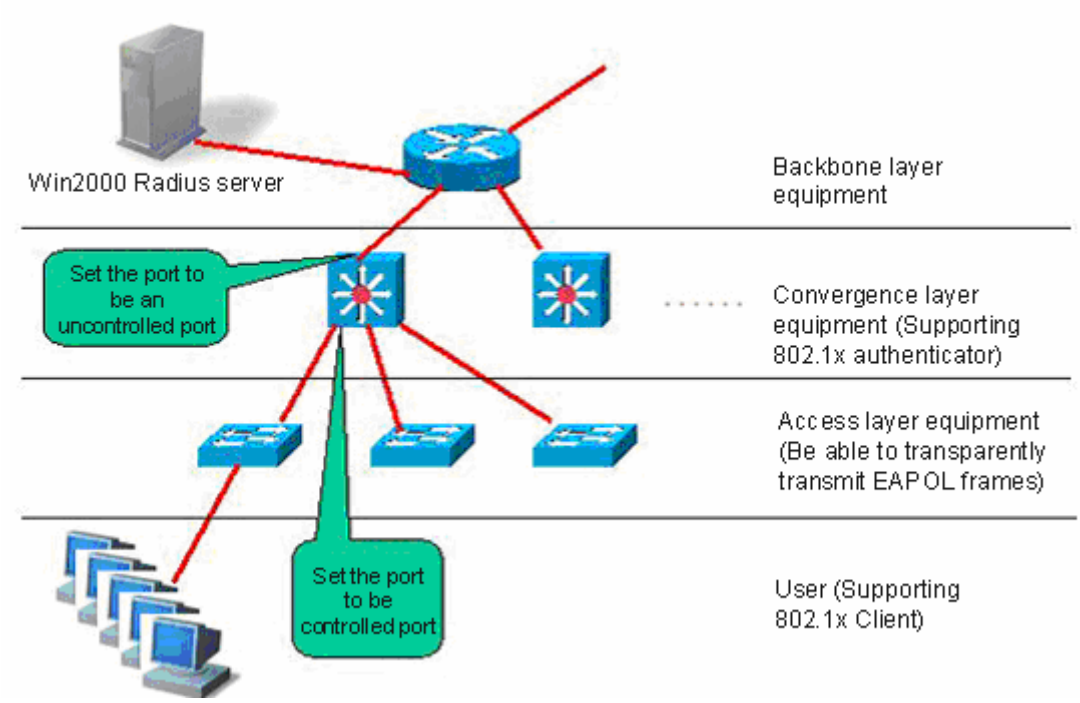
■ Characteristics of this solution:

Each 802.1x-enabled switch is responsible for a small number of clients, thus offering higher speed.The devices are mutually independent, and the restart operation of the device does not affect the users connected with other devices.

User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which switch a user is connected to, making management much easier.

The administrator can manage the device on the access layer through the network.

B. The 802.1x-enabled device is used as the convergence layer device



This solution is described as below:

■ Requirements of this solution:

1. The user supports 802.1x. That is, it is installed with the 802.1x client (Windows XP carried, Star-supplicant or other IEEE802.1x compliant client software).

2. The access layer device should be able to transparently transmit IEEE 802.1x. frames (EAPOL)
3. The convergence layer device supports 802.1x (playing the role of the authenticator)
4. One or multiple RADIUS compliant servers are available as the authentication server.

- Key points for configuration of this solution:

1. The ports connected to the Radius Server and the uplink ports are configured as uncontrolled ports, so that the switch can normally communicate with the server and the authorized users can access network resources through the uplink interface.
2. The ports connected to the access layer switches must be set as controlled ports to control the accessed users, and the users cannot access network resources unless they first pass the authentication.

- Characteristics of this solution:

1. The convergence layer device must be of high quality since the network is large and numerous users are connected, since any of its fault may cause the failures of many users to normally access the network.
2. User management is performed on the Radius Server in a centralized manner. The administrator does not have to know which switch a user is connected to, making management much easier.
3. The access layer device can be the less expensive non-NM switches (as long as they support transparent transmission of EAPOL frames).
4. The administrator cannot manage the device on the access layer through the network.

4.2 Configuring 802.1x

The following sections describe how to configure 802.1x.

- Default Configuration of 802.1x
- Precautions for Configuring 802.1x
- Configuring the communication between the device and Radius server
- Setting the 802.1X Authentication Switch
- Enabling/Disabling the Authentication of a Port
- Enabling Timed Re-authentication
- Enabling/Disabling the Filtering of Non-DES-7200 Supplicant
- Changing the QUIET Time

- Setting the Packet Retransmission Interval
- Setting the Maximum Number of Requests
- Setting the Maximum Number of Re-authentications
- Setting the Server-timeout
- Configuring the device to initiate the 802.1x authentication proactively
- Configuring 802.1x Accounting
- Configuring the IP authorization mode
- Releasing Advertisement
- List of Authenticable Hosts under a Port
- Authorization
- Configuring the Authentication Mode
- Configure the backup authentication server.
- Configuring and Managing Online Users
- Implementing User-IP Binding
- Port-based Traffic Charging
- Implementing Automatic Switching and Control of VLAN
- Implementing GUEST VLAN
- Shielding Proxy Server and Dial-up
- Configuring On-line Client Probe
- Configuring the Option Flag for EAPOL Frames to Carry TAG
- Configuring Port-based User Authentication
- Configuring Port-based Single User Authentication
- Configuring Dynamic ACL Assignment
- Configuring Dot1x MAC Bypass Authentication
- Configuring Dot1x MAC Bypass Authentication Timeout
- Configuring Dot1x MAC Bypass Authentication Violation
- Configuring Dot1x Auth-Fail VLAN
- Configuring Dot1x Auth-Fail Max-Attempt

4.2.1 Default Configuration of 802.1x

The following table lists some defaults of the 802.1x

Item	Default
Authentication	DISABLE
Accounting	DISABLE
Radius Server *ServerIp *Authentication UDP port *Key	*No default *1812 *No default
Accounting Server *ServerIp *Accounting UDP port	*No default *1813
All port types	Uncontrolled port (all ports can perform communication directly without authentication)
Timed re-authentication	Off
Timed reauth_period	3,600 seconds
Interval between two authentication requests	10 seconds
Retransmission interval	3 seconds
Maximum retransmissions	3
Client timeout period	3 seconds, if within which no response is received from the client, the communication is deemed as a failure
Server timeout period	5 seconds, if within which no response is received from the server, the communication is deemed as a failure
Lists of authenticable hosts under a port	No default

4.2.2 Precautions for Configuring 802.1x

- You can perform the following configuration only to the products that support 802.1x.
- The 802.1x can run on both L2 device and L3 device.
- It is required to configure the IP address of the authentication server before the Radius-server authentication mode can operate normally.
- You cannot enable 1X authentication on the 802.1Q TUNNEL port.

- You cannot enable 1X authentication for Aggregate Port.
- If the 1x function is enabled on only one port of a switch, all the port will send the 1x protocol packets to the CPU.

4.2.3 Configuring the communication between the device and Radius server

The Radius Server maintains the information of all users: user name, password, authorization information and accounting information. All users are managed on the Radius Server in a centralized manner, without being distributed over various switches, making easier management for the administrator.

In order for the switch to normally communicate with the RADIUS SERVER, you must set the following parameters:

Radius Server end: You must register a Radius Client. At registration, you must supply the Radius Server switch's IP address, authentication UDP port (add the accounting UDP port, if needed), and the agreed key for communication between the switch and Radius Server, and select EAP support for the Client. The procedure for registering one Radius Client on the Radius Server varies with different software settings. Please refer to the appropriate document.

Device end: The following settings are necessary at the device end to ensure the communication between the device and the server: Configure the IP address of the Radius Server, authentication (accounting) UDP port and the agreed password for the communication with the server.

In the privileged mode, you can set the communication between the switch and the Radius Server via the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
Radius-server key *string*	Configure RADIUS Key.
End	Return to the privileged mode.
Write	Save the configuration.
Show radius server	Show the RADIUS server.

You can use the **no radius-server host** *ip-address* **auth-port** command to restore the authentication UDP port of the Radius Server to its default. You can use the **no radius-server key** command to delete the authentication key of the Radius Server. The following example

sets the Server IP as 192.168.4.12, authentication UDP port as 600, and the key as agreed password:

```
DES-7200# configure terminal
DES-7200(config)# radius-server host 192.168.4.12
DES-7200(config)# radius-server host 192.168.4.12 auth-port 600
DES-7200(config)# radius-server key MsdadShaAdasdj878dajL6g6ga
DES-7200(config)# end
```

- The officially agreed authentication UDP port is 1812.
- The officially agreed accounting UDP port is 1813.
- No less than 16 characters are recommended for the agreed password between the device and the Radius Server.
- The port of the device to connect the Radius Server shall be configured as uncontrolled port.

4.2.4 Setting the 802.1X Authentication Switch

When the 802.1x authentication is enabled, the switch will impose authentication over the host connected to the controlled port, and the hosts that fail the authentication are not allowed to access the network.

In the privileged mode, you can enable the 1x authentication by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
radius-server host *ip-address* [**auth-port** *port*] [**acct-port** *port*]	Configure the RADIUS server
Radius-server key string	Configure RADIUS Key.
aaa authentication dot1x *auth* **group radius**	Configure the dot1x authentication method list
dot1x authentication *auth*	dot1x applies authentication method list
End	Return to the privileged mode.
Write	Save the configuration.
Show running-config	Show the configuration.

The following example enables 802.1x authentication:

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# radius-server host 192.168.217.64
```

```
DES-7200(config)# radius-server key starnet
DES-7200(config)# aaa authentication dot1x authen group radius
DES-7200(config)# dot1x authentication authen
DES-7200(config)# end
DES-7200# show running-config
!
aaa new-model
!
aaa authentication dot1x authen group radius
!
username DES-7200 password 0 starnet
!
radius-server host 192.168.217.64
radius-server key 7 072d172e071c2211
!
!
!
dot1x authentication authen
!
interface VLAN 1
 ip address 192.168.217.222 255.255.255.0
 no shutdown
!
!
line con 0
line vty 0 4
!
end
```

To apply the RADIUS authentication method in the 802.1x, configure the IP address of the Radius Server and make sure normal communication between the device and the Radius Server. Without the coordination of the Radius Server, the switch cannot perform authentication. For how to set the communication between the Radius Server and the switch, please see the previous section.

4.2.5 Enabling/Disabling the Authentication of a Port

If you enable authentication for a port when the 802.1x is enabled, the port becomes a controlled port, and the users under the port must first pass authentication before they can access the network. However, the users under the uncontrolled port can directly access the network.

In the privileged mode, you can set authentication for a port by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface*	Enter the interface configuration mode and specify the Interface to configure.

Command	Function
dot1x port-control auto	Set the port to be a controlled port (enable interface authentication). You can use the no option of the command to disable the authentication of the interface.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x port-control	View the authentication configuration of the 802.1x interface.

You can use the **no dot1x port-control** command to disable the authentication of the interface. The following example sets Ethernet interface 1/1 to be a controlled interface:

```
DES-7200# configure terminal
DES-7200(config)# interface f 1/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config)# end
```

When a port is set as a controlled port, only the EAP packets are allowed to pass; the packets to the CPU are also under control.

Caution

If you hope that cpu can not receive non-EAP packet from any controlled port, you can separate management VLAN from user VLAN.

4.2.6 Enabling Timed Re-authentication

The 802.1x can ask users for re-authentication at periodical intervals, to prevent authorized users from being used by other users. This can also detect disconnection, making more accurate charging. In addition to the re-authentication switch, you can also define the re-authentication interval, which is 3600 seconds by default. In the case of charging based on duration, you should determine the re-authentication interval according to the specific network size, which should be sufficient while as accurate as possible.

In the privileged mode, you can enable/disable re-authentication and set the re-authentication interval by performing the following steps.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x re-authentication	Enable timed re-authentication.
dot1x timeout re-authperiod *seconds*	Set the re-authentication interval.
end	Return to the privileged mode.

Command	Function
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x re-authentication** command to disable timed re-authentication, and use the **no dot1x timeout re-authperiod** command to restore the re-authentication interval to the default.

The following example enables re-authentication and sets the re-authentication interval as 1000 seconds.

```
DES-7200# configure terminal
DES-7200(config)# dot1x re-authentication
DES-7200(config)# dot1x timeout re-authperiod 1000
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:          Disabled
Authentication Mode:    EAP-MD5
Authed User Number:     0
Re-authen Enabled:      Enabled
Re-authen Period:       1000 sec
Quiet Timer Period:     10 sec
Tx Timer Period:        3 sec
Supplicant Timeout:     3 sec
Server Timeout:         5 sec
Re-authen Max:          3 times
Maximum Request:        3 times
Client Online Probe:    Disabled
Eapol Tag Enable:       Disabled
Authorization Mode:     Disabled
```

If re-authentication is enabled, please pay attention to the reasonableness of the re-authentication interval, which must be set according to the specific network size.

4.2.7 Enabling/Disabling the Filtering of Non-DES-7200 Supplicant

When the DES-7200 supplicant product is used as the 802.1x authentication client, authentication may fail if you use some other 802.1x authentication clients at the same time (for example, Windows XP 802.1x authentication function is enabled).

In this case, you can enable this function to filter the 802.1x packets from non-DES-7200 supplicants so that supplicant authentication is not affected by other 802.1x clients. The function is enabled by default.

In the privileged mode, you can enable/disable the filtering by performing the following steps:

Command	Function

Command	Function
configure terminal	Enter the global configuration mode.
dot1x private-supplicant-only	Enable the filtering function.
End	Return to the privileged mode.
Write	Save the configuration.
show dot1x	Show the dot1x configurations.

Following example is the configuration to enable the supplicant function provided by us.

```
DES-7200# configure terminal
DES-7200(config)# dot1x private-supplicant-only
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:              enable
Authentication Mode:        eap-md5
Total User Number:          0(exclude dynamic user)
Authed User Number:         0(exclude dynamic user)
Dynamic User Number:        0
Re-authen Enabled:          enable
Re-authen Period:           2 sec
Quiet Timer Period:         10 sec
Tx Timer Period:            3 sec
Supplicant Timeout:         3 sec
Server Timeout:             5 sec
Re-authen Max:              3 times
Maximum Request:            3 times
Private supplicant only:    enable
Client Online Probe:        disable
Eapol Tag Enable:           disable
Authorization Mode:         disable
```

Use the **no dot1x private-supplicant-only** command to disable this function.

4.2.8 Changing the QUIET Time

When the user authentication fails, the switch does not allow that user to re-authenticate until a specified period, which is referred to as Quiet Period.This value functions to protect the device from malicious attacks. The default interval for Quiet Period is 5 seconds.

A shorter Quiet Period may speed up re-authentication for the users.

In the privileged mode, you can set the Quiet Period by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout quiet-period seconds	Set the Quiet Period.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x timeout quiet-period command to** restore the Quiet Period to its default. In the example below the QuietPeriod value is set as 500 seconds:

```
DES-7200# configure terminal
DES-7200 (config)# dot1x timeout quiet-period 500
DES-7200(config)# end
```

4.2.9 Setting the Packet Retransmission Interval

After the device sends the EAP-request/identity, it resends that message if no response is received from the user within a certain period. By default, this value is 3 seconds. You should modify this value to suit the specific network size.

In the privileged mode, you can set the packet retransmission interval by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout tx-period *seconds*	Setting the Packet Retransmission Interval
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x timeout tx-period** to restore the packet re-transmission interval to its default. The following example sets the packet retransmission interval as 100 seconds:

```
DES-7200# configure terminal
DES-7200(config)# dot1x timeout tx-period 100
DES-7200(config)# end
```

4.2.10 Setting the Maximum Number of Requests

If the switch does not receive response within the ServerTimeout after it sends an authentication request to the RadiusServer, it will retransmit the packets.The maximum number of requests are the maximum retransmission requests of the device, and the authentication fails if this number is exceeded. By default, this value is 3. You should modify this value to suit the specific network size.

In the privileged mode, you can set the maximum number of retransmissions by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x max-req *count*	Set the maximum number of packet re-transmissions.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

```
DES-7200#show dot1x
```

You can use the **no dot1x max-req** command to restore the maximum number of packet re-transmissions to its default. The following example sets the maximum number of packet retransmissions to 5:

```
DES-7200# configure terminal
DES-7200(config)# dot1x max-req 5
DES-7200(config)# end
```

4.2.11 Setting the Maximum Number of Re-authentications

When the user authentication fails, the device attempts to perform authentication for the user once again. When the number of attempts exceeds the maximum number of authentications, the switch believes that this user is already disconnected, and ends the authentication process accordingly. By default, the number is 3. However, you can modify this value.

In the privileged mode, you can set the maximum number of re-authentications by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x reauth-max *count*	Setting the Maximum Number of Re-authentications

Command	Function
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

You can use the **no dot1x reauth-max** command to restore the maximum number of re-authentications to its default. The following example sets the maximum number of re-authentications to 3:

```
DES-7200# configure terminal
DES-7200(config)# dot1x reauth-max 3
DES-7200(config)# end
```

4.2.12 Setting the Server-timeout

This value indicates the maximum response time of the Radius Server. If the switch does not receive the response from the Radius Server within this period, it deems the authentication as a failure.

In the privileged mode, you can set the Server-timeout and restore it to its default by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x timeout server-timeout *seconds*	Set the maximum response time of the Radius Server. You can use the no option of the command to restore it to its default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

4.2.13 Configuring the device to initiate the 802.1x authentication proactively

The 802.1x is secure access authentication based on port. Users must first undergo authentication before they can access the network. In most cases, authentication is initiated by the user end through EAPOL-START packets. For the information about packet interaction during the authentication process, please see “Authentication Initiation and Packet Interaction During Authentication”.

However, authentication needs to be initiated by the switch in some cases. For example, when the switch is reset and the status of the authentication port changes from linkdown to linkup, the switch needs to automatically initiate authentication to ensure that the authenticated users

can continue to use the network. In addition, if you use a 802.1x client that does not actively initiate authentication requests (for example, the Windows XP 802.1x client), the switch should be able to actively initiate authentication. The switch forcedly asks all the users under the authentication port to authenticate by sending the EAP-request/identity multicast packets.

The following section describes how to configure the switch to actively initiate 802.1x authentication and how you should configure appropriately in different application environments.

Turn on/off the switch for the proactive authentication initiation of the device

When this function is disabled, the switch can only initiate an authentication request at resetting or when the status of the authentication port is changed. This ensures that the on-line users can continue to use the network. The switch will not actively initiate an authentication request in any other cases. When this function is enabled, you can configure the times of automatic authentication initiation, authentication request interval, and whether to stop sending requests when the users pass the authentication.

In the privileged mode, you can enable automatic authentication by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req	Enable automatic authentication. It is disabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the dot1x configurations.

The **no** option of the command turns off the function. Only when the function is enabled, the following settings take effect. The user can set the number of proactive authentication requests initiated by the device, which can be determined according to the actual network environment.

In the privileged mode, you can set the number of automatic authentication requests by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req packet-num *num*	The device proactively initiates num 802.1x authentication request messages. If num is equal to 0, the device will continually send that message. The default is 0 (infinite).
end	Return to the privileged mode.
write	Save the configuration.

Command	Function
show dot1x auto-req	Show the configuration.

The **no** option of the command restores the value to its default. The following contents introduce how to configure the message sending interval.

In the privileged mode, you can set the packet sending interval by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req req-interval *interval*	Setting the Packet Sending Interval
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command restores the value to its default. Since sending the authentication request multicast message will cause re-authentication for all users under the authentication interface, the sending interval shall not be too small lest the authentication efficiency is affected.

It is possible to set whether to stop sending the request messages when the user authentication passes. In some applications (only one user under a port, for example), we can stop sending authentication requests to the related port when the device finds the user authentication passes. If the user gets offline, the request is sent continually.

In the privileged mode, you can set this function by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auto-req user-detect	Stop sending the messages when there is some authentication user under the port. This function is enabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auto-req	Show the configuration.

The **no** option of the command disables the function. Before setting this function, take careful considerations on the current network application environment.

The above three commands provide you with flexible application strategies. You can select the appropriate configuration command according to the specific network application environment. To help you configure easily, the following configuration table is provided for your reference:

	Solution 1	Solution 2	Solution 3

	Solution 1	Solution 2	Solution 3
User environment	One port for any user	One port for one user	One port for multiple users
Whether the DES-7200 supplicant should be used as the authentication client	Yes	No	No
Configuration command recommended	Not necessary to enable the dot1x auto-req function	**dot1x auto-req** **dot1x auto-req packet-num** *num* **dot1x auto-req req-interval** *interval* **dot1x auto-req user-detect**	**dot1x auto-req** **dot1x auto-req packet-num** *0* **dot1x auto-req req-interval** *interval* **no dot1x auto-req user-detect**

4.2.14 Configuring 802.1x Accounting

Our 802.1x has implemented the accounting function. Accounting is based on interval. In other words, the 802.1x records the length of the period between the first successful authentication of the user and the user's logoff or when the switch detects user disconnection.

After the first successful user authentication, the switch sends an accounting start request to the server. When the user gets off-line or the switch finds that the user has got off line or when the physical connection of the user is broken, the switch sends an accounting end request to the server. The server group records this information in the database of the server group. Based on such information, the NMS can provide the basis for accounting.

Our 802.1x stresses the reliability of accounting, and it specially supports the backup accounting server to avoid failures of the accounting server. When a server can no longer provide the accounting service due to various reasons, the switch will automatically forward the accounting information to another backup server. This greatly improves the reliability of accounting.

When a user exits by itself, the accounting duration is accurate. When the connection of the user is broken by accident, the accounting accuracy depends on the re-authentication interval (the switch detects the disconnection of a user by using the re-authentication mechanism).

To enable the accounting function of the device, the following settings are necessary on the device:

1. On the Radius Server, register the switch as a Radius Client, like the authentication operation.
2. Set the IP address of the accounting server.
3. Set the accounting UDP port.
4. Enable the accounting service on the precondition that the 802.1x has been enabled.

In the privileged mode, you can set the accounting service by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa group server radius gs	Configure the accounting server group.
server *192.168.4.12* **acct-port** *11*	Add a server to the server group.
exit	Return to the global configuration mode.
aaa accounting network *acct* **start-stop group** *gs*	Configure the accounting method list.
dot1x accounting *acct*	Apply the accounting method list for the 802.1X.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

The **no aaa accounting network** command deletes the accounting method list. The **no dot1x accounting** command restores the default dot1x accounting method. The following example sets the IP address of the accounting server to 192.1.1.1, that of the backup accounting server to 192.1.1.2, and the UDP port of the accounting server to 1200, and enables 802.1x accounting:

```
DES-7200# configure terminal
DES-7200(config)# aaa new-model
DES-7200(config)# aaa group server radius acct-use
DES-7200(config-gs-radius)# server 192.168.4.12 acct-port 1200
DES-7200(config-gs-radius)# server 192.168.4.13 acct-port 1200
DES-7200(config-gs-radius)# exit
DES-7200(config)# aaa accounting network acct-list start-stop group acct-use
DES-7200(config)# dot1x accounting acct-list
DES-7200(config)# end
DES-7200# write memory
DES-7200# show running-config
```

Caution

1. The agreed accounting key must be the same as that of the Radius Server and authentication.
2. The accounting function cannot be enabled unless the AAA is enabled.
3. The accounting is impossible unless the 802.1X authentication passes.
4. By default, the accounting function of the 802.1x is disabled.
5. For the database format of accounting, see the related Radius Server documentation.

Also, the account update is supported. After the account update interval is set on the NAS device, the NAS device will send account update packets to the Radius Server at periodical intervals. On the Radius Server, you can define the number of periods before which the account update packet of a user is not received from the NAS device, the NAS or user will be regarded as off-line. Then, the Radius Server can stop the accounting of the user, and delete the user from the on-line user table.

In the privileged mode, you can set the account update function by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa accounting update	Set the account update function.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

You can disable the account update service by using the **no aaa accounting update** command.

```
DES-7200# configure terminal
DES-7200(config)# aaa accounting update
DES-7200(config)# end
DES-7200# write memory
DES-7200# show running-config
```

The following chapters introduce the propriety features of DES-7200's network products:

To make it easy for broadband operators and to accommodate use in special environments, our 802.1x has been expanded on the basis of the account (such expansion is completely based on the standard, and has totally compatible with IEEE 802.1x).

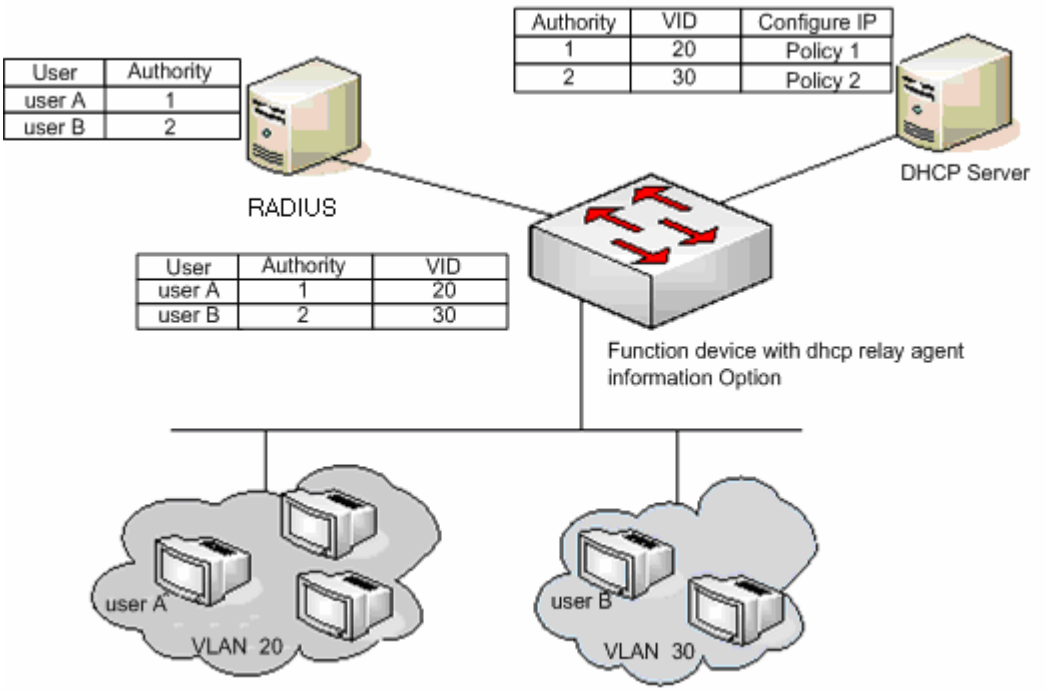
4.2.15 Configuring the IP authorization mode

The 802.1x implemented by DES-7200 can force the authenticated users to use fixed IP. By configuring the IP authorization mode, the administrator can limit the way the user gets IP address. There are four IP authorization modes: DISABLE, DHCP SERVER, RADIUS

SERVER and SUPPLICANT. They are detailed below respectively:

DISABLE mode (default): The device has no limitation for the user IP, and the user only needs to pass the authentication to be able to access the network.

DHCP SERVER mode: The user IP is obtained via specified DHCP SERVER, and only the IP allocated by the specified DHCP SERVER is considered legal. For the DHCP mode, it is possible to use DHCP relay option82 to implement a more flexible IP allocation policy with the 802.1X. Here is a typical diagram for the plan:



The user initiates IP requests via the DHCP Client. The network device with dhcp relay option82 converges the user authority on the RADIUS server to construct the option82 field and encapsulate it in the DHCP request message. That option82 field consists of “vid + permission”. The DHCP Server chooses different allocation policies by using the option82 field.

In this mode, it is required to configure the DHCP Relay and the related option82. If the DHCP relay function is enabled and the option82 policy is selected, see the DHCP Relay Configuration Guide and Command References for the configurations.

RADIUS SERVER mode: The user IP is specified by the RADIUS SERVER. The user can only use the IP specified by the RADIUS SERVER to be able to access the network.

SUPPLICANT mode: The IP bound to the user is the IP of the PC during the SUPPLICANT’s authentication. After the authentication, the user can only use that IP to be able to access the network.

The application models in the four modes are as follows:

- DISABLE mode: Suitable for the environment with no limits for the users. The user can access the network once he/she passes the authentication.
- DHCP SERVER mode: The user PC gets the IP address via DHCP. The administrator configures the DHCP RELAY of the device to limit the DHCP SERVER that the users can access. In this way, only the IPs allocated by the specified DHCP SERVER are legal.
- RADIUS SERVER mode: The user PC uses fixed IP. The RADIUS SERVER is configured with <user-IP> mapping relations that are notified to the device via the Framed-IP-Address attributes of the device. The user has to use that IP to be able to access the network.
- SUPPLICANT mode: The user PC uses fixed IP. The SUPPLICANT notifies the information to the device. The user has to use the IP at authentication to be able to access the network.

Caution When the user switches modes, it will cause all authenticated users to get offline. So, it is recommended to configure the authentication mode before the use.

In the privileged mode, configure the IP authorization mode as follows:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function
aaa authorization ip-auth-mode {disabled | dhcp-server | radius-server | supplicant }	Configure the IP authorization mode
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

The example below configures the IP authorization mode as the RADIUS-SERVER mode:

```
DES-7200# configure terminal
DES-7200(config)# aaa authorization ip-auth-mode radius-server
DES-7200(config)# end
DES-7200# show running-config
!
aaa new-model
!
aaa authorization ip-auth-mode radius-server
!
DES-7200# write memory
```

4.2.16 Releasing Advertisement

Our 802.1x allows you to configure the Reply-Message field on the Radius Server. When

authentication succeeds, the information of the field is shown on our 802.1x client of Star-Supplicant, by which the operators can release some information.

Such information is shown at the first user authorization, but not at re-authentication. This avoids frequently disturbing the user.

The window for showing the advertisement information supports html, which converts the http://XXX.XXX.XX in the message into links capable of direct switching, for easier browsing.

Releasing of the advertising information:

1) The operator configures the Reply Message attribute on the Radius Server end.
2) Only our Star-supplicant client supports such information (free for the users of our switch), while other clients cannot see the information, which however does not affect their normal use.
3) No setting is required at the device end.

4.2.17 List of Authenticable Hosts under a Port

For enhanced security of the 802.1x, we have made expansion without affecting the IEEE 802.1x, allowing the NM to restrict the list of hosts authenticated of a port. If the list of hosts authenticated of a port is empty, any user can be authenticated. If the list is not empty, only the hosts in the list can be authenticated. The hosts that can be authenticated are identified by using the MAC addresses.

The following example adds/deletes the hosts that can be authenticated under a port.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-address-table address *mac-addr* **interface** *interface*	Set the list of the hosts that can be authenticated.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

Caution

If the list of the host is empty, the port allows any host to be authenticated.

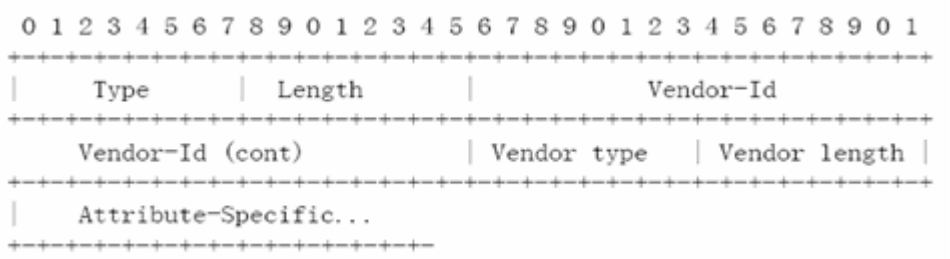
4.2.18 Authorization

To make it easier for operators, our products can provide services of different qualities for

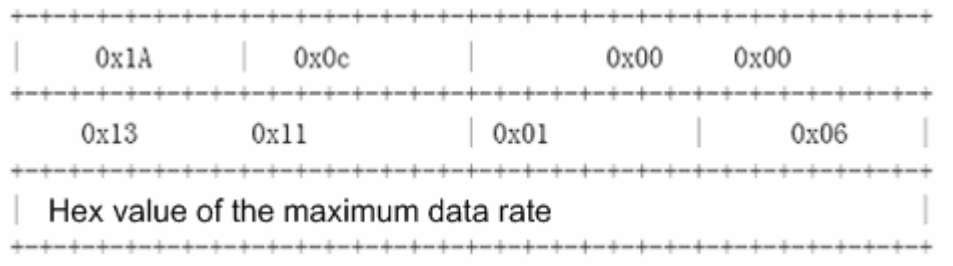
different types of services, for example, offering different maximum bandwidths. Such information is all stored on the Radius Server, and the administrator does not need to configure every switch.

Since the Radius has no standard attribute to represent the maximum data rate, we can only transfer the authorization information by the manufacturer customized attribute.

The general format of the definition is as follows:

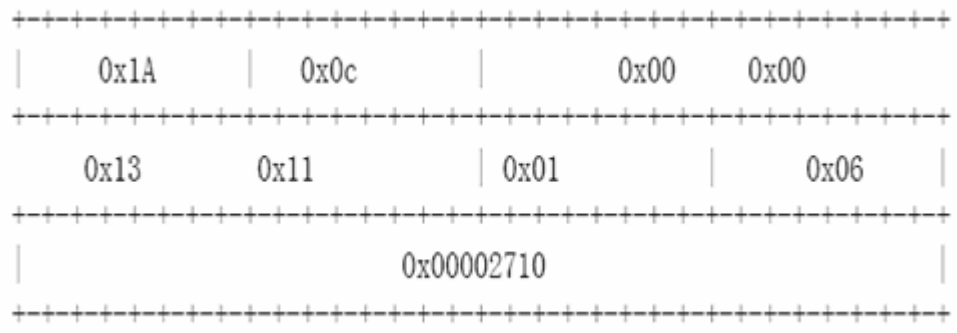


For the maximum data rate, you need to fill in the following values:



The unit of the maximum data rate is kbps.

For users with the maximum data rate of 10M, you need to fill in the following values:



For the customized header, follow those provided above. The maximum data rate is 10M, that is, 10000kbsp, and makes 0x00002710 in the Hex system. You only need to fill in the corresponding field.

This function calls for no settings on the device end, and works as long as the device end supports authorization.

4.2.19 Configuring the Authentication Mode

In the standard, the 802.1x implements authentication through the EAP-MD5. The 802.1X designed by DES-7200 can perform authentication through both the EAP-MD5 (default) mode and the CHAP and PAP mode. The advantage of the CHAP is that it reduces the communication between the switch and the RADIUS SERVER, thus alleviating the pressure on the RADIUS SERVER. Same as the CHAP mode, the communication between the PAP and RADIUS SERVER occurs only once. Although the PAP mode is not recommended for its poor security, it can meet the special needs of the user in some cases. For example, when the security server used only supports the PAP authentication mode, this mode can be selected to fully exploit the existing resources, protecting the existing investment.

In the privileged mode, you can set the authentication mode of the 802.1x by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-mode mode	Configure the authentication mode
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

The following example configures the authentication mode to the CHAP mode:

```
DES-7200# configure terminal
DES-7200(config)# dot1x auth-mode CHAP
DES-7200(config)# end
DES-7200# show dot1x
802.1X Status:        Disabled
Authentication Mode:  CHAP
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Group Server
```

4.2.20 Configure the backup authentication server.

Our 802.1x-based authentication system can support the backup server.When the master

server is down due to various reasons, the device automatically issues a server submission authentication request to the method list server group.

In the privileged mode, you can set the backup authentication server by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Turn on the AAA switch.
aaa group server radius *gs-name*	Configure the server group.
server sever	Configure the server.
server server-backup	Configure the backup server.
End	Return to the privileged mode.
Write	Save the configuration.
show dot1x	Show the configuration.

The following example configures 192.168.4.12 to be the backup server:

```
DES-7200# configure terminal
DES-7200# aaa new-model
DES-7200(config)# aaa group server radius auth-ll
DES-7200(config-gs-radius)# server 192.168.4.1
DES-7200(config-gs-radius)# server 192.168.4.12
DES-7200(config-gs-radius)# end
DES-7200#
```

4.2.21 Configuring and Managing Online Users

DES-7200's devices provide management for authenticated users via SNMP. The administrator can view the information of the authorized users via SNMP, and forcedly log off a user. The user forcedly logged off must pass the authentication again before it can use network resources.

This function calls for no configuration on the device.

4.2.22 Implementing User-IP Binding

With our clients and by correctly configuring the Radius Server, you can implement unique user-IP binding. A user must undergo authentication by using the IP address allocated by the administrator. Otherwise, authentication will fail.

For this function, you do not need to configure the switch. The user needs to use our client and the administrator needs to configure the Radius Server.

4.2.23 Port-based Traffic Charging

In addition to the duration-based billing, DES-7200's network devices provide the traffic-based billing function in case each port of the equipment has only one user access.

This function calls for no configuration on the device but need the support of the Radius server.

4.2.24 Implementing Automatic Switching and Control of VLAN

To implement the auto-switching of the dynamic VLAN, the user VLAN shall be assigned and configured by the remote RADIUS server. The remote RADIUS server encapsulates the VLAN assignment information through the defined RADIUS attributes. After receiving those information and the user authentication, the access device automatically adds the port where the user is to the VLAN assigned by the RADIUS server. It is unnecessary of the manual configurations for the administrator.

You shall use the **show dot1x summary** command to on the access device to view the actual VLAN where the user is. Use the **show dot1x user id** command to view the VLAN assigned by the RADIUS server.

The access device is able to receive the VLAN assigned by the RADIUS server in two ways of the extension RADIUS attributes and the standard RADIUS attributes.

The RADIUS server assigns the VLAN to the access device using the standard-extension attributes. The server encapsulates the extension attributes into the No.26 RADIUS standard attributes. The extension manufacturing ID is in hex 0x00001311. By default, the extension attribute type is 4, you can use the **radius attribute 4 vendor-type** *type* command to set the extension attribute type number to assign the VLAN. For the configuration command, see *RADIUS Configuration*.

The access device supports the RADIUS server to use the standard RADIUS attributes to assign the VLAN, including the following attribute combinations:

No.64 Attribute Tunnel-Type

No.65 Attribute Tunnel-Medium-Type

No.81 Attribute Tunnel-Private-Group-ID

And for the auto-switching of the dynamic VLAN application, the valid range is:

Tunnel-Type=VLAN(13)

Tunnel-Medium-Type=802(6)

Tunnel-Private-Group-ID=VLAN ID or VLAN Name

For the details, see the RFC2868 and the RFC3580.

The processing steps of receiving the assigned VLAN for the access device are: 1. use the assigned VLAN attribute as the VLAN name and view that whether there is the same VLAN name on the access device; 2. if there is the same VLAN name, the port where the user is swithes to the VLAN automatically; if there is no same VLAN name, then the assigned VLAN attribute will be used as the VLAn ID; 3. if the VLAN ID is valid(within the VLAN ID range of the system supported), the port where the user is auto-switches to this VLAN; if the VLAN ID is 0, no VLAN assignment information exist; 4. except for those conditions mentioned above, the user authentication is faulty.

Only the ACCESS port and the TRUNK port are supported by the access device for the 802.1x authentication. In other port modes, it fails to enable the auto-switching function of the dynamic VLAN. The following describes the conditions of the VLAN auto-switching function on the ACCESS and TRUNK ports:

VLAN auto-switching function on the ACCESS port

Without the assigned VLAN configured on the device, if the assigned VLAN is identified as the VLAN ID by the device, the device will create the VLAN with the corresponding VLAN ID and switch the auth-port to the newly- created VLAN; while if the assigned VLAN is identified as the VLAN name by the device, the user authentication will be faulty.

With the assigned VLAN configured on the device, if the assigned VLAN is set as the VLAN not supporting the auto-switching on the ACCESS port, the user authentication will be faulty; while if the assigned VLAN is set as the VLAN supporting the auto-switching on the ACCESS port, the user authentication and the auto-switching implementation of the assigned VLAN will be successful.

The following lists the VLANs not supporting the auto-switching on the ACCESS port:

Private VLAN

Remote VLAN

Super VLAN

Native VLAN configuration on the TRUNK port

For the TRUNK port with the authentication enabled, set the assigned VLAN as the Native VLAN for the port to be authenticated.

With the assigned VLAN configured on the device, if the assigned VLAN is identified as the VLAN ID by the device, the Native VLAN for the port to be authenticated will be set as the assigned VLAN; while if the assigned VLAN is identified as the VLAN name by the device, the user authentication will be faulty.

With the settings of the assigned VLAN configured on the device, if the assigned VLAN is set as the VLAN not supporting the auto-switching on the TRUNK port, the user authentication will be faulty; while if the assigned VLAN is set as the VLAN supporting the auto-switching on the TRUNK port, the user authentication will be successful and the Native VLAN for the port to be authenticated will be set as the assigned VLAN.

The following lists the VLANs not supporting the auto-switching on the TRUNK port:

Private VLAN

Remote VLAN

Super VLAN

To enable the dynamic VLAN auto-switching function on an interface, run the following commands:

1) enable the AAA function

Command	Function
configure terminal	Enter the global configuration mode.
aaa new-model	Enable the AAA function

For the details, see *AAA Configuration*.

2) set the RADIUS server

Command	Function
configure terminal	Enter the global configuration mode.
radius-server host *host-ip*	Configure the RADIUS server.
radius-server key *text*	Configure the RADIUS server shared key.

For the details, see *RADIUS Configuration*.

3) enable the methhod list

Command	Function
configure terminal	Enter the global configuration mode.
aaa authentication dot1x *list1* **group radius**	Configure the authentication method list1.
aaa accounting network *list2* **start-stop group radius**	Configure the accouting method list2.

For the details, see *AAA Configuration*.

4) 802.1x method list

Command	Function
configure terminal	Enter the global configuration mode.
dot1x authentication *list1*	Select the authentication method list1.
dot1x accounting *list2*	Select the accounting method list2.

5) enable the 802.1x authentication on the interface

Command	Function

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface_id*	Enter the interface configuration mode.
dot1x port-control auto	Enable the 802.1x authentication on the interface.

6) enable the VLAN auto-switching on the interface

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface_id*	Enter the interface configuration mode.
dot1x dynamic-vlan enable	Enable the VLAN auto-switching on the interface.

Caution

For the VLAN auto-switching function, the dynamic switching must be enabled on the interface. That is, use the dot1x dynamic-vlan enable command in the interface configuration mode. Or the RADIUS attributes of the encapsulted assigned VLAN will be ignored.

In the interface configuration mode, the **dot1x dynamic-vlan enable** command must be configured after the **dot1x port-control auto** command has been configured. With the **dot1x port-control auto** command configured, the VLAN auto-switching function is disabled.

The private vlan does not support the dynamic VLAN switching function. That is, the private vlan cannot be set as the 802.x dynamic vlan.

7) view the dynamic VLAN auto-switching settings

Command	Function
show dot1x user id *session_id*	View the user information in *session-id,* including the dynamic VLAN auto-switching information.
show dot1x summary	View the actual VLAN where the user is.

For the related precautions, see the chapter of *Other Precautions of 802.1x Configuration*.

4.2.25 Implementing GUEST VLAN Function

If **guest vlan** is set on the switch, then when the port sends the authentication requests of certain quantity proactively but receives no corresponding reply or **eapol** packet, you can add the port to **guest vlan.** Use **show runninng-config** to view the configuration and **show vlan** to check whether the port jumps to guest vlan or not .

Follow these steps to configure a port to allow **GUEST VLAN** jump or not:

Command	Function
configure terminal	Enter the global configuration mode.
interface *interface*	Enter the interface configuration mode.
dot1x dynamic-vlan enable	Allow Vlan jump on the interface.
[**no**] **dot1x guest-vlan** *vid*	Configure whether to enable guest vlan, which is disabled by default.
end	Return to the privileged mode.
write	Save the configuration.
show running-config	Show the configuration.

Caution

1. **Guest vlan** takes effect unless you configure **dot1x dynamic-vlan enable.**
2. It is better not to configure L2 attributes when configuring **guest vlan**, especially not to set **vlan** on the port manually.
3. Exiting **guest vlan** when there is **eapol** packet on the port and the port is **linkdown.** If you configure **guest vlan,** it will check **guest vlan** exchange conditions again when the port is **linkup.**
4. Enabling **guest vlan** on Trunk port causes the users in other vlan on this port access the network without 802.1x authentication. To this end, it is recommeded that **guest vlan** shall be enabled on the Access port.
5. **Guest vlan** does not support the private vlan. That is to say, you can not set the private vlan as the dot1x guest vlan.

4.2.26 Shielding Proxy Server and Dial-up

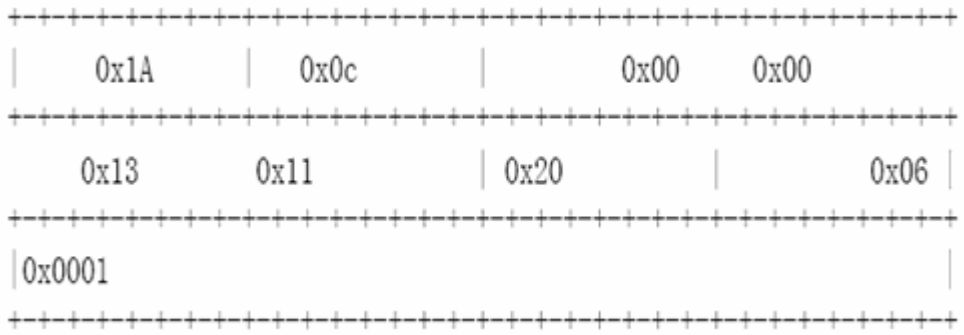
The two major potential threats to network security are: The user sets its own proxy server and the user makes dial-up to access the network after authentication. Star switches provide the function to shield proxy servers and dial-up connections.

To implement this function needs no settings on the device end and needs only the corresponding attributes configured on the Radius server end. Since the Radius has no standard attributes to indicate the maximum data rate, we can transfer the authorization information only through the manufacturer custom attributes. For the general format defined, see the Authorization section.

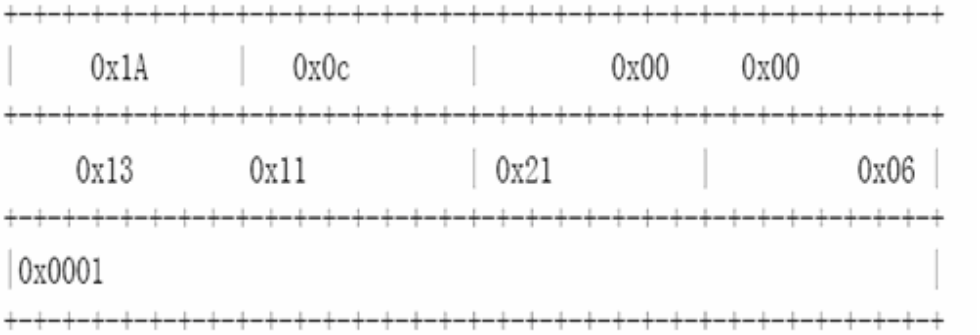
The proxy server shielding function defines the Vendor type of 0x20, and the dial-up shielding function defines the Vendor type of 0x21.

The Attribute-Specific field is a 4-byte manufacturer defined attribute, which defines the actions taken against proxy server access and dial-up access. 0x0000 means normal connection, without shielding detection. 0x0001 means shielding detection.

To shield the access via the proxy server, you should fill in the following information:



To shield the access via the dial-up connection, you should fill in the following information:



4.2.27 Configuring On-line Probe on Client End

To ensure accurate charging, an on-line probe mechanism is needed to detect whether a user is on-line within a short period. The re-authentication mechanism specified in the standard can meet such needs, but it needs the participation of the RADIUS server. Accurate user probe will occupy enormous resources of the switch and RADIUS server. To meet the need to implement accurate charging with few resources occupied, we use a new client on-line probe mechanism. Such mechanism only needs interaction between the switch and client and occupies little network traffic, and it implements minute-level charging accuracy (you can set the charging accuracy).

Caution

To implement on-line client monitoring, the client software must support this function.

The following two timers affect the performance and accuracy of on-line probe:

- Hello Interval: It is the interval at which the client sends advertisement.
- Alive Interval: Client online interval. If the device has not received the client advertisement during this interval, it actively disconnects the client and notifies the billing server. The interval must be greater than the Hello Interval.

In the privileged mode, you can configure the on-line probe function of the client by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
Dot1x client-probe enable	Enable the on-line probe function of the client
Dot1x probe-timer interval *interval*	Configure the Hello Interval
Dot1x probe-timer alive interval	Configure the Alive Interval of the device.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

4.2.28 Configuring the Option Flag for EAPOL Frames to Carry TAG

In accordance with IEEE 802.1x, the EAPOL packets cannot be added with vlan TAG. However, based on the possible application requirements, the selection flag is provided. When the flag is turned on, tags can be outputted according to the related output rule of the trunk ports.

The typical application environment is to enable 802.1x authentication on the convergence layer. For more information, see “Topologies of Typical Applications”.

In the privileged mode, you can configure the flag for EAPOL frames to carry TAG by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x eapol-tag	Enable the flag for EAPOL frames to carry TAG. By default, the function is disabled.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x	Show the configuration.

You can disable this function by using the **no dot1x eapol-tag** command.

4.2.29 Configuring Port-based Authentication

The 802.1x controls users on the basis of their MAC addresses by default. Only the authenticated user can use the network. With port-based authentication, the port is authenticated as long as a user is authenticated on a port. Consequently, all users connecting to this port can access the network.

To configure port-based control mode, execute the following commands in the privileged mode.

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface mode
dot1x port-control auto	Enable the function being controlled.
dot1x port-control-mode {*mac-based*|*port-based*}	Select the controlled mode.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x port-control	Show the configuration of port 802.1X.

You can run **no dot1x port-control-mode** to restore the settings to the default control mode.

Following example shows how to configure the authentication mode of a port.

```
DES-7200(config)#
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 4/5
DES-7200(config-if)# dot1x port-control-mode port-base
```

Caution

In the port-based authentication mode, a port can be connected with only one authenticated user.

Port-based authentication mode can enable or disable dynamic users to migrate among multiple authenticated ports. By default, the migration is allowed. To prohibit the migration, run the following commands one by one in the privileged mode.

Command	Function
configure terminal	Enter the global configuration mode.
dot1x stationarity enable	Disable the migration among ports.
end	Exit to the privileged mode.
write	Save the configuration.

4.2.30 Configuring Port-based Single-user Authentication

By default, 802.1x controls on the basis of user MAC. Only the authenticated users can use the network, while other users connected to the same port is not able to use the network. In the port-based control mode, the port is authenticated when there is an authenticated user on the port. All the users connected to the authenticated port are able to use the network normally.

However, in the port-based control mode, the port-based single-user authentication controls only one authenticated user. The port is authenticated when it allows only one authenticated user who is enable to use the network normally. Then, if you find other users on the port, you should clear all the users on the port and reauthenticate.

From the privileged mode, follow the steps below to configure port-based single-user control mode on the port.

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface configuration mode.
dot1x port-control auto	Enable control function.
dot1x port-control-mode port-based single-host	Port-based single-user control mode.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x port-control	Show 802.1x configuration.
show running-config	Show all configurations.

You can run no dot1x port-control-mode to restore the settings to the default control mode.

Following example shows how to configure the authentication mode of a port.

```
DES-7200(config)#
DES-7200#configure terminal
DES-7200(config)#interface <interface-id>
DES-7200(config-if)#dot1x port-control-mode port-base single-host
```

In the port-based authentiction mode, every port only can receive one authentication user.

Caution

Single-host is port-based single-user 802.1x access control. Use **show dot1x port-control** to display port-based and use **show running-config** to display dot1x port-control-mode port-based single-host.

Since single-host only supports the single-user form, setting default-user-limit on the port manually does not take effect in single-host mode. If you set default-user-limit on the port after setting single-host, only one user can be permitted to use the network still.

In the port-based authentication mode, you can permit or deny dynamic users to migrate among multiple authentication ports, which is permitted by default. If you want to deny the migration of dynamic users, follow the steps below from the privileged mode.

Command	Function
configure terminal	Enters the global configuration mode.
dot1x stationarity enable	Prohibits migration between ports.
End	Returns to the privileged mode.
Write	Saves the configuration.

4.2.31 Configuring Dynamic Acl Assignment

802.1x supports ACL assignment from server and dynamic installation of the assigned ACL. Our product support installing acl by default. They will install acl dynamically on condition that the allowed acl is set on the server and is assigned after the successful user authentication.

To implement dynamic acl assignment, you need to set the port as mac-based authentication mode or port-based single-user authentication mode. The ACL assignment is not supported in the port-based multi-user authentication mode. For the configuration, please refer to the related command configuration manual.

In single-host authentication mode, it supports to renew acl when reauthenticating. That is, acl takes effect when the authenticated user sets acl on the server and reauthenticates.

The mac-based authentication mode does not support ACL update when re-authenticating. That is to say, ACL of the authenticated user can only be assigned once. The new acl is ignored and the original acl remains if the acl changes when re-authenticating.

Caution

Supported acl type: extension type which can explain acl function on our switch.

Execute the following command if you need to support dynamic acl assignment on the server which is not authenticated by our company.

```
DES-7200#configure terminal
DES-7200(config)# radius vendor-specific extend
```

4.2.32 Configuring Dot1x MAC Authentication Bypass

GUEST VLAN provides a method of network accessing without the 802.1x authentication client, but this technology is unable to determine whether the access device is secure or insecure. In some conditions, for the network management and security, although there is no 802.1x authentication client, the administrator still needs to control the validity of the access device. MAB(MAC Authentication Bypass) provides a solution for this application.

With the MAB function enabled on the 802.1x authentication port, the authentication request packets are sent continuously to the port and the client response is expected. If there is no client response within the time of “tx-period*reauth-max”, the MAC address learned on the 802.1x authentication port will be monitored, and the authentication will be initiated by sending the username(the learned MAC address) and keyword to the server. It determines whether the learned MAC address is accessible to the network or not according to the returned authentication result from the server.

To configure the MAB function, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface configuration mode.
dot1x mac-auth-bypass	Set the dot1x MAC authentication bypass.
end	Return to the privileged mode.
Write	Save the configurations.
show running-config	Show all configurations.

Following example shows how to configure the MAB function.

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config-if)# dot1x mac-auth-bypass
```

- Use the format XXXXXXXXXXXX when setting the username and keyword for the MAC address on the server.
- With the port in the MAB mode, only one MAC address that firstly found by the device can be used for the authentication.
- One port for one MAC address authentication is supported in both the port mode and the MAC mode.
- Anytime when the client responses the 802.1x authentication, the MAB on the port takes no effect unless the link state down/up change occurs or the 802.1x function on the port is re-enabled.
- The client online probe function takes no effect for the MAC authentication in the MAB mode.
- With MAB port configured, an authentication request packet is sent at the interval of tx-period. After sending the packets for reauth-max times, if there is no client response, the port enters to the MAB mode. The port in the MAB mode can learn the MAC address and use the learned MAC address as the username for the authentication.
- MAB supports the PAP, CHAP, EAP-MD5 authentication methods. For how to configure the authentication method, see the chapter in *Authentication Method Configuration*.

Caution

- In the MAB mode, after the MAC address authentication failure, if the guest vlan has been configured, the authentication port will enter the guest vlan; if the guest vlan has not been configured, the port stays in the original vlan. The MAB does not support auth-fail VLAN, that is, even though the MAB authentication fails and the auth-fail VLAN has been configured, the port will not enter the auth-fail VLAN.
- If one MAC address has passed the MAB authentication for one port and it appears on other ports, the MAB violation will be set for the latter port.
- MAB cannot be co-used with the security channel.
- The MAB authentication is invalid for the static address and the filtering address.
- The MAB authentication offers the access-auth service for the device without the auth-client software. Those devices generally cannot recognize the 802.1Q TAG labels. To this end, it is recommended that the MAB-auth functon shall be set on the ACCESS port. Otherwise, even though it passes the authentication, the communication between the devices fails.

4.2.33 Configuring Dot1x MAC Authentication Bypass Timeout

After a MAC address authentication in the MAB mode is online, this MAC address will always be online unless the re-auth fails, the port is Down or it is forcibly offline due to the administration policy.

The user can configure the allowed online time of those authentication MAC address. 0 is the default value, indicating that the MAC address is always online.

To configure the MAB timeout, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface configuration mode.
dot1x mac-auth-bypass timeout-activity <value>	Set the MAB timeout time, in seconds. No default value and the valid range is 1-65535.
end	Return to the privileged mode.
write	Save the configurations.
show running-config	Show all configurations.

Following example shows how to configure the MAB timeout time.

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x mac-auth-bypass  timeout-activity 3600
```

Caution

- If the online time for the MAC address authentication is also assigned by the server, this online time is independent from the timeout-activity.
- After it times out, with guest vlan configured on the port, the port switches to the guest vlan. However, during the authentication, the response timeout for the server will not cause the MAB port in the guest vlan.

4.2.34 Configuring Dot1x MAC Authentication Bypass Violation

By default, with one MAC address authenticated in the MAB mode, data of all devices under the port are allowed to be forwarded. However, in some safe applications, if only one MAC address is allowed for the MAB port by the administrator, configure the MAB violation. With the MAB violation configured, once the port enters the MAB mode, the violation occurs if there is more than one 1 Mac address for the port.

To configure the MAB violation on the interface, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface configuration mode.
dot1x mac-auth-bypass violation	Set the MAB violation.
end	Return to the privileged mode.
Write	Save the configurations.
show running-config	Show all configurations.

Following example shows how to configure the MAB violation.

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x mac-auth-bypass violation
```

Caution

- Use the **erridisable recover** command to restore the MAB violation port.
- The same MAC address for the port in the private vlan appears in the primary and the secondary VLAN simultaneously, so the MAB authentication violation shall not be configured on the port in the private vlan. Or it will lead to the MAB violation judgement error and influence the normal use.

4.2.35 Configuring Dot1x Auth-Fail VLAN

With the auth-fail vlan configured on the switch, when the user authentication on the port fails, the port enters to the auth-fail vlan pre-configured,

To configure the auth-fail VLAN in the interface configuration mode, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
interface <*interface-id*>	Enter the interface configuration mode.
dot1x auth-fail vlan <*vid*>	Set the auth-fail VLAN on the interface.
end	Return to the privileged mode.
Write	Save the configurations.
show running-config	Show all configurations.

Following example shows how to configure the auth-fail VLAN.

```
DES-7200# configure terminal
```

```
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x auth-fail vlan 2
```

Caution

- If the configured vlan is inexistent, the vlan will be created dynamically when the port enters the auth-fail vlan, and will be auto-removed when the port exits from the auth-fail vlan.
- If the port is down, it will exit from the auth-fail vlan automatically.
- It allows setting the auth-fail vlan and the guest vlan in the same VLAN.
- In the port mode and in the auth-fail vlan, it only allows the last-auth-fail user for the re-auth, and the auth-requests of other users are dropped. This restriction is not applicable for the MAC mode.
- The auth-fail vlan does not support private vlan. That is, the private vlan cannot be set as the dot1x auth-fail vlan.

4.2.36 Configuring Dot1x Auth-Fail Max-Attempt

To configure the auth-fail max-attempt times, run the following commands:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-fail max-attemp<*value*>	Set the auth-fail max-attempt times, the default value is 3 and the valid range is 1-3.
end	Return to the privileged mode.
Write	Save the configurations.
show running-config	Show all configurations.

Following example shows how to configure the auth-fail max-attempt value.

```
DES-7200# configure terminal
DES-7200(config)# dot1x auth-fail max-attempt 2
```

4.2.37 Configuring Inaccessible Authentication Bypass

When all RADIUS servers configured on the switch are inaccessible, the user's authentication request won't receive any reply, and the administrator won't be able to verify user's identity. From the perspective of user, if no other authentication method is configured on the switch, it won't be able to access the network. To ensure that the new authenticated user can access network, Inaccessible Authentication Bypass (IAB) can be configured on the port.

Execute the following steps to enable IAB:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **interface** <*interface-id*>	Enter interface configuration mode.
DES-7200(config-if)# **dot1x critical**	Configure Inaccessible Authentication Bypass.
DES-7200(config-if)# **end**	Return to privileged mode.
DES-7200# **show running-config**	Display all configurations.

The following example shows how to configure Inaccessible Authentication Bypass:

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config-if)# dot1x critical
```

Note

After IAB is enabled on the port and all servers become inaccessible:

1. IAB will take effect only if the globally configured 802.1x authentication method list contains only RADIUS authentication method and all RADIUS servers have failed. If there are other authentication methods in the list (such as local, none, etc), IAB won't take effect.
2. After globally enabling AAA multi-domain authentication, the globally configured authentication method list won't be adopted during 802.1x user authentication. Since IAB will directly allow the user to pass authentication without the need to enter username after the RADIUS servers in 802.1x authentication method list have all failed, AAA multi-domain authentication will fail on this port.
3. IAB-authorized users won't send accounting request to the accounting server.
4. Normally authenticated users won't be affected and can still access network.
5. When enabling the 802.1x IP authorization, if authenticated user on the port exists, the other user on this port cannot be authenticated through IAB.
6. With GSN address binding function enabled on the port, the user authenticated through the IAB cannot access the network.

4.2.38 Configuring IAB Authentication with Switching VLAN

When 802.1x controlled port enters into IAB state, it won't be able to verify user's identity. You can assign this port to a specific VLAN, and only allow the user to access network resources on this specific VLAN.

Execute the following steps to configure IAB authentication with switching VLAN:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **interface** <*interface-id*>	Enter interface configuration mode.
DES-7200(config-if)# **dot1x critical vlan** <*vlan-id*>	Configure IAB authentication with switching VLAN.
DES-7200(config-if)# **end**	Return to privileged mode.
DES-7200# **show running-config**	Display all configurations.

The following example shows how to configure Inaccessible Authentication Bypass:

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config-if)# dot1x critical
DES-7200(config-if)# dot1x critical vlan 100
```

Note

1. If there are already certain authenticated users on the port before all RADIUS servers fail, new users are authorized to access the network after servers have failed and if no inaccessible VLAN is configured on the port. If IAB authentication with inaccessible VLAN has been configured on the server, new users won't be authorized to access network in order to guarantee that the authenticated users have the priority to use network.
2. If there are already normally authenticated users on the port before all servers have failed, the port will remain the original state and won't jump to the inaccessible VLAN if the servers are failed during user's re-authentication.
3. After all users under the port are disconnected, the port will automatically exit from the inaccessible VLAN.
4. If the inaccessible VLAN configured doesn't exist, the inaccessible VLAN will be created automatically when entered by the port and be removed automatically when exited by the port.
5. The inaccessible VLAN doesn't support private VLAN, remote VLAN and super VLAN (including SUB VLAN).

4.2.39 Configuring IAB Authentication with Recovery action.

When RADIUS server is failed, some users won't be able to pass the authentication, and the switch will authorize the users to access network. When RADIUS server is recovered, this feature will allow IAB users under the port to reinitialize authentication to verify user's identity.

Execute the following steps to configure IAB authentication with recovery action:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **interface** <*interface-id*>	Enter interface configuration mode.
DES-7200(config-if)# **dot1x critical recovery action reinitialize**	Allow IAB users under the port to reinitialize authentication when the server has recovered.
DES-7200(config-if)# **end**	Return to privilege mode.
DES-7200# **show running-config**	Display all configurations.

The following example shows how to configure Inaccessible Authentication Bypass:

```
DES-7200# configure terminal
DES-7200(config)# interface fa 0/1
DES-7200(config-if)# dot1x port-control auto
DES-7200(config-if)# dot1x critical
DES-7200(config-if)# dot1x critical recovery action reinitialize
```

Note After the server has recovered, normally authenticated users under the port can continue to access the network without re-authentication. After the server is failed, users authorized to access network through IAB authentication will be subject to the re-authentication initiated by the switch.

4.3 Viewing the Configuration and Current Statistics of the 802.1x

Our 802.1X provides a full range of state machine information, which is very useful for network management and can be used by the administrator to monitor user status in real time and make easy troubleshooting.

- Viewing the Radius Authentication and Accounting Configuration
- Viewing the Number of Current Users

- Viewing the List of the Addresses Authenticable
- Viewing the User Authentication Status Information
- Showing the 1x Client Probe Time Configuration

4.3.1 Viewing the Radius Authentication and Accounting Configuration

Run the **show radius server** command to check the related configuration of the Radius Sever, and run the **show aaa user** command to view the user-related information.

```
DES-7200# sh radius server
Server IP:       192.168.5.11
Accounting Port: 1813
Authen  Port:    1812
Server State:    Ready
```

4.3.2 Viewing the Number of Current Users

Our 802.1X allows you to view the numbers of two types of users: one is the number of current users, and the other is that of the authorized users. The number of current users refers to the total number of users authenticated (whether successfully or unsuccessfully), while the number of authorized users means the total number of users authorized.

In the privileged mode, run the **show dot1x** command to check the current number of users and authenticated users, 1x configuration, including the current number of users and authenticated users.

The following example shows the 802.1x configuration:

```
DES-7200# show dot1x
802.1X Status:        Disabled
Authentication Mode:  EAP-MD5
Authed User Number:   0
Re-authen Enabled:    Disabled
Re-authen Period:     3600 sec
Quiet Timer Period:   10 sec
Tx Timer Period:      3 sec
Supplicant Timeout:   3 sec
Server Timeout:       5 sec
Re-authen Max:        3 times
Maximum Request:      3 times
Client Oline Probe:   Disabled
Eapol Tag Enable:     Disabled
Authorization Mode:   Disabled
```

4.3.3 Viewing the Authenticable Address Table

Our 802.1x has expanded functions that allow you to set the hosts that can be authenticated on a particular port. This function allows the administrator to view the currently available settings.

In the privileged mode, you can view the list of hosts authenticable by performing the following steps:

Command	Function
configure terminal	Enter the global configuration mode.
dot1x auth-address-table address *mac-addr* **interface** *interface*	Set the list of the hosts that can be authenticated.
end	Return to the privileged mode.
write	Save the configuration.
show dot1x auth-address-table	Show the list of the hosts that can be authenticated.

Use the **no dot1x auth-address-table address** command to delete the specified authenticable host list. The following example shows the list of the hosts that can be authenticated.

```
DES-7200# show dot1x auth-address-table
interface:g3/1
-----------------------------------
mac addr: 00D0.F800.0001
```

4.3.4 Viewing the User Authentication Status Information

The administrator can view the authentication status of the current users of the switch for easier troubleshooting.

In the privileged mode, you can view the user authentication status information by performing the following steps:

Command	Function
show dot1x summary	Viewing the User Authentication Status Information

The following example shows the user authentication status information.

```
DES-7200# show dot1x summary
 ID   MAC       Interface  VLAN  Auth-State  Backend-State Port-Status

---- ----------- --------- ----  ----------  ------------   -----------
1   00d0f8000001 Gi3/1     1   Authenticated  IDLE       Authed
```

4.3.5 Showing the 1x Client Probe Timer Configuration

In the privileged mode, you can view the 1x timer setting by performing the following steps:

Command	Function
show dot1x probe-timer	Show the 1X timer setting

The following example shows the 1.1x timer setting:

```
DES-7200# show dot1x probe-timer
Hello Interval: 20 Seconds
Hello Alive: 250 Seconds
DES-7200#
```

4.3.6 Example of Configuring 802.1X port-based dynamic VLAN assignment

In a school, there are three types of user groups as shown below:

- Students;
- Trusted students (such as student cadres);
- Teaching and administrative staff.

Fundamental requirements are shown below:

- Each member of these three user groups can be connected to any port of the access device and join the corresponding VLAN.
- Complete data isolation shall be achieved between VLANs corresponding to three user groups, namely the members of one group cannot exchange data with members of another group.

Network topology is shown below:

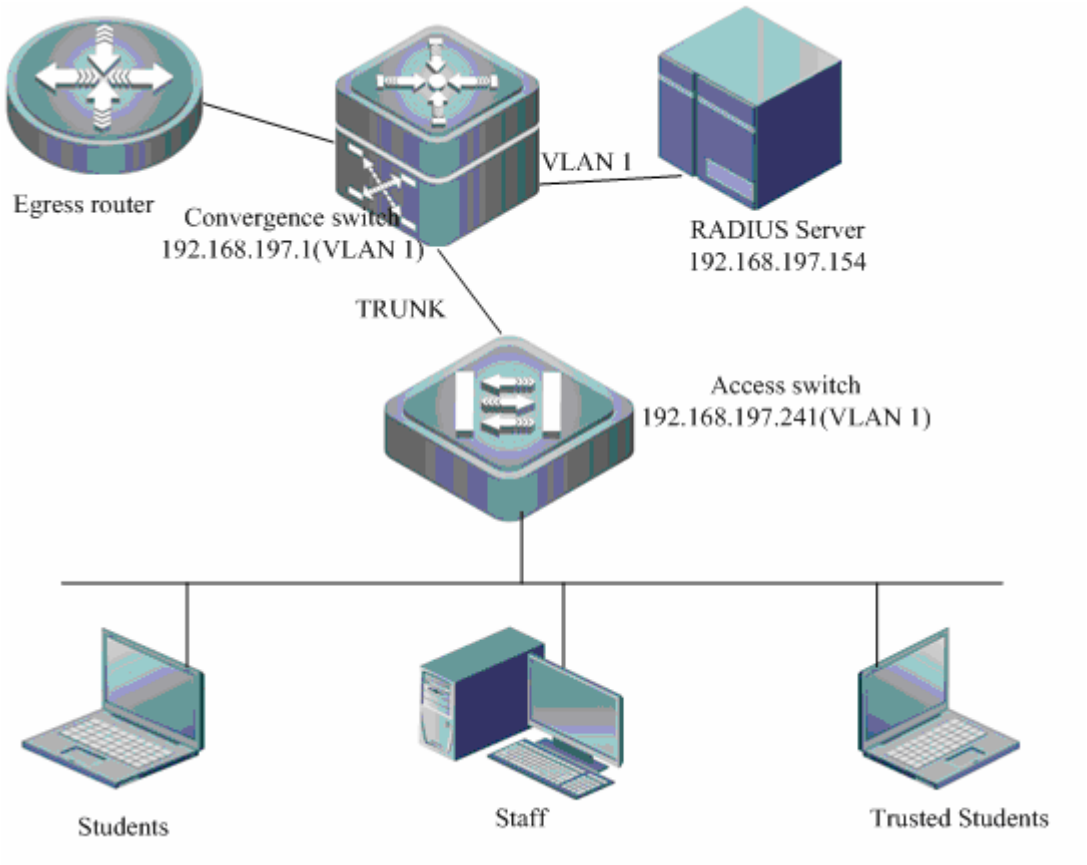


Figure 11 Typical topology of dynamic VLAN assignment

Configuration example is shown below

1. Configure RADIUS server

Include a managerial access device of 192.168.197.241, which uses the default authentication and accounting ports of 1812 and 1813 and the shared key of "shared".

Configure the vlan for users of user group "students"

```
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-ID = "students"
Configure the vlan for users of user group "trusted_students"
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-ID = "trusted_students"
Configure the vlan for users of user group "staff"
Tunnel-Type = "VLAN",
Tunnel-Medium-Type = "IEEE-802",
Tunnel-Private-Group-ID = "staff"
```

2. Configure access switch

Turn on AAA switch

```
configure terminal
aaa new-model
```

Configure RADIUS server

```
configure terminal
radius-server host 192.168.197.154
radius-server key shared
```

Configure authentication method list

```
configure terminal
aaa authentication dot1x default group radius
aaa accounting network default start-stop group radius
```

802.1X to select the authentication method list

```
configure terminal
dot1x authentication default
dot1x accounting default
```

Enable 802.1X authentication on the interface

```
configure terminal
interface range fastEthernet 0/1-48
dot1x port-control auto
```

Enable dynamic VLAN assignment on the interface

```
configure terminal
interface interface_id
dot1x dynamic-vlan enable
```

Create VLANs to join after user authentication

```
configure terminal
```

vlan 2

```
name students
```

vlan 3

```
name trusted_students
```

vlan 4

```
name staff
```

Create the management IP for access device

```
configure terminal
interface vlan 1
ip address 192.168.197.241 255.255.255.0
```

By far, user's needs can be met.

4.4 Other Precautions for Configuring 802.1x

1. Concurrent use of 1X and ACL

In the non-IP authorization mode, if you enable the 802.1x authentication function of a port and at the same time associate one ACL with a interface, the ACL takes effect on the basis of the MAC address. In other words, only the packets from the source MAC addresses of the authenticated users can pass ACL filtering, and the packets from other source MAC addresses

will be discarded. The ACL can only work on the basis of the MAC address.

For example, if the authenticated MAC address is 00d0.f800.0001, then all the packets from the source MAC address of 00d0.f800.0001 can be switched. If the port is associated with an ACL, the ACL will further filter these packets that can be switched, for example, rejecting the ICMP packets from the source MAC address of 00d0.f800.0001.

2. The restrictions for the condition that the users on the interface have being authenticated or the users have been authenticated:

■ The port mode cannot be modified, such as the command **switchport mode trunk** cannot be used.

■ The port Access VLAN can not be modified in the ACCESS mode.

■ The port Allowed VLAN and Native VLAN can not be modified in the TRUNK mode.

■ The port can not exit from or be added to the AP port.

3. The restrictions for the condition that the users in the VLAN have being authenticated or the users have been authenticated:

✧ VLAN can not be deleted

✧ VLAN type cannot be modified, such as the command **private-vlan primary** cannot be used.

4. The restrictions for the condition of multiple user-auth under the same auth-port.

✧ The first user does not assign the VLAN and assign the default VLAN.

✧ The consequent auth-users don't assign VLAN and use the first user to assign the VLAN.

✧ The VLAN assigned consequently must be consistent with the one assigned by the first user; or it fails for the authentication.

✧ The VLAN assigned after the 1st user re-auth must be the same as the one passed the last-auth; or it fails for the authentication.

5. GVRP cannot be co-used with the dynamic VLAN auto-switching function.

6. The VLAN-switching function switches the whole port to another VLAN for the communication after the 802.1x authentication, so the most applicable network topology is that one single user is connected with the ACCESS port. If it is a TRUNK port, although it is configurable, the actual authentication fails. To this end, the VLAN switching function cannot be configured on the TRUNK port.

7. 802.1x function can be co-used with other access control functions, such as the port security, IP+MAC binding,ect. When those access control functions are co-used, the packets can enter the switch on the condition that those packets must address all access controls.

4.5 Typical 802.1X Configuration Examples

4.5.1 802.1X-based AAA Services

4.5.1.1 Network Topology

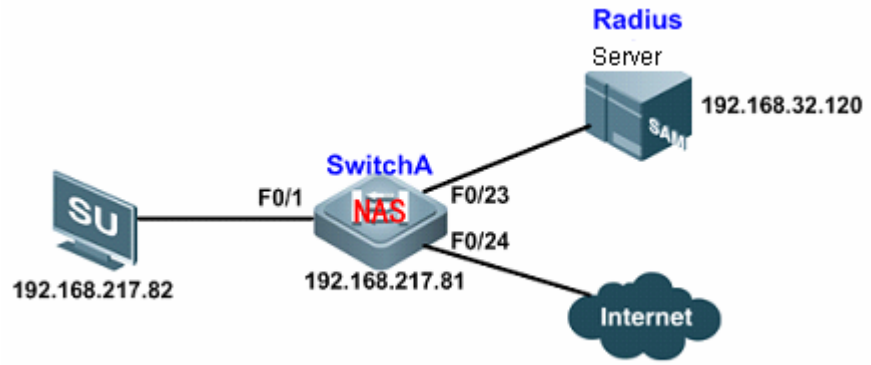


Figure 12 Network topology for the 802.1X-based AAA service

4.5.1.2 Networking Requirements

To ensure the validity of network access, the following requirements must be met:

1. It is required that access users on each port must be subject to 1X authentication in order to control Internet access (unauthenticated users won't be able to access network);
2. Only our client software (supplicant) can be used as the client for 802.1x authentication;
3. Accounting shall be based on online time, and accounting update packets will be periodically sent to Radius Server (real-time accounting packets will be sent to RADIUS server every 15 minutes);
4. After sending the authentication request to RADIUS server, the device will resend the request if no reply is received within 5 seconds, and will try for totally 6 times;
5. Online monitoring of users to prevent authenticated user from being preempted by other users and to detect whether the user is disconnected;
6. To protect server from hostile attacks, the access user can only initialize re-authentication after 500 seconds if it fails in authentication. Meanwhile, after trying for over 5 times, this user will be considered as disconnected and the authentication process will end.

4.5.1.3 Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER; configure 802.1X authentication and configure the device port for client access

as controlled port (here we take port F0/1 as the example); (corresponding to paragraph 1 of "Application Needs")

- Filter non-DES-7200 supplicant (corresponding to paragraph 2 of "Networking requirements")
- Configure 802.1x accounting and accounting update, and configure the interval of accounting update packets (corresponding to paragraph 3 of " Networking requirements ")
- Configure the reply timeout timer of Radius Server as 5s, and configure the maximum authentication retries as 6 times (corresponding to paragraph 4 of " Networking requirements ")
- Configure periodic re-authentication of device (corresponding to paragraph 5 of " Networking requirements ")
- Configure the Quiet Period for failed authentication as 500s (waiting time) and configure the maximum authentication retries as 5 times (corresponding to paragraph 6 of " Networking requirements ")

4.5.1.4 Configuration Steps

Step 1: Configure relevant attributes of Radius Server

Step 2: Configure access switch "SwitchA"

! Turn on AAA switch

```
DES-7200(config)#aaa new-model
```

! Configure RADIUS server

```
DES-7200(config)#radius-server host 192.168.32.120
```

! Configure RADIUS Key

```
DES-7200(config)#radius-server key DES-7200
```

! Configure dot1x authentication method list

```
DES-7200(config)#aaa  authentication dot1x hello group radius
```

! Apply dot1x authentication method list

```
DES-7200(config)#dot1x authentication hello
```

! Configure F0/1 as controlled port (enable port-based authentication)

```
DES-7200(config)#interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)#dot1x port-control auto
DES-7200(config-if-FastEthernet 0/1)#exit
```

! Filter non-DES-7200 supplicant

```
DES-7200(config)#dot1x private-supplicant-only
```

! Configure 802.1X accounting method list

```
DES-7200(config)#aaa accounting network jizhang start-stop group radius
```

! Apply 802.1X accounting method list

```
DES-7200(config)#dot1x accounting jizhang
```

! Configure accounting update

```
DES-7200(config)#aaa accounting update
```

! Configure the accounting update interval as 15 minutes

```
DES-7200(config)#aaa accounting update periodic 15
```

! Configure the reply timeout timer of Radius Server as 5s

```
DES-7200(config)#dot1x timeout server-timeout 5
```

! Configure maximum transmission retries as 6 times

```
DES-7200(config)#dot1x max-req 6
```

! Enable periodic re-authentication

```
DES-7200(config)#dot1x re-authentication
```

! Configure the re-authentication interval as 1000s

```
DES-7200(config)#dot1x timeout re-authperiod 1000
```

! Configure the Quiet Period of device as 500s

```
DES-7200(config)#dot1x timeout quiet-period 500
```

! Configure the maximum authentication retries of device as 5 times

```
DES-7200(config)#dot1x reauth-max 5
```

! Configure the default route of device

```
DES-7200(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

! Configure the IP address of device

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

Step 3: Use authentication client (such as supplicant) to carry out authentication; type in the correct username and password and select the network adapter, and the authentication will succeed after a few seconds.

4.5.1.5 Verify Configurations

Step 1: Display the authentication state information of current user in order to eliminate faults.

```
DES-7200#show dot1x summary
ID       MAC      Interface VLAN   Auth-State    Backend-State Port-Status
User-Type
-------- --------------  --------- ---- --------------- -------------
----------- ---------
1       00d0.f864.6909  Fa0/1    1    Authenticated   Idle         Authed
static
```

Step 2: Display detailed information about authenticated user.

```
DES-7200#show dot1x user id 1

User name: qq
User id: 1
Type: static
```

```
Mac address is 00d0.f864.6909
Vlan id is 1
Access from port Fa0/1
Time online: 0days 0h 2m24s
User ip address is 192.168.217.82
Max user number on this port is 6000
Authorization session time is 20736000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name qq_1_0_0 :
```

Step 3: Display 1X configurations about the existing number of users and the number of authenticated users;

```
DES-7200#show dot1x


802.1X Status:       enable
Authentication Mode:  eap-md5
Total User Number:   1(exclude dynamic user)
Authed User Number:  1(exclude dynamic user)
Dynamic User Number:  0
Re-authen Enabled:   enable
Re-authen Period:    1000 sec
Quiet Timer Period:  500 sec
Tx Timer Period:     3 sec
Supplicant Timeout:  3 sec
Server Timeout:      5 sec
Re-authen Max:       5 times
Maximum Request:     6 times
Private supplicant only:  enable
Client Online Probe:  disable
Eapol Tag Enable:    disable
Authorization Mode:  disable
```

Step 4: Display Radius authentication and accounting related configurations;

```
DES-7200#show radius server

Server IP:   192.168.32.120
Accounting Port:  1813
Authen  Port:    1812
Server State:    ready
```

4.5.2 Application of 802.1X port-based dynamic VLAN assignment

4.5.2.1 Network Topology

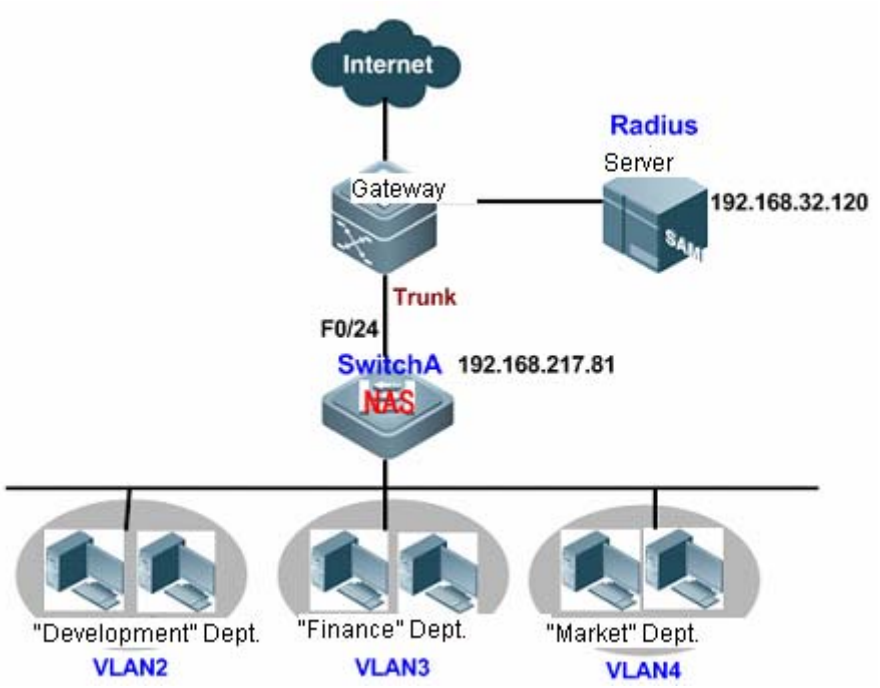


Figure 13 Topoloy for 802.1X port-based dynamic VLAN assignment

4.5.2.2 Networking requirements

A company has three user groups, namely "development" department, "finance" department and "market" department. The following needs must be met:

- Each member of these three user groups can be connected to any port of the access device and join the corresponding VLAN after successful authentication ("development" department to join VLAN2, "finance" department to join VLAN3, and "market" department to join VLAN4).
- Complete data isolation shall be achieved between VLANs corresponding to three user groups, namely the members of one group cannot exchange data with members of another group.

4.5.2.3 Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER;

- Configure 802.1X authentication and configure the device port for client access as controlled port;
- Enable dynamic VLAN assignment on the corresponding interface;
- Create VLANs to join after user authentication.

4.5.2.4 Configuration Steps

Step 1: Configure relevant attributes of Radius Server

Step 2: Configure access switch "SwitchA"

! Turn on AAA switch

```
DES-7200(config)#aaa new-model
```

! Configure RADIUS server

```
DES-7200(config)#radius-server host 192.168.32.120
```

! Configure RADIUS key

```
DES-7200(config)#radius-server key DES-7200
```

! Configure dot1x authentication method list

```
DES-7200(config)#aaa  authentication dot1x hello group radius
```

! Apply dot1x authentication method list

```
DES-7200(config)#dot1x authentication hello
```

! Configure 802.1X accounting method list

```
DES-7200(config)#aaa accounting network jizhang start-stop group radius
```

! Apply 802.1X accounting method list

```
DES-7200(config)#dot1x accounting jizhang
```

! Configure the port as controlled port (enable port-based authentication)

```
DES-7200(config)#interface range fastEthernet 0/1-23
DES-7200(config-if-range)#dot1x port-control auto
```

! Enable dynamic VLAN assignment on the corresponding interface

```
DES-7200(config-if-range)# dot1x dynamic-vlan enable
```

! Create VLANs to join after user authentication

```
DES-7200(config)#vlan 2
DES-7200(config-vlan)#name development
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 3
DES-7200(config-vlan)#name finance
DES-7200(config-vlan)#exit
DES-7200(config)#vlan 4
DES-7200(config-vlan)#name market
DES-7200(config-vlan)#exit
```

! Configure uplink port F0/24 as the trunk port.

```
DES-7200(config)#interface fastEthernet 0/24
```

```
DES-7200(config-if-FastEthernet 0/24)#switchport mode trunk
```

! Configure the default route of device

```
DES-7200(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

! Configure the IP address of device

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

Step 3: Use client to complete authentication. After successful authentication, the CLI will display: "%DOT1X-4-TRANS_AUTHOR: Setting interface FastEthernet 0/1 author-vlan 2 succeeded."

We can see that the user has been assigned to VLAN2.

4.5.2.5 Verify Configurations

Step 1: Display the authentication state information of current user to see the true VLAN to which the user belongs.

```
DES-7200#show dot1x summary
   ID       MAC      Interface VLAN   Auth-State    Backend-State
Port-Status User-Type
-------- --------------  --------- ---- --------------- -------------
----------- ---------
5       00d0.f864.6909  Fa0/1    2    Authenticated   Idle         Authed
static
```

Step 2: Display detailed information about authenticated user.

```
DES-7200#show dot1x user id 5

User name: st
User id: 5
Type: static
Mac address is 00d0.f864.6909
Vlan id is 2
Access from port Fa0/1
Time online: 0days 0h 4m35s
User ip address is 192.168.217.82
Max user number on this port is 6000
Authorization vlan is 2
Authorization session time is 20731685 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name st_1_0_0 :
```

4.5.3 Application of 802.1X port-based Guest VLAN and VLAN assignment

4.5.3.1 Network Topology

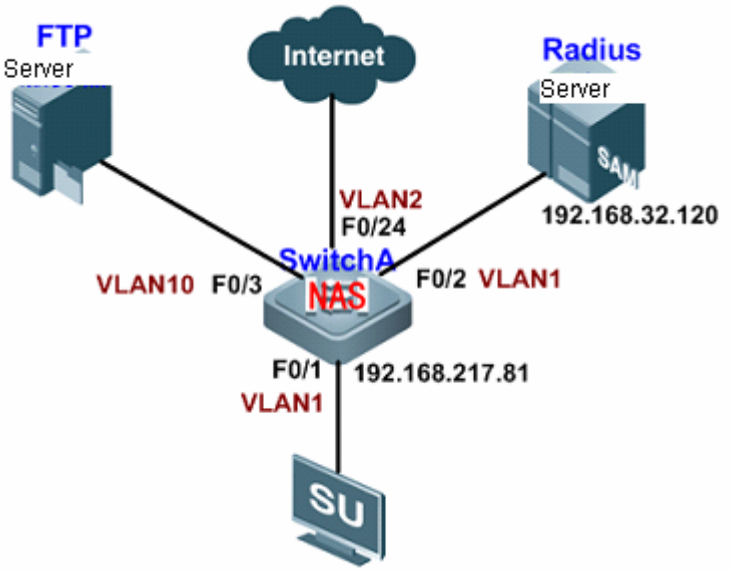


Figure 14 topology for 802.1X port-based Guest VLAN and VLAN assignment

4.5.3.2 Networking Requirements

The client accesses network through 802.1x authentication. RADIUS server is the authentication server, and FTP server is the server used by the client for software downloading and pack upgrade while it belongs to VLAN10. Radius Server is used for authentication, authorization, accounting and dynamic VLAN assignment, and it belongs to VLAN1. The Internet-connecting port F0/24 of switch belongs to VLAN2. The following needs must be met:

- If the switch receives no reply after sending authentication request packets (EAP-Request/Identity) for the configured number of tries, F0/1 will join the Guest VLAN (VLAN10). By this time, both Supplicant and FTP Sever belong to VLAN10, and Supplicant can access FTP Server and download 802.1x client.
- After successful authentication, RADIUS server will assign VLAN2. By this time, both Supplicant and F0/24 belong to VLAN2, and Supplicant can access Internet.

4.5.3.3 Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER;
- Configure 802.1X authentication and configure the device port for client access as controlled port;

- Enable dynamic VLAN assignment on the corresponding interface;
- Configure whether or not enable guest VLAN on the corresponding interface.

4.5.3.4 Configuration Steps

Configure access switch "SwitchA":

! Configure the VLANs to which the port belong:

```
DES-7200(config)#interface fastEthernet 0/3
DES-7200(config-if-FastEthernet 0/3)#switchport access vlan 10
DES-7200(config-if-FastEthernet 0/3)#exit
DES-7200(config)#interface fastEthernet 0/24
DES-7200(config-if-FastEthernet 0/24)#switchport access vlan 2
DES-7200(config-if-FastEthernet 0/24)#exit
```

! Turn on AAA switch

```
DES-7200(config)#aaa new-model
```

! Configure RADIUS server

```
DES-7200(config)#radius-server host 192.168.32.120
```

! Configure RADIUS key

```
DES-7200(config)#radius-server key DES-7200
```

! Configure dot1x authentication method list

```
DES-7200(config)#aaa  authentication dot1x hello group radius
```

! Apply dot1x authentication method list

```
DES-7200(config)#dot1x authentication hello
```

! Configure 802.1X accounting method list

```
DES-7200(config)#aaa accounting network jizhang start-stop group radius
```

! Apply 802.1X accounting method list

```
DES-7200(config)#dot1x accounting jizhang
```

! Configure the port as controlled port (enable port-based authentication)

```
DES-7200(config)#interface fastEthernet 0/1
DES-7200(config-if-FastEthernet 0/1)#dot1x port-control auto
```

! Enable dynamic VLAN assignment on the corresponding interface

```
DES-7200(config-if-FastEthernet 0/1)# dot1x dynamic-vlan enable
```

! Enable GUEST VLAN assignment on the interface

```
DES-7200(config-if-FastEthernet 0/1)#dot1x guest-vlan 10
```

! Configure the default route of device

```
DES-7200(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

! Configure the IP address of device

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

4.5.3.5 Verify Configurations

Step 1: If no reply is received after sending authentication request packets (EAP-Request/Identity) for the configured number of tries, the user connected to the port will automatically join VLAN10. The CLI will prompt:

```
%DOT1X-5-TRANS_DEFAULT_TO_GUEST: Transformed interface FastEthernet 0/1
from default-vlan 1 to guest-vlan 10 ok.
```

Step 2: The user downloads 802.1x client. After successful authentication, the CLI will prompt:

```
%DOT1X-4-TRANS_AUTHOR: Setting interface FastEthernet 0/1 author-vlan 2
succeeded.
```

1. Display the authentication state information of current user:

```
DES-7200#show dot1x summary
   ID       MAC      Interface VLAN   Auth-State    Backend-State
Port-Status User-Type
-------- --------------  --------- ---- -------------- -------------
----------- ---------
8       00d0.f864.6909  Fa0/1    2    Authenticated   Idle        Authed
static
```

Step 2: Display detailed information about authenticated user.

```
DES-7200#show dot1x user id 8

User name: st
User id: 8
Type: static
Mac address is 00d0.f864.6909
Vlan id is 2
Access from port Fa0/1
Time online: 0days 0h 4m25s
User ip address is 192.168.201.56
Max user number on this port is 6000
Authorization vlan is 2
Authorization session time is 20736000 seconds
Supplicant is private
Start accounting
Permit proxy user
Permit dial user
IP privilege is 0
 user acl-name st_1_0_0 :
```

4.5.4 Application of port-based 1X authentication and IP authorization

4.5.4.1 Network Topology

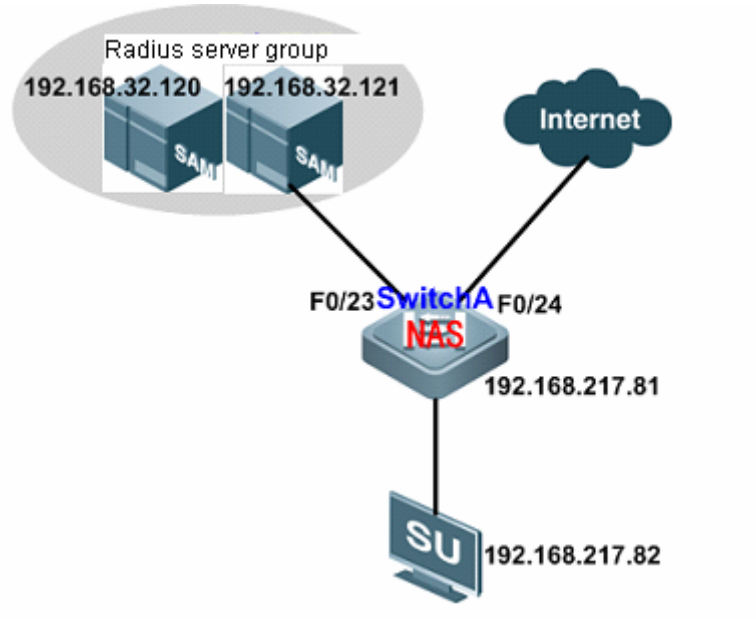


Figure15 topology for port-based 1X authentication and IP authorization

4.5.4.2 Networking Requirements

The client accesses network through 802.1x authentication. RADIUS server is the authentication server. The following application needs must be met:

- When the active server fails due to certain reason, the device can automatically submit authentication request to the next server in the method list.
- When a user connected to one port of device passes the authentication, all users connected to this port will be able to access network freely.
- Dynamic user is not allowed to move between multiple authentication ports.
- The IP of an authenticated user must be assigned by the RADIUS Server, namely the authenticated user can only use the IP specified by RADIUS Server to access network.

4.5.4.3 Configuration Tips

- Turn on AAA switch and configure the communication between device and RADIUS SERVER;
- Configure 802.1X authentication and configure the device port for client access as controlled port;

- Configure active/standby server group
- Configure the control mode of user authentication under the corresponding port as port-based authentication;
- Configure to prohibit dynamic user from moving between ports;
- Configure IP authorization mode as radius Server mode.

4.5.4.4 Configuration Steps

Configure access switch "SwitchA":

! Turn on AAA switch

```
DES-7200(config)#aaa new-model
```

! Configure RADIUS server

```
DES-7200(config)#radius-server host 192.168.32.120
DES-7200(config)#radius-server host 192.168.32.121
```

! Configure RADIUS key

```
DES-7200(config)#radius-server key DES-7200
```

! Configure server group (select active server and standby server)

```
DES-7200(config)#aaa group server radius rj
DES-7200(config-gs-radius)#server 192.168.32.120
DES-7200(config-gs-radius)#server 192.168.32.121
```

! Configure dot1x authentication list

```
DES-7200(config)#aaa  authentication dot1x hello group radius
```

! Apply dot1x authentication method list

```
DES-7200(config)#dot1x authentication hello
```

! Configure 802.1X accounting method list

```
DES-7200(config)#aaa accounting network jizhang start-stop group radius
```

! Apply 802.1X accounting method list

```
DES-7200(config)#dot1x accounting jizhang
```

! Configure the port as controlled port (enable port-based authentication)

```
DES-7200(config)#interface range fastEthernet 0/1-22
DES-7200(config-if-range)#dot1x port-control auto
```

! Configure the control mode of user authentication under the corresponding port as port-based authentication

```
DES-7200(config-if-range)# dot1x port-control-mode port-based
DES-7200(config-if-range)#exit
```

! Configure to prohibit dynamic user from moving between ports;

```
DES-7200(config)#dot1x stationarity enable
```

! Configure IP authorization mode of device as RADIUS Server mode

```
DES-7200(config)#aaa authorization ip-auth-mode radius-server
```

! Configure the default route of device

```
DES-7200(config)#ip route 0.0.0.0 0.0.0.0 192.168.217.1
```

! Configure the IP address of device

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.217.81 255.255.255.0
```

4.5.4.5 Verify Configurations

Step 1: Display the authentication state information of current user:

```
DES-7200#show dot1x summary
   ID       MAC      Interface VLAN   Auth-State    Backend-State
Port-Status User-Type
-------- --------------  --------- ---- -------------- -------------
----------- ---------
none    00d0.f864.6909  Fa0/1    1    Authenticated   Idle        Authed
Dynamic
```

Step 2: Move this user to another authenticated port. It can be found that the user won't be able to access network.

5 Port-based Flow Control Configuration

5.1 Storm Control

5.1.1 Overview

Too many broadcast, multicast or unknown unicast packets in the LAN will slow the network speed and increase the possibility of packet transmission timeout significantly. This is called LAN storm. Protocol stack implementation errors or wrong network configuration may lead to such storms.

Storm control can be conducted upon the broadcast, multicast and unknown unicast data streams respectively. When the rate of the broadcast, multicast or unknown unicast packets received by the interface exceeds the specified bandwidth throttling, the device only allows the packets within the bandwidth throttling. The packets that exceed the throttle will be discarded until the data stream becomes normal again. This prevents excessive flooding packets from entering the LAN to form a storm.

5.1.2 Configuring Storm Control

In the interface configuration mode, use the following command to configure storm control:

Command	Function
DES-7200(config-if)# **storm-control** {**broadcast** | **multicast** | **unicast**} [{ **level** *percent* | **pps** *packets* | *rate-bps*]	**broadcast**: Enable the broadcast storm control function. **multicast**: Enable the unknown multicast storm control function. **unicast**: Enable the unknown unicast storm control function. *percent:* Set according to the bandwidth percentage, for example, 20 means 20% *packets*: Set according to the pps, which means packets per second *Rate-bps*: rate allowed

In the interface configuration mode, you can disable the storm control on the appropriate interface by using the **no storm-control broadcast**, **no storm-control multicast**, or n**o storm-control unicast** command.

The following example enables the multicast storm control on GigabitEthernet 0/1 and set the allowed rate as 4M.

```
DES-7200# configure terminal
DES-7200(config)# interface GigabitEthernet 0/1
DES-7200(config-if)# storm-control multicast 4096
DES-7200(config-if)# end
```

Note

1. By default, for DES-7200 series, the storm control function for broadcast, multicast and unknown unicast packets is disabled.

3. For DES-7200 series, the level-based storm control has certain errors for the packets in the length of more than 64 bytes. The longer the packet length is, the greater the comparable error value is. The error formula is (packet length-64)/84.

4. The reference bandwidth for the level-based storm control is the maximum bandwidth supported by the physical port, but not converted from the bandwidth of the physical port in service.

5. If you enable storm control with the **storm-control broadcast** command, the default setting or 14880PPS is used.

5.1.3 Viewing the Enable Status of Storm Control

To view the storm control status of the interface, use the following command:

Command	Function
DES-7200**# show storm-control** [*interface-id*]	Show storm control information.

The instance below shows the enabled status of the storm control function of interface Gi1/3:

```
DES-7200# show storm-control gigabitEthernet 0/3
Interface  Broadcast Control  Multicast Control  Unicast Control action
GigabitEthernet 0/3 Disabled  Disabled   Disabled    none
```

You can also view the enabling status of the storm control function of all interfaces at a time:

```
DES-7200# show storm-control
Interface  Broadcast Control  Multicast Control  Unicast Control Action
--------- ----------------- ----------------- ------- ------- ------
```

```
GigabitEthernet 0/1   Disabled   Disabled   Disabled   none
GigabitEthernet 0/2   Disabled   Disabled   Disabled   none
GigabitEthernet 0/3   Disabled   Disabled   Disabled   none
GigabitEthernet 0/4   Disabled   Disabled   Disabled   none
GigabitEthernet 0/5   Disabled   Disabled   Disabled   none
GigabitEthernet 0/6   Disabled   Disabled   Disabled   none
GigabitEthernet 0/7   Disabled   Disabled   Disabled   none
GigabitEthernet 0/8   Disabled   Disabled   Disabled   none
GigabitEthernet 0/9   Disabled   Disabled   Disabled   none
GigabitEthernet 0/10  Disabled   Disabled   Disabled   none
GigabitEthernet 0/11  Disabled   Disabled   Disabled   none
GigabitEthernet 0/12  Disabled   Disabled   Disabled   none
GigabitEthernet 0/13  Disabled   Disabled   Disabled   none
GigabitEthernet 0/14  Disabled   Disabled   Disabled   none
GigabitEthernet 0/15  Disabled   Disabled   Disabled   none
GigabitEthernet 0/16  Disabled   Disabled   Disabled   none
GigabitEthernet 0/17  Disabled   Disabled   Disabled   none
GigabitEthernet 0/18  Disabled   Disabled   Disabled   none
GigabitEthernet 0/19  Disabled   Disabled   Disabled   none
GigabitEthernet 0/20  Disabled   Disabled   Disabled   none
GigabitEthernet 0/21  Disabled   Disabled   Disabled   none
GigabitEthernet 0/22  Disabled   Disabled   Disabled   none
GigabitEthernet 0/23  Disabled   Disabled   Disabled   none
GigabitEthernet 0/24  Disabled   Disabled   Disabled   none
```

5.2 Protected Port

5.2.1 Overview

In some application environments, some ports are not required to communicate with each other on a device. In such case, frame forwarding is not allowed between the protected ports, no mattter the frames are unicast frames, broadcast frames or multicast frames. To achieve this purpose, you can set some ports as protected ports.

Once ports are set as protected ports, they cannot communicate with each other. However, protected ports can still communicate with unprotected ports.

There are two protected port modes: one is to block layer 2 forwarding between protected ports but allow layer 3 routing; the other is to block layer 2 forwarding and layer 3 routing between protected ports. The first mode is by default when both modes are supported.

When you set two protected ports as a SPAN port pair, the frames transmitted or received by the source port of SPAN are sent to the destination port of SPAN according to the SPAN setting. Therefore, it is not recommended to set the destination port of SPAN as the protected port (and you can also save system resources by doing so).

The device supports setting the Aggregated Port as the protected port. Once you do that, all the member ports of the Aggregated Port will be set as the protected port.

5.2.2 Configuring the Protected Port

Set one port as the protected port:

Command	Function
DES-7200(config-if)**# switchport protected**	Set this interface as a protected port

You can reset a port as unprotected port with the **no switchport protected** command in the interface configuration mode.

The following example describes how to set the Gigabitethernet 0/3 as the protected port.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport protected
DES-7200(config-if)# end
```

Caution For DES-7200 series, the destination port of the remote mirroring cannot be configured as the protected port on the RSPAN destination device.

5.2.3 Configuring the Route-deny Between Protected Ports

Command	Function
DES-7200(config)**# protected-ports route-deny**	Set the route-deny between the protected ports.

You can reenable the Layer 3 route between the protected ports using the **no protected-ports route-deny** command in the interface configuration mode.

The following example describes how to disable the Layer 3 route between the protected ports.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# protected-ports route-deny
DES-7200(config)# end
```

5.2.4 Showing Protected Port Configuration

Command	Function

Command	Function
DES-7200(config-if)**# show interfaces switchport**	Show the configuration of the switching port

You can use the command of **show interfaces switchport** to view the configuration of protected port.

```
DES-7200# show interfaces gigabitethernet 0/3 switchport
Interface   Switchport  Mode   Access Native Protected   VLAN lists
---------   ----------  ----   ------ ------ --------   ----
GigabitEthernet 0/3  enabled   Trunk  1   1    Enabled    ALL
```

5.3 Port Security

5.3.1 Overview

Port security function allows the packets to enter the switch port by the source MAC address, source MAC+IP address or source IP address. You can control the packets by setting the specific MAC address statically, static IP+MAC binding or IP binding, or dynamically learning limited MAC addresses. The port with port security enabled is named as secure port. Only the packets with the source MAC address in the port security address table, or IP+MAC binding configured, or IP binding configured, or the learned MAC address, can join the switch communication, while other packets are dropped.

To enhance security, you can bind the MAC address with the IP address as the secure address. Of course you can also designate the MAC address without binding the IP address.

You can add the secure addresses on the port in the following ways:

- You can manually configure all the secure addresses of the port by using the commands in the interface configuration mode.
- You can also let this port automatically learn these addresses, which will become the secure address on this port till the total number reaches the maximum value. Note that, however, the automatically-learned secure addresses will not be bound with the IP address. On the same port, if you have configured a secure address bound with the IP address, the port cannot be added with any secure address by automatic learning.
- Manually configure some secure addresses, and let the device to learn the rest.

The port security also supports the Sticky MAC address, which can converts the secure addresses learned dynamiclly to the statically configured. You can use the **show running-config** command to display the configuration. With the configuration saved, learning these dynamic secure addresses after restarting the system is unnecessary. If this function is not enabled, then the dynamically learned sercure MAC

addresses should be learned again after the reboot.

When a port is configured as a secure port and the maximum number of its secure addresses is reached, a security violation occurs if the port receives a packet whose source address is not one of the secure addresses on the port. When security violations occur, you can set the following methods to handle:

- **protect:** When the maximum number of secure addresses is reached, the secure port discards the packet of unknown addresses (none of which are among the secure addresses of the port).This is the default method for handling exceptions.
- **restrict:** In the case of violation, a Trap notification is sent
- **shutdown:** In the case of violation, the port is shut down and a Trap notification is sent.

5.3.2 Configuring Port Security

5.3.2.1 Default Configuration of Port Security

The table below shows the default configuration of port security:

Item	Default Configuration
Port security switch	The port security function is disabled for all the ports.
Maximum number of secure addresses	128
Secure address	None
Handling mode for violations	Protect
Secure address binding mode	None
Sticky MAC address learning	Disabled

5.3.2.2 Port Security Configuration Guide

The following restrictions apply to port security configuration:

- A secure port is not an Aggregate Port.
- A secure port is not the destination port of SPAN.
- A secure port is and can only be an Access Port.

The 802.1x authentication and port security are mutually exclusive in enabling. The 802.1x authentication and port security can ensure the validity of the network users. You can enable either of them to control port access.

At the same time, the secure addresses of the IP+MAC addresses and IP addresses

share with the ACLs the hardware resources of the system. Therefore, when you apply the ACLs on one secure port, the IP+MAC addresses and IP addresses on the port can be configured with less secure addresses.

The secure addresses for the same secure port must have the same format, namely either all or none of them are bound with IP addresses. If a security port includes these two types of security addresses at the same time, the secure address not bound with the IP address will fail (the secure address bound with the IP address has a high priority).

5.3.2.3 Configuration of Secure Ports and Violation Handling Modes

In the interface configuration mode, configure secure ports and violation handling modes by using the following commands:

Command	Function
DES-7200(config-if)# **switchport port-security**	Enable the port security function of this interface.
DES-7200(config-if)# **switchport port-security maximum** *value*	Set the maximum number of secure addresses on the interface. The range is between 1 and 1000 and the default value is 128.
DES-7200(config-if)# **switchport port-security violation**{**protect** | **restrict** | **shutdown**}	Set the violation handling mode: **protect**: Protected port. When the number of secure addresses if full, the security port will discard the packets from unknown address (that is, not any among the secure addresses of the port). **restrict**: In the case of violation, a Trap notification is sent **shutdown**: In the case of violation, the port is shut down and a Trap notification is sent. When a port is closed because of violation, you can recover it from the error status by using the **errdisable recovery** command in the global configuration mode.
DES-7200(config-if)# **switchport port-security mac-address sticky**	Enable the Sticky MAC address learning.

In the interface configuration mode, you can disable the port security function of an interface with the command **no switchport port-security**. Use the command **no switchport port-security maximum** to recover to the default maximum value. Use the command **no switchport port-security violation** to set violation handling to the default mode. Use the command **no switchport port-security mac-address sticky** to set the Sticky MAC address learning to the default mode.

The instance below describes how to enable the port security function on interface gigabitethernet 0/3. The maximum number of addresses to be set is 8 and the violation handling mode is set as protect.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security maximum 8
DES-7200(config-if)# switchport port-security violation protect
DES-7200(config-if)# switchport port-security mac-address sticky
DES-7200(config-if)# end
```

Note

1. If the DOT1X has been enabled on the interface and the authenticated user number has exceeded the maximum limit, it fails to enable the port security function.
2. With the port security and DOT1X function enabled at the same time, If the secure address ages out, the DOT1X user can continue to communicate after the re-authentication.
3. It needs no authentication to access to the network for the secure address on the static port.
4. For the DES-7200 series, with IP+MAC binding configured in the IPv6 compatible mode on the security port, the IPv6 packets corresponds to the secure address but not the IP+MAC binding address can be transmitted.
5. If the violation mode is modified on the interface, the new violation mode takes effect only after the security port restores to the non-violation state.

5.3.2.4 Configuration of Secure Addresses on the Secure Port

In the global configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
DES-7200(config)# **switch portport-security interface** *interface-id* **mac-address** *mac-address*〕**vlan** [*vlan_id*]	In the global configuration mode, manually configure the secure addresss on the port.

In the interface configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
DES-7200(config-if)# **switchportport-security** ［**mac-address** *mac-address*］ **vlan** [*vlan_id*]	In the interface configuration mode, manually configure the secure addresses on the port.
DES-7200(config-if)# **switchportport-security** ［**mac-address sticky** *mac-address*］ **vlan** [*vlan_id*]	In the interface configuration mode, manually configure the Sticky secure addresses on the port.

In the interface configuration mode, you can use the command **no switchport port-security mac-address** *mac-address* to delete the secure address of this interface. Use the command **no switchport port security sticky mac-address** *mac-address* to delete the Sticky secure address of this interface.

The example below describes how to configure a secure address for interface gigabitethernet 0/3: 00d0.f800.073c and bind it with an IP address: 192.168.12.202.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security mac-address 00d0.f800.073c
ip-address 192.168.12.202
DES-7200(config-if)# end
```

The example below describes how to configure a secure address for the Sticky-MAC-learning-enabled interface gigabitethernet 0/3: 00d0.f800.073c.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security mac-address sticky
DES-7200(config-if)# switchport port-security mac-address sticky
00d0.f800.073c  vlan 1
DES-7200(config-if)# end
```

5.3.2.5 Configuration of Secure Address Binding on the Secure Port

In the global configuration mode, add secure address binding for secure ports by using the following commands:

Command	Function

Command	Function
DES-7200(config)# **switchport port-security interface** i*nterface-id* binding [*mac-address* vlan *vlan_id*] [*ipv4-address*]| [*ipv6-address*]	In the global configuration mode, manually configure the secure addresss binding on the port.

In the interface configuration mode, add secure addresses for secure ports by using the following commands:

Command	Function
DES-7200(config-if)**# switchport port-security binding** [*mac-address* vlan *vlan_id*] [*ipv4-address*]|[*ipv6-address*]	In the interface configuration mode, manually configure the secure addresss binding on the port.

The example below describes how to configure a secure address for interface gigabitethernet 0/3 and bind it with an IP address: 192.168.12.202.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security binding 192.168.12.202
DES-7200(config-if)# end
```

The example below describes how to configure a secure address for interface gigabitethernet 0/3 and bind it with an source IP+MAC address: 192.168.12.202: 00d0.f800.073c.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitethernet 0/3
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport port-security
DES-7200(config-if)# switchport port-security binding 00d0.f800.073c vlan 1
192.168.12.202
DES-7200(config-if)# end
```

Note

For the packets that correspond to the IP+MAC binding and IP binding, they can be forwarded on the condition that the source MAC address must be the secure address at the same time. For the dynamic secure address, before adding the secure address to the secure address table, any packets that correspond to the secure addrss binding or IP binding can not be forwarded.

5.3.2.6 Configuration of Aging Time for Secure Addresses

You can configure the aging time for all the secure addresses on an interface. To enable this function, you need to set the maximum number of secure addresses. In this way, you can make the device automatically add/remove the secure addresses to/from the interface.

In the interface configuration mode, configure the aging time for secure addresses by using the following command:

Command	Function
DES-7200(config-if)**#switchport port-security aging**{**static** | **time** *time* }	**static**: When this keyword is added, the aging time will be applied to both the manually configured secure address and automatically learnt addresses. Otherwise, it is applied only to the automatically learnt addresses. **time**: indicates the aging time for the secure address on this port. Its range is 0-1440 and unit is Minute. If you set it to be 0, the aging function actually is disabled. The aging time is the absolute time, which means that an address will be deleted automatically after the *Time* specified expires after the address becomes the secure address of the port. The default value of *Time* is 0.

In the interface configuration mode, use **no switchport port-security aging time** to disable the port security aging. Use the **no switchport port-security aging static** to apply the aging time only to dynamically learned security address.

The example below describes how to configure the port security aging time on interface Gigabitethernet 0/3. The aging time is set to 8 minutes and it is applicable to statically-configured secure addresses:

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)# interface gigabitthernet 0/3
DES-7200(config-if)# switchport port-security aging time 8
DES-7200(config-if)# switchport port-security aging static
DES-7200(config-if)# end
```

5.3.3 Viewing Port Security Information

In the privileged mode, you can view the security information of a port by using the following commands.

Command	Function
DES-7200**#show port-security interface** [*interface-id*]	View the port security configuration of an interface.
DES-7200**#show port-security address**	View the secure address information.
DES-7200# **show port-security address** [*interface-id*]	Show the secure address information on an interface.
DES-7200# **show port-security**	Show the statistics of all the security ports, including the maximum number of secure addresses, the number of current addresses, and violation handling mode.

The example below shows the port security configuration on interface **gigabitethernet 0/3**:

```
DES-7200# show port-security interface gigabitethernet 0/3
Interface Gi0/3
Port Security: Enabled
Port status : down
Violation mode:Shutdown
Maximum MAC Addresses:8
Total MAC Addresses:0
Configured MAC Addresses:0
Aging time : 8 mins
SecureStatic address aging : Enabled
```

The instance below shows all the secure addresses in the system.

```
DES-7200# show port-security address
Vlan Mac Address IP Address Type Port Remaining Age(mins)
---------------------------------------- ------------------
1  00d0.f800.073c   192.168.12.202    Configured   Gi0/3    8
1  00d0.f800.3cc9   192.168.12.5     Configured   Gi0/1    7
```

You can also only show the secure address on one interface. The instance below shows the secure address on interface gigabitsethernet 0/3.

```
DES-7200# show port-security address interface gigabitethernet 0/3
Vlan Mac Address IP Address Type Port Remaining Age(mins)
---- --------------- ---------- ------ ------------------
1   00d0.f800.073c  192.168.12.202 Configured Gi0/3    8
```

The example below shows the statistic information of the secure port.

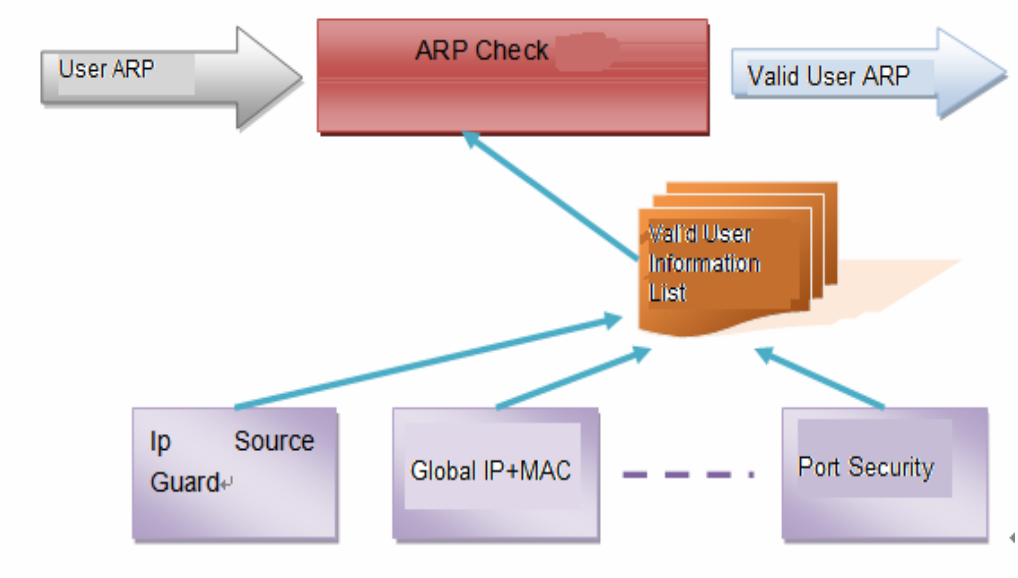
```
DES-7200# show port-security
Secure Port MaxSecureAddr(count) CurrentAddr(count) Security Action
-------- ----------------  ----------------  ------------
Gi0/1      128                1              Restrict
Gi0/2      128                0              Restrict
Gi0/3      8                  1             Protect
```

5.4 ARP-CHECK

5.4.1 Overview

ARP-Check function filters all ARP packets on the logic interface and dropps all illegal ARP packets, avoiding the ARP fraud in the network and improving the network stability.

DES-7200 switches support multiple IP security application(such as IP Source Guard, globle IP+MAC binding, port security, ect), which effectively filter the user IP packets and avoid the illegal user to use the network resources. The ARP check function generates the corresponding ARP filtering information accoding to the legel user information (IP or IP+MAC), implementing the illegal ARP packet filtering in the network.



ARP Check and other security functions

As shown in the above figure, ARP Check function checks whether the Sender IP field or the <Sender IP, Sender MAC> field of all ARP packets on the logic interface matches with the legal user information(IP or IP+MAC), and the ARP packets that not match with the legal user information. The ARP Check function supported security function modules include:

1. Check the IP field only: IP mode for the port security and the ip source guard.

2. Check the IP+MAC field: IP+MAC binding mode for the port security, global IP+MAC binding, 802.1x IP authorization, IP Source Guard, GSN binding function.

There are two modes of ARP-CHECK: enabled, disabled mode. The disabled mode is by default.

- In the enabled mode, ARP Check function is enabled or disabled according to the current security function running state on the switch.

Enabling/disabling the following functions may trigger to enable/disable the ARP Check function:

1. Global IP+MAC binding

2. 802.1X IP authorizaiton

3. IP Source Guard

4. GSN binding

Adding the legal user for the first time or removing the last legal user may trigger to enable/disable the ARP Check function:

1. IP+MAC binding mode for the port security

2. IP-only mode for the port security

ARP check is enabled no matter whether there is security configuration. If there is no legal user on the port, all the arp packets from this port will be discarded.

- In the disabled mode, ARP packet on the port is not checked.

Caution

1. Enabling ARP check of port security addresses will decrease the maximum number of the security addresses of binding IP on all the ports by half.

5.4.2 Configuring ARP-CHECK

Use the following commands to configure ARP-CHECK in the privileged mode:

Command	Action
DES-7200# **configure t**	Enter the global configuration mode.
DES-7200(config)**#interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **arp-check**	Enable arp check.
DES-7200(config-if)# **no arp-check**	Disable arp check.
DES-7200(config-if)**#arp-check auto**	Restore to the default configuration: enabled.

5.4.3 Showing the ARP Check Entry on the interface

Use the following commands to show the ARP check entry information on the interface:

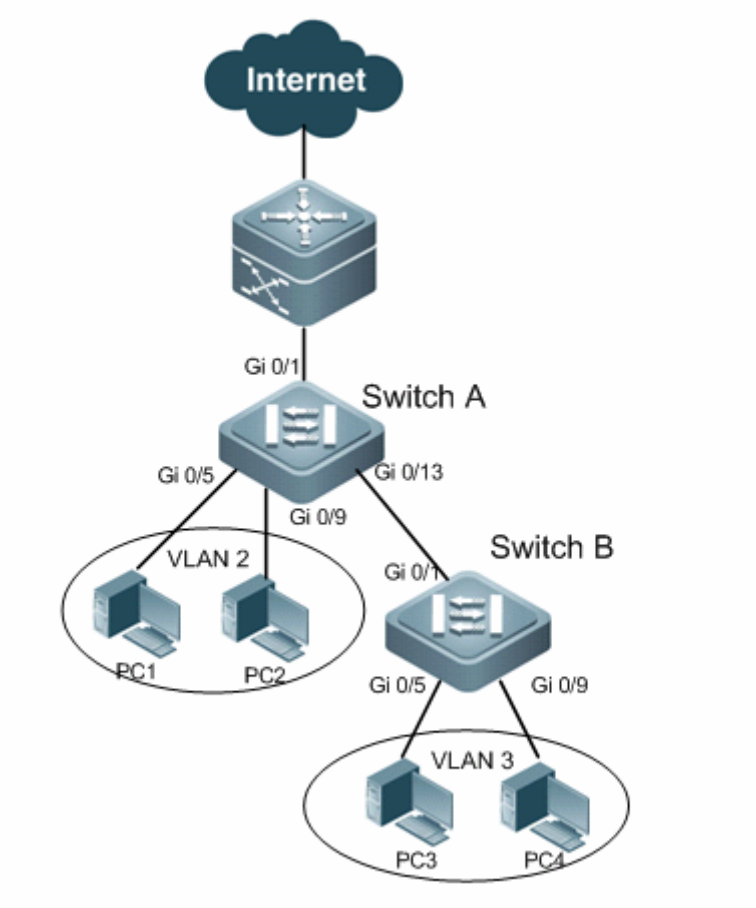
Command	Action
DES-7200#**show interface** { *interface-type interface-number* } **arp-check list**	Show the ARP check entry information.

The example below shows the ARP check entry information:

```
DES-7200#show interfaces arp-check list
  Interface            Sender MAC       Sender IP      Policy Source
----------------------- --------------- --------------- --------------------
  Gi 0/1               00D0.F800.0003   192.168.1.3      address-bind
  Gi 0/1               00D0.F800.0001   192.168.1.1      port-security
  Gi 0/4                                192.168.1.3      port-security
  Gi 0/5               00D0.F800.0003   192.168.1.3      address-bind
  Gi 0/7               00D0.F800.0006   192.168.1.6      AAA ip-auth-mode
               Gi 0/8               00D0.F800.0007   192.168.1.7      GSN
```

5.5 Example of Port-based Flow Control Combination

5.5.1 Topological Diagram



Network topology

5.5.2 Application Requirements

The above diagram shows the simplified topology of an typical Intranet. The following requirements must be met:

1. Prevent the devices form being attacked by broadcast, multicast and unknown unicast packets.
2. Allow directly connected users (users directly connected to Switch A) to access Internet with the specified IP/MAC address; packets with source address different from the specified IP/MAC address will be discarded to avoid source IP/MAC spoofing.

3. Access users (users accessing Switch B) are not allowed to carry out layer-2 packet communication, so as avoid the mutual interference between access users (such as ARP spoofing or DOS attack).

5.5.3 Configuration Tips

Configuration tips:

1. Enable storm control on the ports of all access devices (Switch A and Switch B).
2. Configure port security feature on the ports (Gi 0/5 and Gi 0/9) of access device (Switch A) to meet the second requirement.
3. Configure port protection on the access device (Switch B) to meet the third requirement.

Note:

After enabling port security and configuring IP/MAC entries, ARP Check will be enabled automatically to check the source address of ARP packets according to the configured IP/MAC address.

5.5.4 Configuration Steps

Configure Switch A

Step 1: Create the VLAN to which the switch belongs and configure port attributes.

! Create VLAN 2

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan 2
DES-7200(config-vlan)#exit
```

! Configure port attributes

```
DES-7200(config)#interface gigabitEthernet 0/5
DES-7200(config-if-GigabitEthernet 0/5)#switchport access vlan 2
DES-7200(config-if-GigabitEthernet 0/5)#exit
DES-7200(config)#interface gigabitEthernet 0/9
DES-7200(config-if-GigabitEthernet 0/9)#switchport access vlan 2
DES-7200(config-if-GigabitEthernet 0/9)#exit
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#switchport mode trunk
DES-7200(config-if-GigabitEthernet 0/1)#exit
DES-7200(config)#interface gigabitEthernet 0/13
DES-7200(config-if-GigabitEthernet 0/13)#switchport mode trunk
DES-7200(config-if-GigabitEthernet 0/13)#exit
```

Step 2: Enable storm control on all access ports.

```
DES-7200(config)#interface range gigabitEthernet 0/1,0/5,0/9,0/13
DES-7200(config-if-range)#storm-control broadcast
DES-7200(config-if-range)#storm-control multicast
DES-7200(config-if-range)#storm-control unicast
DES-7200(config-if-range)#exit
```

Step 3: Enable port security on the port directly connecting with users and bind the IP address and MAC address

! Bind the access user: IP (1.1.1.1)/MAC (0000.0000.0001)

```
DES-7200(config)#interface gigabitEthernet 0/5
DES-7200(config-if-GigabitEthernet 0/5)#switchport port-security
DES-7200(config-if-GigabitEthernet 0/5)#switchport port-security
mac-address 0000.0000.0001 ip-address 1.1.1.1
DES-7200(config-if-GigabitEthernet 0/5)#exit
```

! Bind the access user: IP (1.1.1.2)/MAC (0000.0000.0002)

```
DES-7200(config)#interface gigabitEthernet 0/9
DES-7200(config-if-GigabitEthernet 0/9)#switchport port-security
DES-7200(config-if-GigabitEthernet 0/9)#switchport port-security
mac-address 0000.0000.0002 ip-address 1.1.1.2
DES-7200(config-if-GigabitEthernet 0/9)#exit
```

Configure Switch B

Step 1: Create the VLAN to which the switch belongs and configure port attributes.

! Create VLAN 3

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#vlan 3
DES-7200(config-vlan)#exit
DES-7200(config)#interface gigabitEthernet 0/5
DES-7200(config-if-GigabitEthernet 0/5)#switchport access vlan 3
DES-7200(config-if-GigabitEthernet 0/5)#exit
DES-7200(config)#interface gigabitEthernet 0/9
DES-7200(config-if-GigabitEthernet 0/9)#switchport access vlan 3
DES-7200(config-if-GigabitEthernet 0/9)#exit
DES-7200(config)#interface gigabitEthernet 0/1
DES-7200(config-if-GigabitEthernet 0/1)#switchport mode trunk
DES-7200(config-if-GigabitEthernet 0/1)#exit
```

Step 2: Enable storm control on all access ports.

```
DES-7200(config)#interface range gigabitEthernet 0/1,0/5,0/9
```

```
DES-7200(config-if-range)#storm-control broadcast
DES-7200(config-if-range)#storm-control multicast
DES-7200(config-if-range)#storm-control unicast
DES-7200(config-if-range)#exit
```

Step 3: Enable port protection on all access ports.

```
DES-7200(config)#interface gigabitEthernet 0/5
DES-7200(config-if-GigabitEthernet 0/5)#switchport protected
DES-7200(config-if-GigabitEthernet 0/5)#exit
DES-7200(config)#interface gigabitEthernet 0/9
DES-7200(config-if-GigabitEthernet 0/9)#switchport protected
DES-7200(config-if-GigabitEthernet 0/9)#exit
```

5.5.5 Verification

Step 1: Check the configurations of Switch A. Key points: whether storm control has been enabled on respective ports, whether port security has been enabled on the port directly connecting with users and whether IP+MAC addresses have been bound statically.

```
DES-7200#show running-config
vlan 2
!
interface GigabitEthernet 0/1
 switchport mode trunk
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/5
 switchport access vlan 2
 switchport port-security mac-address 0000.0000.0001 ip-address 1.1.1.1
 switchport port-security
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/9
 switchport access vlan 2
 switchport port-security mac-address 0000.0000.0002 ip-address 1.1.1.2
 switchport port-security
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
```

```
interface GigabitEthernet 0/13
 switchport mode trunk
 storm-control broadcast
 storm-control multicast
 storm-control unicast
```

Step 2: Check the configurations of Switch B. Key points: whether storm control has been enabled on respective ports, and whether port protection has been enabled on the port directly connecting with users.

```
DES-7200#show running-config
vlan 3
!
interface GigabitEthernet 0/1
 switchport mode trunk
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/5
 switchport access vlan 3
 switchport protected
 storm-control broadcast
 storm-control multicast
 storm-control unicast
!
interface GigabitEthernet 0/9
 switchport access vlan 3
 switchport protected
 storm-control broadcast
 storm-control multicast
 storm-control unicast
```

Step 3: View address bindings on the ports of Switch A and ARP check enabling state.

```
DES-7200#show port-security all
Vlan Port  Arp-Check  Mac Address IP Address  Type remaining Age (mins)
---- -------- ---------- -------------- --------------
2    Gi0/5 Enabled  0000.0000.0001 1.1.1.1   Configured      -
2    Gi0/9 Enabled  0000.0000.0002 1.1.1.2   Configured     -
```

Step 4: View port security configurations on GigabitEthernet 0/5 of Switch B. Port security configurations on other ports won't be further introduced.

```
DES-7200#show interfaces gigabitEthernet 0/5 switchport
Interface   Switchport Mode    Access Native Protected VLAN lists
----------------------- ---------- --------- ------ ------
```

```
GigabitEthernet0/5 enabled ACCESS   3   1    Enabled   ALL
```

5.6 Limiting the Number of Access IPs on the Port

- Overview
- Default configurations to limit the number of access IPs on the port
- Configure the maximum number of access IPs on the port
- Display the number of access IPs on the port

5.6.1 Overview

DES-7200 switches support multiple access control applications (such as: IP Source Guard, port security, global IP+MAC binding and etc). These port access applications implement access control through the source IP address of the user in order to filter IP packets and prevent invalid users from using network resources.

The feature of limiting the number of access IPs on the port is intended to limit the number of access IPs bound by these secure access applications on the port, so as to limit the number of users sharing the port bandwidth of switch.

You can configure the number of IP addresses allowed to access network for each port. If the number of IP addresses bound by respective access applications on the port hasn't reached the configured threshold, the access applications shall be able to further bind and add valid users; if the number of IP addresses has reached the configured threshold, the access applications won't be able to further bind valid users.

If the number of IP addresses under the port has exceeded the configured threshold, the excessive IP addresses won't be allowed to pass through.

Caution

1. Limiting the number of access IPs on the port will take effect only if IP+MAC bindings or IP bindings of access control applications have taken effect. If no access application has been configured on the port (or if the port is the excluded port of global IP+MAC bindings), the limiting won't take effect.
2. When a same IP address is bound by IP+MAC binding and IP binding, it will be treated as two user IPs.
3. The access IP limiting only applies to IPv4 packets.
4. Except for the excluded port of global IP+MAC binding, the users added via global IP+MAC binding will be included into the number of IP addresses limited on each port.

5.6.2 Default Configurations to Limit the Number of Access IPs on the Port

The following table shows the default configurations to limit the number of access IPs on the port

Function	Default setting
Limiting the number of access IPs on the port	This feature is disabled on all ports. The default value is 0.

5.6.3 Configuring the Maximum Number of Access IPs on the Port

In privileged mode, configure the maximum number of access IPs on the port:

Command	Function
DES-7200# configure	Enter configuration mode
DES-7200(config)#interface interface-id	Enter interface mode
DES-7200(config-if)#nac-author-user maximum value	Configure the maximum number of access IPs on the port
DES-7200(config-if)**#no nac-author-user maximum**	Disable the maximum number of access IPs on the port

5.6.4 Displaying the Number of Access IPs on the Port

You can view the maximum number of access IPs configured on the port and the number of IP address bindings:

Command	Function
DES-7200**#show nac-author-user**	Display the maximum number of access IPs on the port and the number of IP address bindings.

As shown below:

```
DES-7200#show nac-author-user
 Port     Cur_num  Max_num
 --------  -------  -------
 Fa0/1    2        50
```

```
Fa0/2    0        0
Fa0/3    2        100
Fa0/4    0        0
Fa0/5    0        200
Fa0/6    0        0
Fa0/7    0        0
Fa0/8    0        0
```

6 URPF Configuration

6.1 Introduction to URPF

6.1.1 Overview

In recent years, frequent DOS (Denial of service) attacks caused by forged source address are bringing about many troubles to ISPs and network maintenance.

Fig. 1 shows a common scenario of using forged source address to perform DOS attacks:

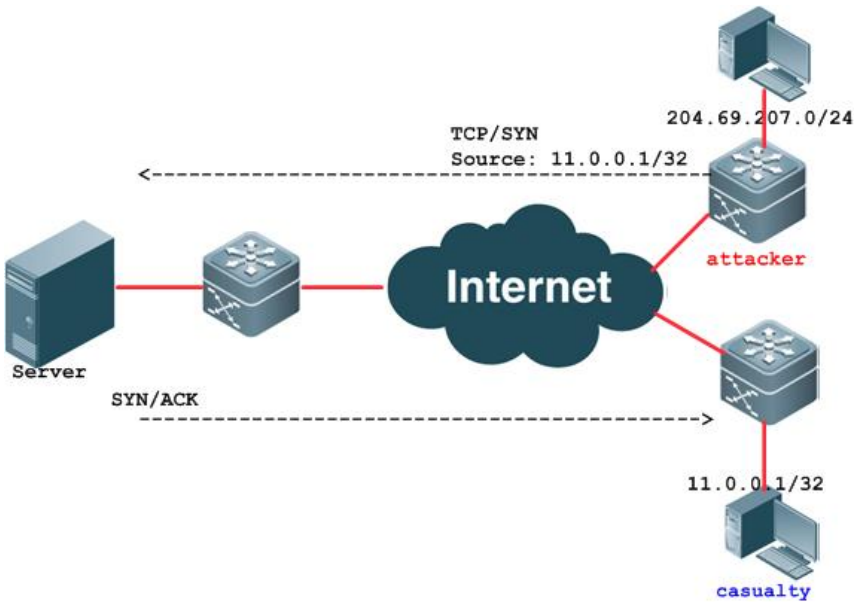


Fig 1 Scenario of source address based attacks

The attacker initiates attacks by sending messages with forged real source address of 11.0.0.1, making the server to send excessive SYN/ACK messages to the host unrelated to this attack, and the host with real source address is also affected. What's worse, if the network administrator identifies that this address is related to the attack on the network and discards all data streams from this source address, the denial of service to the source address is hence incurred.

The emergence of URPF (Unicast Reverse Path Forwarding) well addresses the above problem.

It is known that during message forwarding, the forwarding table is looked up according to the destination address contained in the IP message received, and the message is forwarded

according to the entry found in the forwarding table. URPF will look up the forwarding table according to source address and receiving interface of the incoming message. If the source address is not found in the forwarding table, then the message will be discarded; if the outgoing interface specified in the forwarding table doesn't match with the receiving interface of the message, then the message will also be discarded. Otherwise, the message will be forwarded.

URPF can protect the network by intercepting source address spoofing attacks.

6.1.2 Characteristics of URPF

6.1.2.1 Strict mode

Technical requirements of conventional URPF: URPF will look up the forwarding table according to source address and receiving interface of the incoming message. If the source address is not found in the forwarding table, then the message will be discarded; if the outgoing interface specified in the forwarding table doesn't match with the receiving interface of the message, then the message will also be discarded. This requires that the "receiving interface of the message received must be the outgoing interface of the route reaching this source address". We call such a URPF check mode as URPF strict mode.

Note	URPF strict mode is generally deployed on the point-to-point interface, and the data streams from both directions need to pass this point-to-point interface.

6.1.2.2 Loose mode

URPF strict mode has its limitations, and is particularly not applicable to the asymmetrical routing environment and multi-homed network environment.

Due to the need of network flow control and routing policy, asymmetrical routing is a commonly found network application. Fig 2 shows an example of asymmetrical routing. If G1/2 on R1 enables URPF strict mode and receives packets from the network segment of 192.168.20.0/24, URPF check will indicate the interface of G1/1 and the message will not be able to pass URPF check. The URPF strict mode will result in the loss of data streams.

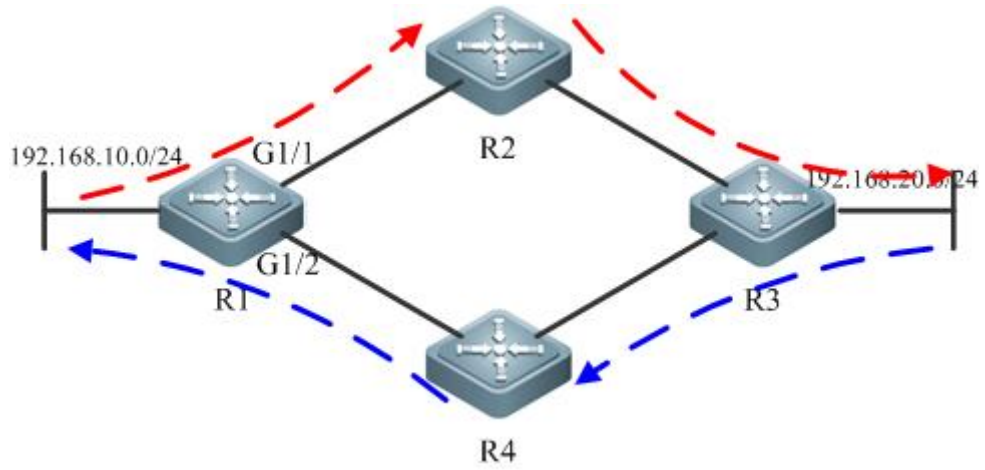


Fig 2 Asymmetrical routing

Multi-homed network is the common network application found between user and IPS or between ISPs. As shown in Fig 3, the user network A is simultaneously connected to multiple ISPs, and the incoming and outgoing streams are always asymmetrical. The figure shows that user network A is visiting user network B.

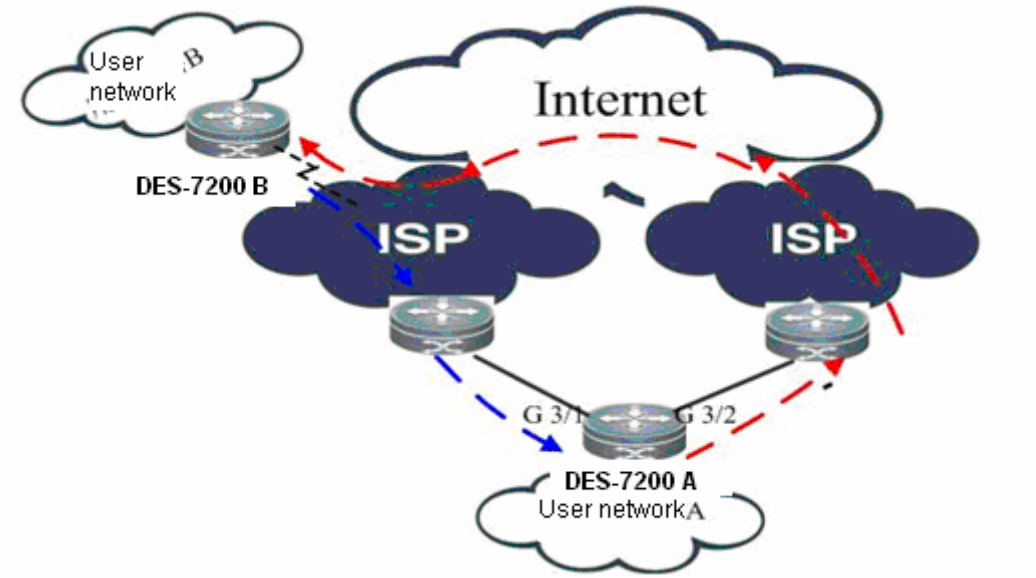


Fig 3 Multi-homed network

In the above two applications, valid messages will be filtered if URPF strict mode is enabled. Therefore, URPF loose mode is introduced.

URPF loose mode: Reverse route check is conducted according to the source IP of incoming message. As long as the route is found, the next-hop outgoing interface may not necessarily be the interface that receives the message. The introduction of URPF loose mode well solves the asymmetrical stream problem in the aforementioned asymmetrical routing application and multi-homed network.

6.1.2.3 URPF monitoring

In order to conveniently monitor the drop rate of messages after URPF is enabled, DES-7200 can inform the user of such drop rate via Syslog and Trap. The mechanism will be detailed in this section.

URPF monitoring has introduced the following concepts:

- Drop rate：The number of packets discarded due to URPF check within a specific period of time divided by this time. Unit: packets/second (pps).
- Drop rate computation interval: The time interval from the previous calculation of drop rate to the recalculation of drop rate.
- Drop rate sampling interval: The time interval for calculating the number of packets dropped. This value most not be smaller than drop rate computation interval.
- Drop rate notification threshold: The maximum drop rate allowed. When the drop rate is higher than this threshold, the user will be notified via Syslog or Trap. The user may also adjust the drop rate notification threshold according to actual situations of the network.
- Drop rate notify hold-down time: The time interval between two successive notifications. The user may adjust notify hold-down time according to actual situations of the network to avoid frequent Log printing or Trap sending.

The following figure describes two successive computations of drop rate:

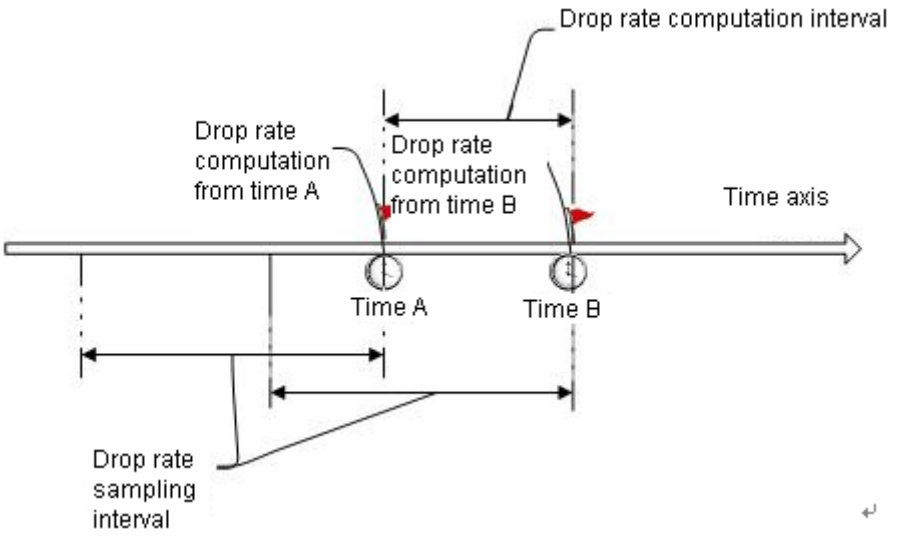


Fig 4 Two successive computations of drop rate

Main points of URPF monitoring:

- Drop rate computation

After URPF function is enabled, within the time interval of "0-drop rate sampling interval

(including the sampling time point reaching the drop rate)", the drop rate is calculated by dividing the currently calculated number of dropped packets by the time of URPF running. The subsequent method for drop rate computation: Calculated the number of currently dropped packets at every drop rate computation interval, deduct the number of dropped packets before the drop rate sampling interval, and then divide the difference by drop rate sampling interval to obtain the current drop rate.

- Interface-based and global-based drop rate computation and monitoring is allowed.

For configurations related to URPF monitoring, please refer to “Configure URPF drop rate notification”.

6.1.3 Operating principle

The operating principle of URPF has been described in the section of "Characteristics of URPF".

URPF functions can be applied to IPv4/IPv6 messages according to configurations. However, please note that the following messages will not be subject to URPF check.

URPF check is only applied to the source address with destination address being IPv4/IPv6 message, and those with destination address being multicast message will be skipped.

For DHCP/BOOTP messages with source IP address being 0.0.0.0 and destination IP address being 255.255.255.255, the URPF check will be skipped.

For IPv6 messages with source IP address being Link local address, the URPF check will be skipped.

6.1.4 Application restrictions

DES-7200 products which support URPF include:

Router products.

B-class line cards of DES-7200 series products and DES-7200-MPLS line cards.

The URPF function supported by our router products has the following application restrictions:

Router products only support URPF function during progress forwarding. If the fast forwarding is enabled on the interface (interface configuration mode: ip ref), the URPF function will be enabled.

URPF function also has the following characteristics in switch and router products:

After URPF is enabled, a route pointing source address to NULL interface will still be subject to URPF check instead of discarding.

After URPF is enabled, URPF will override ACL (interface configuration mode: ip access-group in) during packet check.

If URPF strict mode is enabled, incoming messages with source address being the address of receiving interface will be discarded. If URPF loose mode is enabled, such messages will pass the interface.

6.1.5 Protocol specification

Protocol specifications related to URPF include:

RFC 2827, Network Ingress Filtering: DDOS Attacks which employ IP Source Address Spoofing

RFC 3704, Ingress Filtering for Multi-homed Networks

6.2 Default configurations

The following table describes the default configurations of URPF.

Function	Default setting
URPF global configuration mode	Disabled
URPF interface configuration mode	Disabled
URPF drop rate monitoring	Disabled
URPF drop rate computation interval	30s
URPF drop rate sampling interval	URPF drop rate computation interval * 5
URPF drop rate notification threshold	1000pps
URPF drop rate notify hold-down time	300s
URPF Trap sent for drop rate notification	Disabled

6.3 Configure URPF functions

The following section describes how to configure the basic functions of URPF:

(Required) Configure URPF (global configuration mode)

(Required) Configure URPF (interface configuration mode)

(Optional) Configure URPF drop rate notification

View URPF configurations

6.3.1 Configure URPF (global configuration mode)

After MPLS line cards are inserted into DES-7200 series switches, messages will be forwarded via MPLS line cards. Please enable URPF function according to the following steps:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **ip verify unicast source reachable-via rx**	Enable URPF function **rx**: Use strict mode to perform URPF check
DES-7200(config)# **end**	Exit global configuration mode
DES-7200# **show ip urpf**	Display URPF configurations and statistics

To disable global URPF function, execute "no ip verify" command in the global configuration mode.

Caution	1. URPF function configured in the global configuration mode is only valid after MPLS line cards are inserted into DES-7200 series switches. After URPF function is enabled, URPF check will be applied to IPv4 messages. 2. URPF function configured in the global configuration mode only supports strict mode. If used with equal-cost routing, it will switch into loose mode. 3. URPF function configured in the global configuration mode doesn't support URPF check with default route. 4. Coexistence of URPF function configured in global configuration mode and URPF function configured in interface configuration mode is not supported. 5. Please note that: When DES-7200 series devices are directly linked to the network segment of user, it is not suggested to use URPF global configuration. If the directly link user intends to forward messages via DES-7200 series devices, the URPF check may fail as DES-7200 series devices haven't got the ARP entries of the directly link user and valid packets will be discarded.

Configuration example:

Enable URPF in global configuration mode:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# ip verify unicast source reachable-via rx
```

6.3.2 Configure URPF (interface configuration mode)

By default, URPF is not enabled on the interface. To enable URPF function on the interface, please follow the following steps:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **interface** *interface-name*	Access interface configuration mode
DES-7200(config-if)# **ip verify unicast source reachable-via** {**any** | **rx**} [**allow-default** | *acl_name*]	Enable URPF function **any:** use loose mode to perform URPF check **rx**：Use strict mode to perform URPF check **allow-default**：Allowing the use of default route to perform URPF check *acl-name*: ACL number, supporting: 1 to 99 (IP standard access list) 100 to 199 (IP extended access list) 1300 to 1999 (IP standard access list, expanded range) 2000 to 2699 (IP extended access list, expanded range)
DES-7200(config-if)# **end**	Exit interface configuration mode and return to privilege mode
DES-7200# **show ip urpf interface** *interface-name*	Display URPF configurations and statistics

 **Note**	1. By default, the default route is not used for URPF check; if so required by the user, the user can use "allow-default" to enable this function. 2. By default, messages failing in the URPF check will be discarded. If ACL (acl-name) is configured, such message will then undergo ACL check after failing in URPF check. If ACL doesn't exist or the message points to a deny ACE, such message will be discarded. If the message points to a permit ACE, the message will be forwarded.

 **Caution**	1. After this command is enabled, DES-7200 series devices will perform URPF check of IPv4/IPv6 messages. Routers will perform URPF check of IPv4 messages. 2. URPF function is only supported on Routed Port and L3 AP port of B-class line cards on DES-7200 series products, and has the following restrictions: ■ URPF function doesn't support ACL option. ■ URPF function doesn't support the use of IPv6 route with 65-127 bit prefix to perform URPF check. ■ After URPF function is enabled, all messages received by the physical port of these interfaces will be subject to URPF check, thus broadening the scope of URPF check. A typical application scenario is: If a message received by Tunnel interface is received from the aforementioned physical port, this message will also be subject to URPF check. If such an application scenario exists, be cautious when enabling URPF check. ■ After URPF function is enabled, the route forwarding capacity of the device will be reduced by 50%. ■ After URPF strict mode is enabled, if the messages received by the interface correspond with equal-cost routing during URPF check, it will switch into loose mode. ■ After MPLS line cards are inserted into DES-7200 series switches, the URPF function configured on the interface will not take effect. 3. Coexistence of URPF function configured in global configuration mode and URPF function configured in interface configuration mode is not supported.

Configuration example:

Perform strict URPF check of messages received by interface GigabitEthernet 0/21; no need to use default route for URPF check.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface gigabitEthernet0/21
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip verify unicast source reachable-via rx
```

6.3.3 Configure URPF drop rate notification

To configure URPF drop rate notification, you must enable URPF function first.

Configure URPF drop rate notification according to the following steps:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **ip verify urpf drop-rate compute interval** *seconds*	Configure URPF drop rate computation interval Unit: second; scope: 30-300; default: 30s
DES-7200(config)# **ip verify urpf drop-rate notify hold-down** *seconds*	Configure URPF drop rate notify hold-down time Unit: second; scope: 30-300; default: 300s
DES-7200(config)# **interface** *interface-name*	Enter interface configuration mode
DES-7200(config-if)# **ip verify urpf drop-rate notify**	Enable URPF drop rate monitoring
DES-7200(config-if)# **ip verify urpf notification threshold** *rate-value*	Configure URPF drop rate notification threshold Unit: pps; scope: 0-4294967295; default: 1000pps
DES-7200(config-if)# **exit**	Exit interface configuration mode and return to global configuration mode
DES-7200(config)# **snmp-server enable traps urpf**	Send Trap messages after the URPF drop rate has exceeded the notification threshold.
DES-7200(config)# **snmp-server host** {*host-addr*| **ipv6** *ipv6-addr*} **traps** *word* **urpf**	Configure the host to receive URPF Trap.
DES-7200(config)# end	Exit global configuration mode
DES-7200# **show ip urpf**	Display URPF configurations and statistics

Note	By default, the drop rate notification threshold is 1000pps. The user may adjust the drop rate notification threshold according to the actual situations of the network.

Caution	1. Drop rate monitoring is only effective in the interface configuration mode, and is not supported in the global configuration mode. 2. In the interface configuration mode, the drop rate will be calculated according to the messages dropped by the interface after URPF check is enabled.

Configuration example:

Perform strict URPF check of messages received by interface GigabitEthernet 0/21; no need to use default route for URPF check; monitor URPF drop rate via SNMP Trap; drop rate notification threshold is configured to 500pps; the SNMP host to receive Trap messages is 192.168.12.219.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# ip verify urpf notification threshold 500
DES-7200(config)# snmp-server enable traps urpf
DES-7200(config)# snmp-server host 192.168.12.219 public urpf
DES-7200(config)# interface gigabitEthernet0/21
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip verify unicast source reachable-via rx
```

6.3.4 View URPF configurations

URPF provides the following command to display various configurations and statistics.

Command	Function
show ip urpf [**interface** *interface-name*]	Display URPF configurations and statistics

Furthermore, URPF also provides the following commands to clear URPF statistical information:

Command	Function
clear ip urpf [**interface** *interface-name*]	Clear the statistics of packets dropped in URPF check

6.4 Typical URPF configuration example

6.4.1 Example of strict mode configuration

6.4.1.1 Networking requirements

Fig 5 shows an example of typical hierarchical network architecture.

In order to avoid messages with forged source address is transmitted from user PC to the core-layer network, it is expected that the source address attack messages are isolated in the access layer or distribution layer, so as to eliminate such invalid data on the distribution-layer and core-layer network.

By enabling URPF strict mode on the interface linking distribution-layer device and access-layer device, the aforementioned needs can be satisfied.

6.4.1.2 Network topology

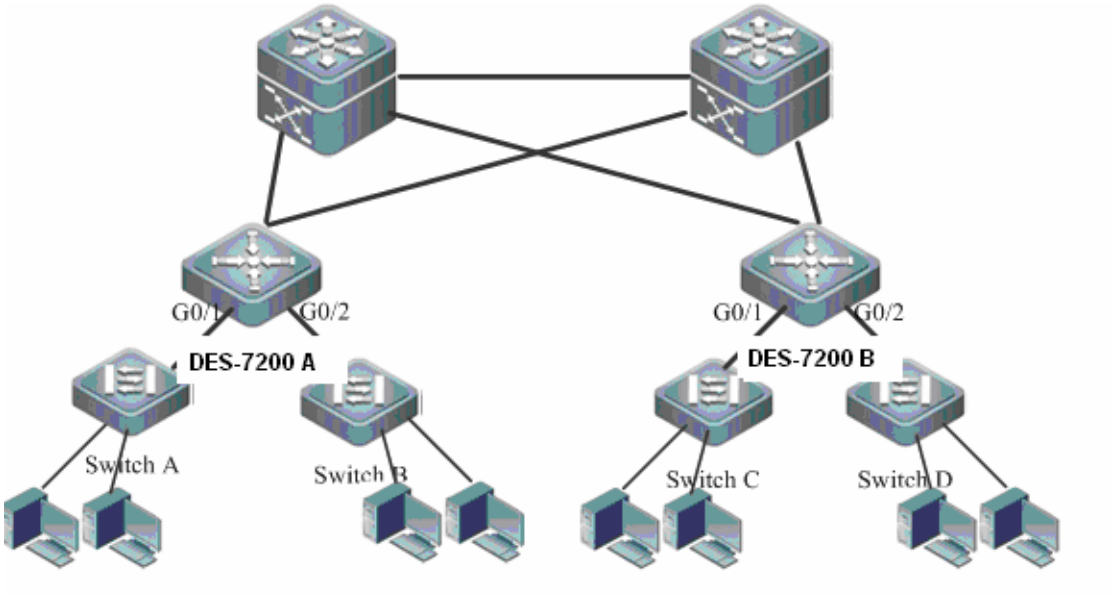


Fig 5 Application of URPF strict mode

6.4.1.3 Configuration steps

As shown in Fig 5, URPF strict mode is enabled on the distribution-layer device: enable URPF strict mode on device DES-7200 A and device DES-7200 B, as shown below:

Configurations of device DES-7200-A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
DES-7200(config)# interface gigabitEthernet0/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 195.52.1.1 255.255.255.0
DES-7200(config-if)# ip verify unicast source reachable-via rx
DES-7200(config-if)# ip verify urpf drop-rate notify
```

The configurations to enable URPF strict mode are same on interface G0/2 of DES-7200-A and G0/1 and G0/2 of DES-7200-B.

6.4.1.4 Verification

Check URPF configurations of device DES-7200-A

DES-7200 **#show ip urpf interface** *gigabitEthernet 0/1*

IP verify source reachable-via RX

IP verify URPF drop-rate notify enabled

IP verify URPF notification threshold is 1000pps

Number of drop packets in this interface is 124

Number of drop-rate notification counts in this interface is 0

6.4.2 Example of loose mode configuration

6.4.2.1 Networking requirements

The section of URPF loose mode describes the common application scenario of URPF loose mode, including asymmetrical routing environment and multi-homed network environment.

This section describes the configurations of outlet device connecting ISP in the multi-homed network as shown in Fig 3.

6.4.2.2 Network topology

See Fig 3: multi-homed network.

6.4.2.3 Configuration steps

As shown in Fig 3, on the outlet device of DES-7200-A in user network, in order prevent invalid messages from attacking the interior user network, URPF loose mode

is enabled on G3/1 and G3/2 connecting two ISPs, so as to isolate invalid messages outside the user network.

Configurations of device DES-7200-A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface gigabitEthernet3/1
DES-7200(config-if)# ip address 195.52.1.2 255.255.255.252
DES-7200(config-if)# ip verify unicast source reachable-via any
DES-7200(config-if)# ip verify urpf drop-rate notify
DES-7200(config-if)# exit
DES-7200(config)# interface gigabitEthernet3/2
DES-7200(config-if)# ip address 152.95.1.2 255.255.255.252
DES-7200(config-if)# ip verify unicast source reachable-via any
DES-7200(config-if)# ip verify urpf drop-rate notify
DES-7200(config-if)# end
```

6.4.2.4 Verification

Check URPF configurations of device DES-7200-A

DES-7200 #show ip urpf

IP verify URPF drop-rate compute interval is 300s

IP verify URPF drop-rate notify hold-down is 300s

Interface gigabitEthernet3/1

IP verify source reachable-via ANY

IP verify URPF drop-rate notify enabled

IP verify URPF notification threshold is 1000pps

Number of drop packets in this interface is 4121

Number of drop-rate notification counts in this interface is 2

Interface gigabitEthernet3/2

IP verify source reachable-via ANY

IP verify URPF drop-rate notify enabled

IP verify URPF notification threshold is 1000pps

Number of drop packets in this interface is 352

Number of drop-rate notification counts in this interface is 0

7 CPU Protection Configuration

7.1 Overview

7.1.1 Function of CPU Protect

Malicious attacks often occur in networks. By forging a large number of different management and protocol packets, these attacks make the switch too busy to deal with normal management and protocol packets, and thus affecting the security and the switch and the stability of the network at a large extent.

CPU Protect Policy (CPP) can effectively prevent malicious attacks in the network by packet identification and attack packet suppression, which can:

- Reduce the influence of attack packets on the switch (CPU protection)
- Enable load balance for the packets of different priority queues.

Meanwhile, CPP offers flexible configuration of packet policies for customized configuration based on real network environments.

7.1.2 Principles of CPU Protect

CPP adopts packet identification, packet bandwidth control, priority queue mapping and queue scheduling to protect CPU and key packets.

- Packet Identificatioin

Packet identification classifies all the packets sent to the switch for processing, for example, ARP, BPDU and GVRP and the alike (for details of data classification on various products, refer to Section CPU Protect Default Value).

- Packet Bandwidth Control

Administrator can configure bandwidth for each type of packets to suppress attack packets at high rate in the network.

- Priority Queue Mapping

Eight priority queues are supported. You can configure priority queue for each type of packets.

- Queue Scheduling

Poll scheduling algorithm is used to ensure that the protocol packets of different priority queues are sent to CPU for processing in time. Each queue is of the same scheduling weight.

7.2 Configuring CPU Protect

The following sections describe how to configure CPU Protect.

- CPU Protect Default Value
- Configuring the Bandwidth for Each Type of Packet
- Configuring the Priority Queue for Each Type of Packet

7.2.1 CPU Protect Default Value

The following lists the packet type identified by the switch and the default factory configurations. Use the command **no cpu-protected type** to restore the maximum bandwidth and priority setting of the packet to the default value.

- **DES-7200 Series**

Packet Type	Description	Bandwidth (pps)	Priority Queue
arp	ARP Packet	10000	3
bpdu	IEEE BPDU Packet	128	6
dhcp-relay-c	DHCP Relay function DHCP Client Packet	128	4
dhcp-relay-s	DHCP Relay function DHCP Server Packet	128	4
dhcps	DHCP Snooping function DHCP Packet	128	4
dot1x	802.1X EAPOL Packet	128	4
dvmrp	DVMRP Packet	128	5
gvrp	IEEE GVRP Packet	128	5
igmp	IGMP Packet	128	4
ip4-packet-local	Local IPV4 Packet	4096	0
ip4-packet-other	Other IPV4 Packet	200	0
ip6-packet-local	Local IPV6 Packet	4096	0
ip6-packet-other	Other IPV6 Packet	200	0
isis	ISIS Packet	128	5
mpls	MPLS Label Distribute Protocol(LDP) Packet	128	5

non-ip-packet-other	Other non-IP Packet	2048	0
option82	DHCP Option82 Packet	128	4
ospf	OSPF Packet	2000	5
ospf3	OSPF Version3 Packet	2000	5
pim	PIM IPV4 Packet	128	5
rerp	Rapid Ethernet Ring Protection protocol (RERP) Packet	128	6
reup	Rapid Ethernet Uplink Protection protocol(REUP) Packet	128	6
rip	IPV4 RIP Packet	128	5
ripng	IPV6 RIP Packet	128	5
rldp	Rapid Link Detection Protocol(RLDP) Packet	128	6
rldp-loop	RLDP Packet	128	6
slow_packet	IEEE SLOW Packet	128	6
tp_guard	Topology Protection Protocol(TPP) Packet	128	7
ttl0	IPV4 Packet with ttl=0	128	0
ttl1	IPV4 Packet with ttl=1	128	1
tunnel-bpdu	BPDU Tunnel Packet	128	5
tunnel-gvrp	GVRP Tunnel Packet	128	5
ipv4-icmp-local	ICMP-V4 Packet	1600	6
lacp	LACP Packet	128	4
udp-helper	UDP Helper function UDP Broadcast Packet	128	4
unknown-ipmc	Unknown IPV4 Multicast Packet	128	3
unknown-ipmcv6	Unknown IPV6 Multicast Packet	128	3
vrrp	VRRP Packet	128	6
vrrpv6	IPv6 VRRP Packet	128	6
dhcps6	IPv6 packets of DHCP IPv6 Snooping	128	4
dhcps6 client	IPv6 client packets of DHCP IPv6 Relay	128	4
dhcps6 server	IPv6 server packets of DHCP IPv6 Relay	128	4
mld	Multicast Listener Discovery packet	1000	4
nd-snp-ns-na	ND Snooping neighbor request and advertisement packet	10000	3

nd-snp-rs	ND Snooping router request packet	128	4
nd-snp-ra-redirect	ND Snooping router advertisement and redirection packet	128	4
hop_limit1	IPv6 Packet with Hop Limit=1	800	1
mpls_ttl0	MPLS Packet with TTL=0	128	1
mpls_ttl1	MPLS Packet with TTL=1	128	1

7.2.2 Configuring the Bandwidth for Each Type of Packet

In the configuration mode, configure the bandwidth of each type of packet by performing the following steps:

Command	Function
DES-7200(config)# **cpu-protect type** {**arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **err-ttl** | **unknown-ipmc** | **dvmrp | ...**} **pps** *pps_vaule*	Set the bandwidth for the packets in PPS, which is an integer.
DES-7200# **end**	Return to the privileged mode.

This example shows the bandwidth configuration process:

```
DES-7200(config)#cpu-protect type bpdu pps 200
Set packet type bpdu pps 100.
```

7.2.3 Configuring the Priority Queue for Each Type of Packet

In the configuration mode, configure the priority queue of each type of packet by performing the following steps:

Command	Function
DES-7200(config)# **cpu-protect type** {**arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **err-ttl** | **unknown-ipmc | ...**} **pri** *pri_vaule*	Set the priority queue for the packets, *pri_value* is an integer.
DES-7200# **end**	Return to the privileged mode.

This example shows the priority queue configuration process:

```
DES-7200(config)# cpu-protect type bpdu pri 7
Set packet type bpdu priority 7.
```

7.3 Viewing CPU Protect information

You can view the following information about the CPU Protect:

- View the statistics of the packets received by the CPU of the management board/single switch/stacking system
- View the statistics of the packets received by the CPU of the line card
- View the statistics of the specific type of the received packets
- View the summary of the CPP priority queue and bandwidth

7.3.1 Showing the Statistics of the Packets Received by the Management Board/Single Switch/Stacking System

In the privileged mode, show the statistics of the packets received by the CPU of the management board/single switch/stacking system by using the following commands:

Command	Function
DES-7200# **show cpu-protect mboard**	Show the statistics of the packets received by the management board/single switch/stacking system.

The following example shows how to show the CPP information of the management board:

```
DES-7200#show cpu-protect mboard
Type              Pps      Total    Drop
 ------------------- --------- --------- ---------
 tp-guard           0        0        0
 arp               0        13       0
 dot1x              0        0        0
 rldp               0        0        0
 rerp               0        0        0
 reup               0        0        0
 slow-packet         0        0        0
 bpdu               0        0        0
 isis               0        0        0
 dhcps              0        0        0
 gvrp               0        0        0
 ripng              0        0        0
 dvmrp              0        0        0
 igmp               0        0        0
 mpls               0        0        0
 ospf               0        0        0
 ospf3              0        0        0
 pim               0        0        0
 pimv6              0        0        0
 rip               0        0        0
```

```
vrrp              0       0       0
vrrp6             0       0       0
dhcps6            0       0       0
dhcp6_client      0       0       0
dhcp6_server      0       0       0
mld               0       0       0
nd-snp-ns-na      0       0       0
nd-snp-rs         0       0       0
nd-snp-ra-redirect  0       0       0
unknown-ipmc      0       0       0
unknown-ipmcv6    0       0       0
stargv-ipmc       0       0       0
stargv6-ipmc      0       0       0
bgp_ttl1          0       34      0
ttl1              0       0       0
hop_limit1        0       0       0
mpls-ttl1         0       0       0
ttl0              0       22      0
mpls-ttl0         0       0       0
dhcp-relay-c      0       0       0
dhcp-relay-s      0       0       0
option82          0       0       0
udp-helper        0       0       0
tunnel-bpdu       0       0       0
tunnel-gvrp       0       0       0
ip4-packet-local  0       156     0
ip6-packet-local  0       0       0
ip4-packet-other  0       5       0
ip6-packet-other  0       0       0
ipv6mc            0       15      0
non-ip-packet-other  0       0       0
```

7.3.2 Showing the Statistics of the Packets Received by the CPU of the Line Card

In the privileged mode, show the statistics of the packets received by the CPU of a specific line card by using the following commands:

Command	Function
DES-7200# **show cpu-protect slot** *slot_id*	Show the packets received by the CPU of a specific line card. *slot_id*: slot ID

The following example shows the CPU protection information of the line card in slot 2.

```
DES-7200(config)# show cpu-protect slot 2
 Type              Pps      Total    Drop
 ------------------- --------- --------- ---------
 tp-guard          0       0       0
 arp               0       3       0
 dot1x             0       0       0
 rldp              0       0       0
```

```
rerp                0        0        0
reup                0        0        0
slow-packet         0        0        0
bpdu                0        0        0
isis                0        0        0
dhcps               0        0        0
gvrp                0        0        0
ripng               0        0        0
dvmrp               0        0        0
igmp                0        0        0
mpls                0        0        0
ospf                0        0        0
ospf3               0        0        0
pim                 0        0        0
pimv6               0        0        0
rip                 0        0        0
vrrp                0        0        0
vrrp6               0        0        0
dhcps6              0        0        0
dhcp6_client        0        0        0
dhcp6_server        0        0        0
mld                 0        0        0
nd-snp-ns-na        0        0        0
nd-snp-rs           0        0        0
nd-snp-ra-redirect  0        0        0
unknown-ipmc        0        0        0
unknown-ipmcv6      0        0        0
stargv-ipmc         0        0        0
stargv6-ipmc        0        0        0
bgp_ttl1            0        0        0
ttl1                0        0        0
hop_limit1          0        0        0
mpls-ttl1           0        0        0
ttl0                0        0        0
mpls-ttl0           0        0        0
dhcp-relay-c        0        0        0
dhcp-relay-s        0        0        0
option82            0        0        0
udp-helper          0        0        0
tunnel-bpdu         0        0        0
tunnel-gvrp         0        0        0
ip4-packet-local    0        0        0
ip6-packet-local    0        0        0
ip4-packet-other    0        0        0
ip6-packet-other    0        0        0
ipv6mc              0        5        0
non-ip-packet-other 0        0        0
```

7.3.3 Showing the Statistics of the Specific Type of the Received Packets

In the privileged mode, show the priority queue and bandwidth of each type of packet by using the following commands:

Command	Function
DES-7200# **show cpu-protect type arp** | **bpdu** | **dhcp** | **ipv6mc** | **igmp** | **rip** | **ospf** | **vrrp** | **pim** | **ttl1** | **unknown-ipmc** | **dvmrp**	Show the statistics of the packets received by each type.

The following example shows the statistics of the arp packets by using the **show cpu-protec type arp** command:

```
DES-7200# show cpu-protect type arp
 Slot        Type          Pps       Total      Drop
 ---------   ------------ --------- ---------  ---------
 MainBoard   arp           200       15         0
 Slot-2      arp           200       15         0
```

7.3.4 Showing the Summary of CPP Priority Queue and Bandwidth

In the privileged mode, show the summary of priority queue and bandwidth by using the following commands:

Command	Function
DES-7200# **show cpu-protect summary**	Show the summary of the CPP priority queue and bandwidth.

The following example shows the summary of the CPP priority queue and bandwidth by using the **show cpu-protect summary** command:

```
DES-7200# show cpu-protect summary
Type              Pps      Pri
 ------------------- --------- ---------
 tp-guard          128      7
 arp               10000    3
 dot1x             128      4
 rldp              128      6
 rerp              128      6
 reup              128      6
 slow-packet       128      6
 bpdu              128      6
 isis              128      5
 dhcps             128      4
 gvrp              128      5
 ripng             128      5
```

```
dvmrp              128      5
igmp               1000     4
mpls               128      5
ospf               2000     5
ospf3              2000     5
pim                128      5
pimv6              128      5
rip                128      5
vrrp               128      6
vrrp6              128      6
dhcps6             128      4
dhcp6_client       128      4
dhcp6_server       128      4
mld                1000     4
nd-snp-ns-na       10000    3
nd-snp-rs          128      4
nd-snp-ra-redirect 128      4
unknown-ipmc       128      3
unknown-ipmcv6     128      3
stargv-ipmc        128      3
stargv6-ipmc       128      3
bgp_ttl1           128      1
ttl1               2000     1
hop_limit1         800      1
mpls-ttl1          128      1
ttl0               128      0
mpls-ttl0          128      1
dhcp-relay-c       128      4
dhcp-relay-s       128      4
option82           128      4
udp-helper         128      4
tunnel-bpdu        128      5
tunnel-gvrp        128      5
ip4-packet-local   4096     0
ip6-packet-local   4096     0
ip4-packet-other   200      0
ip6-packet-other   200      0
ipv6mc             128      0
non-ip-packet-other  4096     0
```

8 DoS Protection Configuration

8.1 DoS Protection Configuration

8.1.1 Overview

The DoS protection function can defend against Land attacks, invalid TCP message attacks and invalid L4 message attacks.

Land attack

The attacker sends a SYN packet to the destination host with the source address/port the same as the destination address/port and causes system crash while the attacked host attempts to establish a TCP link with itself (infinite loop).

Invalid TCP message attack

The header of TCP message contains several flag fields:

1. SYN: Connection flag. TCP SYN message sets this flag to 1 in order to request a connection.

2. ACK: Acknowledgment flag. In a TCP connection, except for the first message (TCP SYN), all other messages are set to be the acknowledgement to last message.

3. FIN: Finish flag. When a host receives a TCP message with FIN flag, it will terminate this TCP connection.

4. RST: Reset flag. When IP protocol stack receives a TCP message with nonexistent target port, it will reply a message with RST flag.

5. PSH: notifies the protocol stack to push up TCP data to the upper-layer program as soon as possible.

Invalid TCP message attack consumes host resources and leads to system crash by setting invalid flag fields. The followings are some frequently found invalid TCP messages:

1. TCP message with both SYN bit and FIN bit

Under normal conditions, SYN flag (connection request flag) and FIN flag (connection termination flag) cannot exist in the same TCP message, and RFC has no related stipulations on how IP protocol stack shall deal with such a deformed message. Therefore, the protocol stack of different operating systems will handle in different ways after receiving such a message. By utilizing this feature, the attacker sends a message with both SYN flag and FIN flag to identify the type of operating system, and initiate further attacks against the target operating system.

2. TCP message with no flag

Under normal conditions, any TCP message will contain at least one of SYN, FIN, ACK, RST and PSH flags. The first TCP message (TCP connection request message) will contain SYN flag, and the following messages will all contain ACK flag. Based on such an assumption, some protocol stack doesn't have the corresponding handling process for TCP message with no flag. Therefore, such a protocol stack may crash upon receipt of such a message. The attacker will utilize this feature to attach the target host.

3. TCP message with FIN flag but no ACK flag

Under normal conditions, except for the first message (SYN message), all other messages will contain the ACK flag, including TCP connection termination message (with FIN flag). However, some attackers may send a TCP message with FIN flag but no ACK flag to the target host, leading to the crash of target host.

Self-consumption attack

In this condition, the attacker sends the message with the same Layer-4 port number as the target host service to the target host, so that the target host sends the TCP request and connection to itself. This attack quickly exhausts the target host resources, even leads the system crash.

8.1.2 DoS Protection Configuration

8.1.2.1 Default DoS Protection Configuration

The default DoS protection configuration is given below:

Function	Default setting
land attack protection	Disabled
Invalid TCP message attack protection	Disabled
Self-consumption message attack protection	Disabled

8.1.2.2 Defending against Land attack

To enable Land attack protection function, run the following commands:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **ip deny land**	Enable Land attack protection function
DES-7200(config)# **end**	Return to privilege mode

8.1.2.3 Defending against invalid TCP message attack

To enable invalid TCP message attack protection function, run the following commands:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **ip deny invalid-tcp**	Enable invalid TCP message attack protection function
DES-7200(config)# **end**	Return to privilege mode

8.1.2.4 Defending against self-consumption message attack

To enable self-consumption message attack protection function, run the following commands:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **ip deny invalid-l4port**	Enable self-consumption message attack protection function
DES-7200(config)# **end**	Return to privilege mode

8.1.3 Displaying DoS Protection Status

8.1.3.1 Displaying Land attack protection status

To display Land attack protection status, run the following commands:

Command	Function

show ip deny land	Display Land attack protection status

The example below shows how to display the Land attack protection status:

```
DES-7200# show ip deny land
     DoS Protection Mode            State
-------------------------------------   -----
  protect against land attack           On
```

8.1.3.2 Displaying invalid TCP message attack protection status

To display invalid TCP message attack protection status, run the following commands:

Command	Function
show ip deny invalid-tcp	Display invalid TCP message attack protection status

The example below shows how to display the invalid TCP message attack protection status:

```
DES-7200# show ip deny invalid-tcp
     DoS Protection Mode             State
-------------------------------------   -----
  protect against invalid tcp attack        On
```

8.1.3.3 Displaying self-consumption attack protection status

To display self-consumption attack protection status, run the following commands:

Command	Function
show ip deny invalid-l4port	Display self-consumption attack protection status

The example below shows how to display the self-consumption attack protection status:

```
DES-7200# show ip deny invalid-l4port
     DoS Protection Mode             State
-------------------------------------   -----
  protect against invalid l4port attack  On
```

8.2 Ingress Filtering for DoS Attack Protection

8.2.1 Overview

In recent years, the spread of various DoS (Denial of Service) attack messages over Internet has brought about considerable troubles to Internet users. There are many kinds of DoS attacks, while the basic form of DoS attack utilizes valid service requests to occupy excessive service resources, thus making valid users unable to get service response. The attack messages will mainly disguise the source IP to avoid exposure.

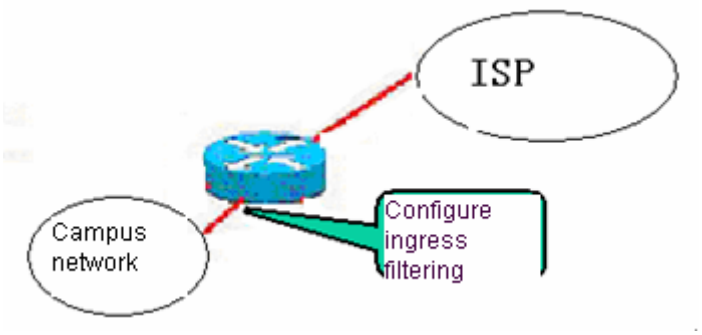
In regard to this, RFC2827 has proposed to set up Ingress Filtering at network access point to prevent messages with disguised source IP from accessing the network. Such an approach puts emphasis upon the early stage of attack and overall prevention of DoS attacks, and thus has satisfactory effects. Such filtering can also help ISP and network administrator to accurately locate the attackers using true and valid source IP addresses.

DES-7200 adopts RFC2827-based ingress filtering rules to defend against DoS attacks. The filtering is achieved through the automatic generation of specific ACLs by the switch itself, and will not pile any pressure on network forwarding.

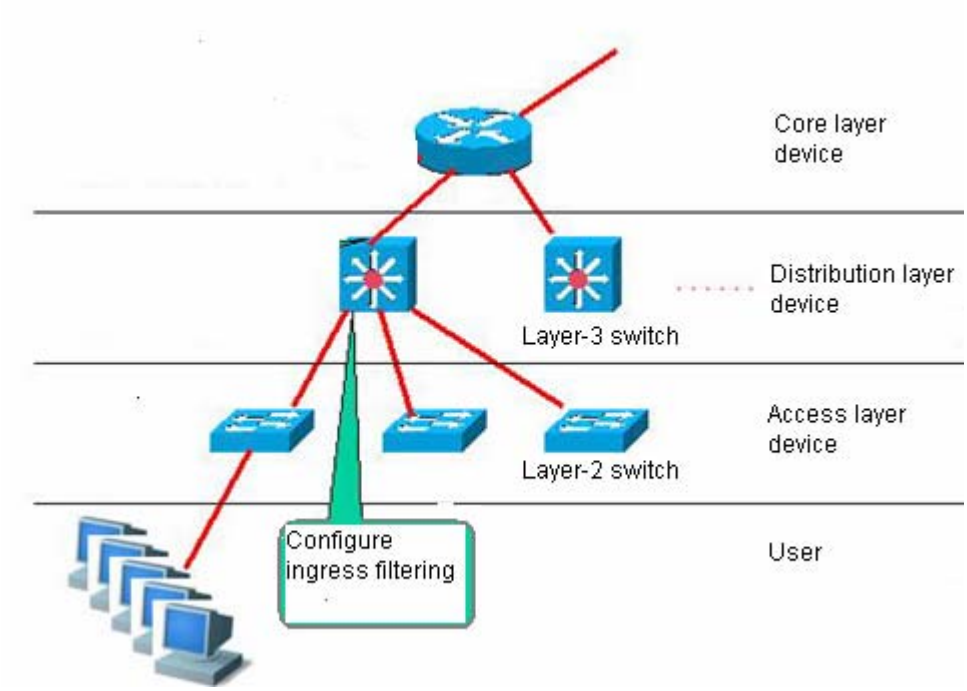
Of course, you can also use the address binding or Dot1x function of DES-7200 to achieve filtering effect, or by setting up ACLs.

8.2.2 Typical applications

A. ISP deploys ingress filtering on the access router to prevent messages with disguised source IP from accessing ISP and Internet:



B. The enterprise network (campus network) deploys ingress filtering on layer-3 switch to prevent messages with disguised source IP from accessing enterprise (campus) network:



8.2.3 Configuring Ingress Filtering to Defend Against DoS Attack

8.2.3.1 Default configuration

The ingress filtering for defending against DoS attacks is disabled on all network interfaces.

8.2.3.2 Precautions

Only layer-3 interfaces with network address can support ingress filtering for defending against DoS attacks.

By enabling defeat DoS based ingress filtering on the designated layer-3 interface, the system will automatically establish the corresponding ACL for the network interface to restrict the access of disguised source IP, and apply the ACL to the ingress of layer-3 interface.

For example: The network address on SVI 1 is 192.168.5.1/24. If “ip deny spoofing-source” is configured in the interface configuration mode, the following ACL will be generated automatically and applied to this interface.

```
permit 192.168.5.0 0.0.0.255
permit host 0.0.0.0 (This ACE permits the access of DHCP requests with source address being 0.0.0.0)
deny any
```


Caution

- This filtering can only be configured on the direct link interface. Apply ingress filtering on convergence-layer interface (uplink port) will prevent Internet messages with various source IP addresses from reaching the downlink hosts at the convergence layer.
- After configuring DoS protection based ingress filtering, the no command must be used to disable DoS protection function in order to modify the address of network interface.

8.2.4 Set up Ingress Filtering to Defend Against DoS Attack

To set up ingress filtering, run the following commands:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter layer-3 interface
DES-7200(config-if)# **ip deny spoofing-source**	Ingress filtering function to defend against disguised source IP based DoS attacks. Drop all incoming messages without consistent prefix with this network interface. (Note: Only layer-3 interface can be configured with this function)
DES-7200(config-if)# **show running interface** *interface-id*	Verify the configuration of ingress filtering.

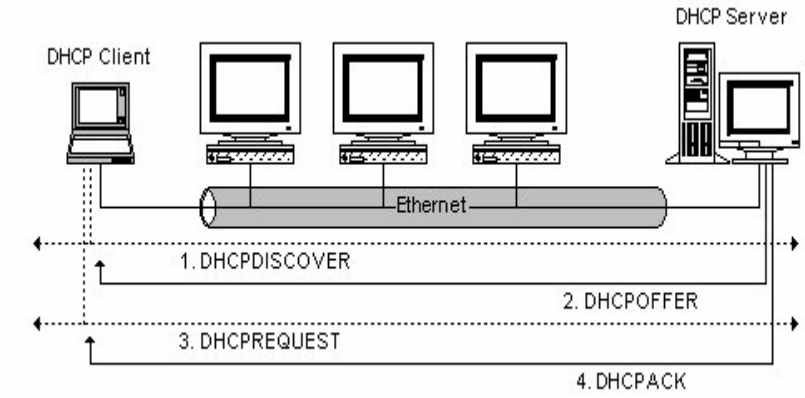
Use the **no ip deny spoofing-source** command to disable the ingress filtering function (for DoS attack protection) in the interface configuration mode.

9 DHCP Snooping Configuration

9.1 Overview

9.1.1 Understanding DHCP

The DHCP protocol is widely used to dynamically allocate the recycled network resources, for example, IP address. A typical IP acquisition process using DHCP is shown below:



The DHCP Client sends a DHCP DISCOVER broadcast packet to the DHCP Server. The Client will send the DHCP DISCOVER again if it does not receive a response from the server within a specified time.

After the DHCP Server receives the DHCP DISCOVER packet, it allocates resources to the Client, for example, IP address according to the appropriate policy, and sends the DHCP OFFER packet.

After receiving the DHCP OFFER packet, the DHCP Client sends a DHCP REQUEST packet to obtain the server lease and notify other servers of receiving the address allocated by the server.

After receiving the DHCP REQUEST packet, the server verifies whether the resources are available. If so, it sends a DHCP ACK packet. If not, it sends a DHCP NAK packet. Upon receiving the DHCP ACK packet, the DHCP Client starts to use the resources assigned by the server in condition that the ARP verification resources are available. If it receives the DHCP NAK packet, the DHCP Client will send the DHCP DISCOVER packet again.

9.1.2 Understanding DHCP Snooping

DHCP Snooping monitors users by snooping the packets exchanged between the clients and the server. DHCP Snooping can filter DHCP packets and illegal servers by proper configuration. Some terms and functions used in DHCP Snooping are explained below:

DHCP Snooping TRUST port: Because the packets for obtaining IP addresses through DHCP are in the form of broadcast, some illegal servers may prevent users from obtaining IP addresses, or even cheat and steal user information. To solve this problem, DHCP Snooping classifies the ports into two types: TRUST port and UNTRUST port. The device forwards only the DHCP reply packets received through the TRUST port while discarding all the DHCP reply packets from the UNTRUST port. In this way, the illegal DHCP Server can be shielded by setting the port connected to the legal DHCP Server as a TRUST port and other ports as UNTRUST ports.

DHCP Snooping binding database: By snooping the packets between the DHCP Clients and the DHCP Server, DHCP Snooping combines the IP address, MAC address, VID, port and lease time into a entry to form a DHCP Snooping user database.

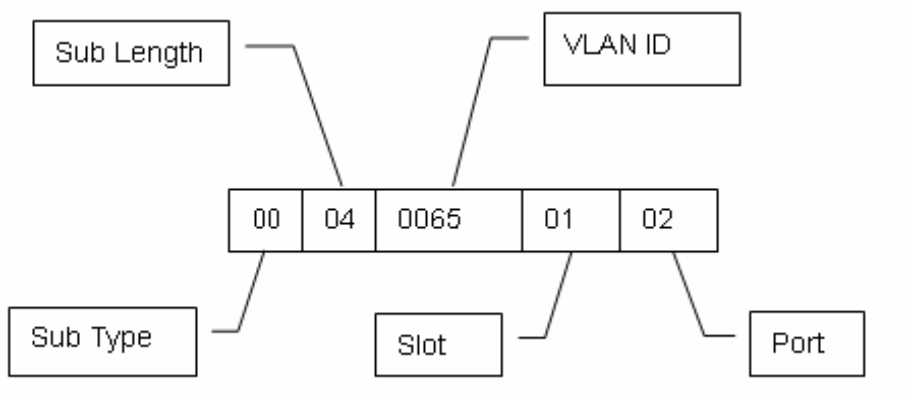
DHCP Snooping checks the validity of DHCP packets that pass through the device, discards illegal DHCP packets, and records user information to create a DHCP Snooping binding database for ARP inspection and query. The following DHCP packets are considered illegal:

- The DHCP reply packets received on the UNTRUST ports, including DHCPACK, DHCPNACK, DHCPOFFER, etc.
- DHCP Client values in the source MAC and DHCP packets are in different packets when MAC check is enabled.
- DHCPRELEASE packets whose port information is inconsistent with that in the the DHCP Snooping binding database.

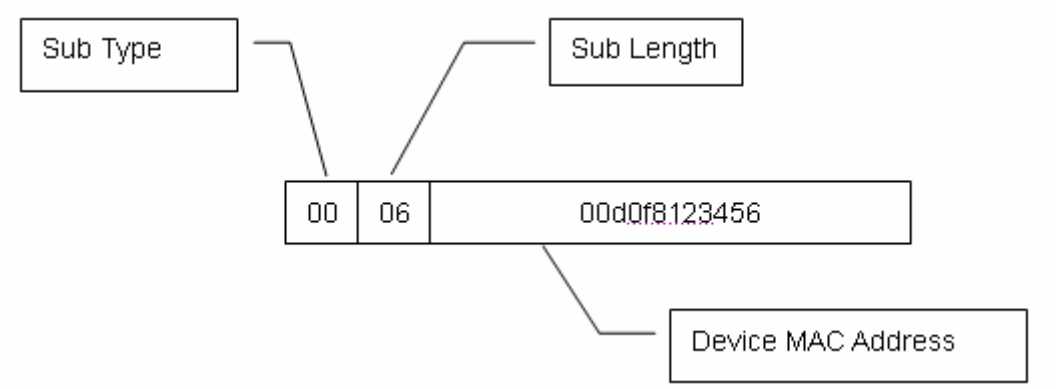
9.1.3 Understanding DHCP Snooping Information Option

Some network administrators want to assign IP address to current users upon their positions. That is, they want to assign IP addresses to users according to the information on the network equipments that users connect so that the switch can add the user-related device information to the DHCP request packet in DHCP option way while performing DHCP Snooping. According to RFC3046, the option number used is 82. You can obtain more user information by uploading option82 to the content server. As a result, you can assign IP addresses accurately. The format of option82 uploaded by DHCP Snooping is shown as follows:

Agent Circuit ID



Agent Remote ID



9.1.4 DHCP Snooping Related Security Functions

In the DHCP-enabled network, the general problem facing administrator is that some users use private IP addresses rathe than dynamically obtaining IP addresses. As a result, some users using dynamic IP addresses cannot access the network, making network application more complex. In dynamic DHCP binding mode, the device records how legal users obtain IP addresses during the course of DHCP Snooping for security purpose. There are three ways of security control. The first one is to enable address binding for legal users in conjunction with the IP Source Guard function; the second one is to use DAI to check the validity of users by controlling ARP; the third one is to bind the ARP message of legal users in conjunction with the ARP Check function. It should be noted that given the limit of hardware entries in the first mode, the switch supports limited DHCP users. Where there are too many users on the switch, some legal users may not access the network for they cannot add hardware entries. In addition, the second method will influece the performance of the switch at a large extent, because all ARP messages are forwarded and processed by CPU.

For the details on the priorities of DHCP Snooping and other security functions, refer to *Port*

Security White Paper and *Security Function Depolyment White Paper*.

9.1.5 Understanding DHCP Snooping and IP Source Guard

The IP Source Guard function maintains an IP source address database. By setting the user information of the database (IP and MAC) to be the hardware filtering entry, it allows the corresponding users to access the network. For details, refer to IP Source Guard Configuration.

By snooping the DHCP process, the DHCP Snooping maintains a user IP address database and offers it to the IP Source Guide funciton for filtering so that only the users dynamically obtaining IP address can access the network.

Furthermore, the DHCP binding filters IP packets rather than ARP messages. To enhance security and prevent from ARP Spoofing, check the ARP validity of DHCP bound users. For more information, refer to *DAI Configuration*.

9.1.6 Understanding DHCP Snooping and ARP Inspection

ARP Inspection checks all the ARP messages travelling through the switch. DHCP Snooping needs to offer the database information for ARP Inspection to use. After receiving an ARP message, the DAI-enabled swtich queries the database bound by the DHCP Snooping. The ARP message is learned and forwarded only when its source MAC, source IP and port are matched or otherwise it is dropped.

9.1.7 Understanding DHCP Snooping and ARP Check

As with ARP Inspection, ARP Check checks all the ARP messages travelling through the switch. DHCP Snooping needs to offer the database information for ARP Check to use. After receiving an ARP message, the ARP Check-enabled swtich queries the database bound by the DHCP Snooping. The ARP message is learned and forwarded only when its source MAC, source IP and port are matched or otherwise it is dropped.

9.1.8 Other Precautions on DHCP Snooping Configuration

The DHCP Snooping function and the DHCP Option82 function of 802.1xare mutually exclusive. That is, you can not enable the DHCP Snooping function and the DHCP Option82 function of 802.1x at the same time.

DHCP Snooping snoops only the DHCP process of users. ARP Inspection is necessary to restrict users to use the IP address assinged by the DHCP protocol for Internet access. However, ARP Inspection needs to check all ARP messages, which will influence the overall performance of the switch.

When the DHCP client with Hybrid interface connects to the DHCP Server through untagged VLAN, the share VLAN should be enabled and the untagged VLAN should be set to be share VLAN. For the number of share VLANs supported, refer to Section *Share VLAN Configuration* of *Configuration Guide*.

9.2 DHCP Snooping Configuration

9.2.1 Enabling and Disabling DHCP Snooping

The DHCP Snooping function of the device is disabled by default. To enable DHCP Snooping and then monitor DHCP packets, execute the following command.

Command	Function
DES-7200**# configure terminal**	Enter the global configuration mode.
DES-7200(config)**# [no] ip dhcp snooping**	Enable or disable DHCP snooping.

The following example demonstrates how to enable the DHCP snooping function of the device:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping
DES-7200(config)# end
```

Caution

DHCP Snooping and Private VLAN function cannot enabled at the same time.

9.2.2 Enabling Filtering the DHCP Request Message on the Port

By default, filtering the DHCP request message is disabled on the port. To enable this funciton, execute the following command.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface*	Enter the interface configuration mode.
DES-7200(config)# [**no**] **ip dhcp snooping suppression**	Enable or disable filtering the DHCP request message.

The following example demonstrates how to enable filtering the DHCP request message:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip dhcp snooping suppression
```

9.2.3 Enabling DHCP Snooping in VLAN

This command enables DHCP Snooping in the VLAN.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# [**no**] **ip dhcp snooping vlan** {*vlan-rng* | {*vlan-min* [*vlan-max*]}}	Enable DHCP Snooping in the VLAN.

Here is an example of enabling the DHCP Snooping in VLAN1000:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping vlan 1000
DES-7200(config)# end
```

9.2.4 Configuring DHCP Source MAC Address Check Function

After configuring this command, the device will match the MAC address of the DHCP Request packet from the UNTRUST port against the one in the client field and discard unmatched packet. By default, this funciton is not enabled.

To configure the source MAC address check function, execute the following command:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# [**no**]**ip dhcp snooping verify mac-address**	Enable or disable the source MAC address check function.

The following example shows how to enable the DHCP source MAC address check function:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping verify mac-address
DES-7200(config)# end
```

9.2.5 Configuring DHCP Snooping Information Option

By default, this function is disabled. After configuring this command, when DHCP Snooping forwards the packets, option82 will be added to all DHCP request packets and removed from all reply packets.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# [**no**] **ip dhcp snooping Information option**	Enable or disable the DHCP snooping information option.

The following configuration enables DHCP snooping information option:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping information option
DES-7200(config)# end
```

Caution

After this function is configured, DHCP relay option82 function configured on the device will be ineffective.

9.2.6 Writing the DHCP Snooping Database to Flash Periodically

By default, this function is disabled. DHCP Snooping provides a command to write the DHCP Snooping database to the flash periodically in order to prevent loss of DHCP user information

when the device restarts due to an electricity failure.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# [**no**] **ip dhcp snooping database write-delay** [*time*]	Specify the interval at which the switch writes the DHCP database to the flash. *time*: 600s to 86400s. The default value is 0.

The following example sets the interval at which the switch writes the DHCP databse to the flash to 3600s:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping database write-delay 3600
DES-7200(config)# end
```

Caution

You need to set a proper time for writing to the flash since erasing and writing to the flash frequently shortens its life. A shorter time helps to save the device information more effectively. A longer time reduces the times of writing to the flash and increases service life of flash.

9.2.7 Writing DHCP Snooping Database to Flash Manually

To prevent loss of DHCP user information when the device restarts due to an electricity failure, the administrator can write the DHCP Snooping binding database to the flash manually.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip dhcp snooping database write-to-flash**	Write the DHCP Snooping binding database to the flash manually.

The following example demonstrates how to write the DHCP Snooping binding database to the flash:

```
DES-7200# configure terminal
DES-7200(config)# ip dhcp snooping database write-to-flash
DES-7200(config)# end
```

9.2.8 Configuring a Port as a TRUST Port

By default, all the ports are UNTRUST ports. After configuring this command, a port is set as the TRUST port and connected to the legal DHCP server.

Command	Function

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# [**no**] **ip dhcp snooping trust**	Set the port as a trust port.

The following example shows how to set GigabitEthernet 4/1 as a TRUST port:

```
DES-7200# configure terminal
DES-7200(config)# interface GigabitEthernet 4/1
DES-7200(config-if)# ip dhcp snooping trust
DES-7200(config-if)# end
```

9.2.9 Configuring Rate of Receiving DHCP Packet

This command configures rate of receiving DHCP in the corresponding interface:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# [**no**] **ip dhcp snooping limit rate** *rate-value*	Configures rate of receiving DHCP packet on the port.

The following example shows how to set the rate of receiving DHCP packet on GigabitEthernet 4/1 as 100pps:

```
DES-7200# configure terminal
DES-7200(config)# interface GigabitEthernet 4/1
DES-7200(config-if)# ip dhcp snooping limit rate 100
DES-7200(config-if)# end
DES-7200# show ip dhcp snooping
Switch DHCP snooping  status                 :   ENABLE
DHCP snooping  Verification of hwaddr field status   :   DISABLE
DHCP snooping database write-delay time       :   0 seconds
DHCP snooping option 82 status               :   ENABLE
DHCP snooping Support Bootp bind status      :   ENABLE

Interface                  Trusted      Rate limit (pps)
------------------------      -------      ----------------
GigabitEthernet 4/1          NO                    100
```

9.2.10 Clearing Dynamic User Information from the DHCP Snooping Binding Database

To clear dynamic user information from the DHCP Snooping binding database, execute the following command.

Command	Function
DES-7200# **clear ip dhcp snooping binding**	Clear information from the current database.

The following example shows how to clear information from the current database manually:

```
DES-7200# clear ip dhcp snooping binding
```

9.3 Showing DHCP Snooping Configuration

9.3.1 Showing DHCP Snooping

To show DHCP Snooping, execute the following command:

Command	Function
DES-7200# **show ip dhcp snooping**	Show the configuration of DHCP snooping.

For example:

```
DES-7200# show ip dhcp snooping
Switch DHCP snooping  status                    :   ENABLE
DHCP snooping  Verification of hwaddr field status   :   DISABLE
DHCP snooping database write-delay time         :   0 seconds
DHCP snooping option 82 status            :   ENABLE
DHCP snooping Support Bootp bind status    :   ENABLE
Interface                  Trusted      Rate limit (pps)
------------------------      -------      ----------------
GigabitEthernet 4/1          NO                     100
```

9.3.2 Showing the DHCP Snooping Database

To show the DHCP Snooping database, execute the following command:

Command	Function
DES-7200# **show ip dhcp snooping binding**	View the user information in the DHCP Snooping binding database.

For example:

```
DES-7200# show ip dhcp snooping binding
Total number of bindings: 1
MacAddress       IpAddress      Lease(sec)   Type         VLAN  Interface
------------------ --------------- ------------ ------------- -----
--------------------
001b.241e.6775       192.168.12.9      863996           dhcp-snooping  1
GigabitEthernet 0/5
```

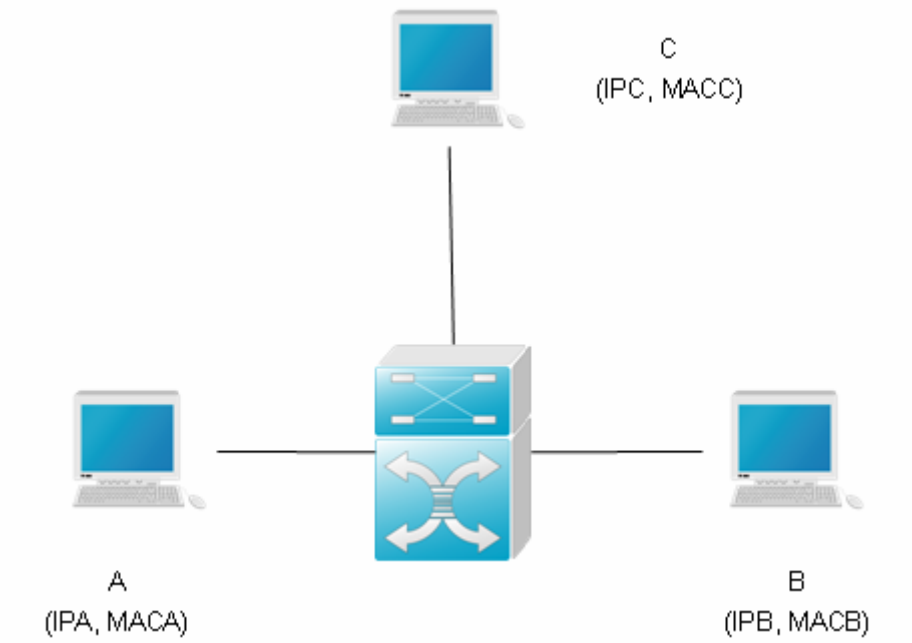
10 Dynamic ARP Inspection Configuration

10.1 Overview

DAI, an acronym of Dynamic ARP Inspection, refers to inspect the validity of received ARP packets. Illegal ARP packets will be discarded.

10.1.1 Understanding ARP Spoofing Attack

ARP itself does not check the validity of incoming ARP packets, a drawback of ARP. In this way, attackers can launch ARP spoofing attacks easily by exploiting the drawback of the protocol. The most typical one is the man in the middle attack, which is described as follows:



As shown in the diagram, devices A, B and C are connected to DES-7200 device and located in the same subnet. Their IP and MAC addresses are respectively represented by (IPA, MACA), (IPB, MACB) and (IPC, MACC). When device A needs to communicate with device B in the network layer, device A broadcasts an ARP request in the subnet to query the MAC value of device B. Upon receiving this ARP request packet, device B updates its ARP buffer using IPA and MACA, and sends an ARP response. Upon receiving this response, device A

updates its ARP buffer using IPB and MACB.

With this model, device C will cause the corresponding relationship of ARP entries in device A and device B incorrect. The policy is to broadcast ARP response to the network continuously. The IP address in this response is IPA/IPB, and the MAC address is MACC. Then, ARP entries (IPB and MACC) will exist in device A, and ARP entries (IPA and MACC) exist in device B. Communication between device A and device B is changed to communication with device C, which is unknown to devices A and B. Device C acts as an intermediary and it just modifies the received packets appropriately and forwards to another device. This is the well-known man in the middle attack.

10.1.2 Understanding DAI and ARP Spoofing Attacks

DAI ensures that only legal ARP packets are forwarded by the device. It mainly performs the following operations:

- Intercept all the ARP request and response packets at the untrusted port that corresponds to VLAN with the DAI inspection function enabled.
- Check the validity of the intercepted ARP packets according to the setting of DHCP database before further processing.
- Drop the packets that do not pass the inspection.
- Appropriately process the packets that pass the inspection and send them to the destinations.

According to the DHCP snooping binding database, whether ARP packets is valid or not can be checked . For details, refer to *DHCP Snooping Configuration*.

10.1.3 Interface Trust Status and Network Security

ARP packets are checked according to the trust status of each port on the device. DAI check is ignored for the packets that are received through trust ports and are considered as legal ARP packets. DAI check will be performed strictly for the ARP packets that are received through untrusted ports.

In a typical network configuration, layer 2 port connected to the network device should be set as a trust port, and layer 2 port connected to the host device should be set as an untrusted port.

Note

Incorrectly configuring a layer 2 port as an untrusted port may affect normal communication of the network.

For specific configuration commands, refer to *ip arp inspection trust, show ip arp inspection interface.*

10.1.4 Limiting the Rate of ARP Packets

Checking DAI validity will consume a certain CPU resources. Limiting the rate of ARP packets, namely the number of ARP packets received per second, can efficiently prevent the DAI-specific DoS attack. By default, 15 ARP packets are received on an untrusted port per second. This limit does not apply to a trusted port. You can configure rate limit with the **ip arp inspection limit-rate** command on the Layer 2 interface configuration mode.

For details, refer to **ip arp inspection limit-rate** and **show ip arp inspection interface.**

10.2 Configuring DAI

DAI is an **ARP**-based security filtering technology. A series of filtering policies are configured, so that validity of ARP packets that pass the device is checked more effectively.

To use the functions of DAI, selectively perform the following tasks:

- Enabling DAI Packet Check Function for Specified VLAN (required)
- Set Trust Status of Port (optional)
- Set the Maximum Rate of Receiving ARP Packets on the Port(Optional)
- Related Configuration of DHCP Snooping Database (optional)

10.2.1 Enabling DAI Packet Check Function for Specified VLAN

By default, the DAI packet check function is disabled for all VLANs.

If no DAI packet check function has enabled VLAN vid, DAI-related security check will be skipped for the ARP packets with vlan-id = vid (ARP packet rate restriction is not skipped).

Use the **show ip arp inspection vlan** command to check whether the DAI packet check function has been enabled for all VLANs.

To configure the DAI packet check function for VLAN, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config)# **ip arp inspection vlan** *vlan-id*	Turn on the DAI packet check function switch for VLAN *vlan-id*

Command	Function
DES-7200(config)**# no ip arp Inspection vlan** [*vlan-id*]	Turn off the DAI packet check function switch for VLAN *vlan-id* Disable the DAI packet check function for all VLANs if *vlan-id* is ignored

10.2.2 Setting the Trust Status of Port

This function is used in the layer 2 interface configuration mode, and this layer 2 interface is a member port of SVI.

All the layer 2 ports are untrusted by default.

If the port is trusted, ARP packets will not be check further. Otherwise, the validity of the current ARP packet will be checked using information in the DHCP snooping database.

To set the trust status of a port, execute the following commands in the interface configuration mode:

Command	Function
DES-7200(config-if)**# ip arp inspection trust**	Set the port as a trust port.
DES-7200(config-if)**# no ip arp inspection trust**	Set the port as an untrusted port.

10.2.3 Related Configuration of DHCP Snooping Database

Refer to *DHCP Snooping Configuration*.

If DHCP Snooping database is not configured, all the ARP packets pass inspection.

10.3 Showing DAI Configuration

10.3.1 Showing Whether DAI Function Is Enabled for VLAN

To show the enabling status of VLAN, execute the following command in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **show ip arp inspection vlan**	Show the enabling status of each VLAN

10.3.2 Showing DAI Configuration Status of Each Layer 2 Interface

To show the DAI configuration status of each layer 2 interface, execute the following command in the global configuration mode:

Command	Function
DES-7200(config)# **show ip arp inspection interface**	Show the DAI configuration of each layer 2 interface (including trust status and rate restriction)

For the products supporting NFPP, rate limit is done by NFPP, not DAI. Consequently, this command shows only the trust status of an interface.

10.4 Precautions of Configuring the Rate of ARP Packets

Caution

In the single-device environment, when the CPU is busy, the rate of sending ARP packets is limited to appropriately 150PPS~380PPS, even if the rate oversizely exceeds the rate limitation. The deviation of the rate value may occur in different environment.

In the stack environment, when the CPU of the backup device is busy, the rate of sending ARP packets on the port is appropriately a dozon PPS with the rate limit configured.

10.5 Typical DAI Configuration Example

10.5.1 Topological Diagram

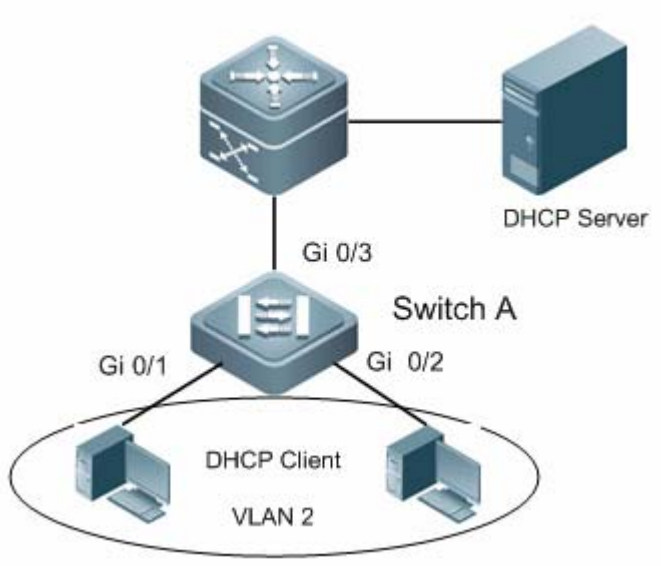


Figure2 DHCP deployment environment

10.5.2 Application Requirements

As shown above, the IP address of user PC is automatic allocated by the DHCP server. To ensure that users can access network normally, the following requirements must be met:

1. User PC can only acquire IP address from the specified DHCP server, and no additional DHCP server is allowed.
2. Only the IP address allocated by the valid DHCP server can access network, and IP address cannot be configured at will.

10.5.3 Configuration Tips

- **Configuration tips**

1. On the access switch (SwitchA), enable DHCP Snooping and configure the uplink port (GigabitEthernet 0/3) connecting valid DHCP server as the trusted port to meet the first requirement.
2. On the access switch (SwitchA), further enable DAI to meet the second requirement.

- **Note**

If the convergence switch or core switch is connected with other PCs and there may be a private DHCP server, DHCP Snooping shall also be enabled.

10.5.4 Configuration Steps

- **Configure Switch A**

Step 1: Configure the VLAN to which the PC-connecting port belongs.

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface range gigabitEthernet 0/1-2
DES-7200(config-if-range)#switchport access vlan 2
```

Step 2: Enable DHCP Snooping.

```
DES-7200(config-if-range)#exit
DES-7200(config)#ip dhcp snooping
```

Step 3: Enable DAI on the corresponding VLAN.

```
DES-7200(config)#ip arp inspection vlan 2
```

Step 4: Configure the uplink port as the trusted port of DHCP Snooping

```
DES-7200(config)#interface gigabitEthernet 0/3
DES-7200(config-if-GigabitEthernet 0/3)#ip dhcp snooping trust
```

Step 5: Configure the uplink port as the trusted port of DAI.

```
DES-7200(config-if-GigabitEthernet 0/3)#ip arp inspection trust
```

10.5.5 Verifications

Step 1: Verify whether the configurations are correct. Key points: whether DHCP Snooping/DAI has been enabled, and whether the trusted port is correct.

```
DES-7200#show running-config
ip dhcp snooping
!
ip arp inspection vlan 2
!
interface GigabitEthernet 0/1
 switchport access vlan 2
!
interface GigabitEthernet 0/2
 switchport access vlan 2
!
interface GigabitEthernet 0/3
ip dhcp snooping trust
ip arp inspection trust
```

Step 2: View DHCP SNOOPING enabling state and the corresponding trusted port.

Key point: whether the uplink port has been configured as the trusted port.

```
DES-7200#show ip dhcp snooping
Switch DHCP snooping  status                :   ENABLE
DHCP snooping  Verification of hwaddr status   :   DISABLE
DHCP snooping database write-delay time       :   0 seconds
DHCP snooping option 82 status               :   DISABLE
DHCP snooping Support bootp bind status       :   DISABLE
Interface                  Trusted      Rate limit (pps)
------------------------      -------      ----------------
GigabitEthernet 0/3          YES         unlimited
```

Step 3: View DAI state. Key point: VLAN enabling state and whether the uplink port has been configured as the trusted port.

```
DES-7200#show ip arp inspection vlan
Vlan    Configuration
----    -------------
2       Enable
DES-7200#show ip arp inspection interface
      Interface        Trust State
--------------------    -----------
GigabitEthernet 0/1     Untrusted
GigabitEthernet 0/2     Untrusted
GigabitEthernet 0/3     Trusted
```

To view the database binding information generated by DHCP Snooping, execute "**show ip dhcp snooping binding**" command.

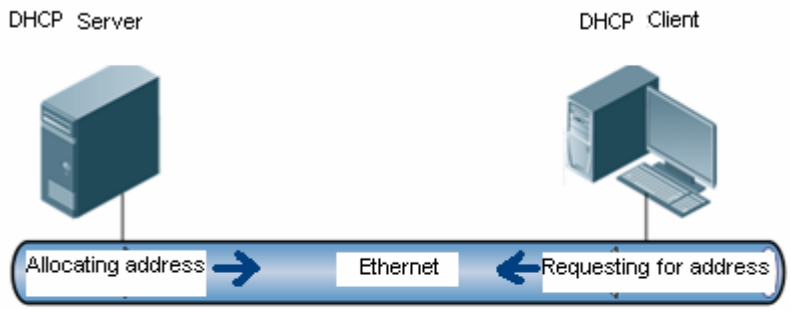
11 IP Source Guard Configuration

11.1 Brief Introduction of IP Source Guard

11.1.1 Understanding DHCP

In the typical DHCP-enabled network, the DHCP server is responsible for managing and allocating addresses for hosts. The hosts apply for legal network addresses from the DHCP server. DHCP is helpful for administrators to manage network addresses and avoid address conflict.

Figure 1 Normal DHCP Address Allocation



However, the server/client mode can not guarantee the efficiency and security of network address management. The traditional DHCP mode is required to have higher security characters because of the illegal packets or even attack packets from the clients (as shown in Figure 3) and various feigned servers (as shown in Figure 2)in the network.

DHCP Snooping solves the problem. The security problem of traditional DHCP mode can be solved by enabling DHCP Snooping on the device connecting the DHCP server with the DHCP clients. DHCP Snooping divides the network into two parts: untrusted network that shields all the DHCP Server response packets in the network and checks the security of the request from the client; trusted network that forwards

the request received from legal client to the server in that trusted network which allocates and manages addresses.

Figure 2 Network with feigned DHCP server

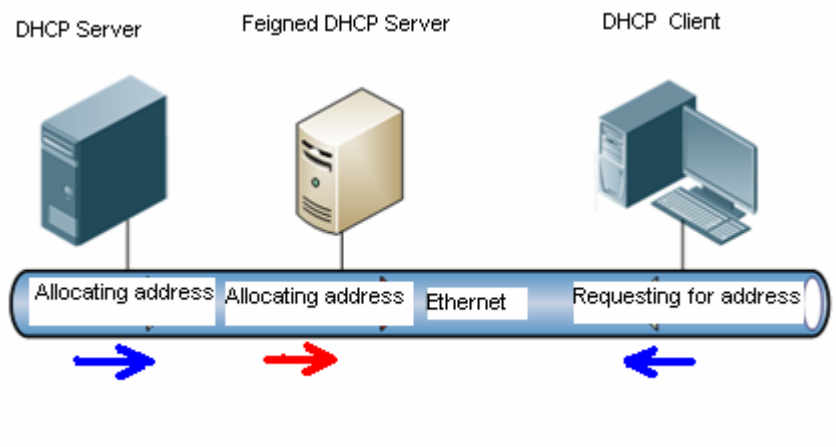


Figure 3 Network with feigned DHCP client attack

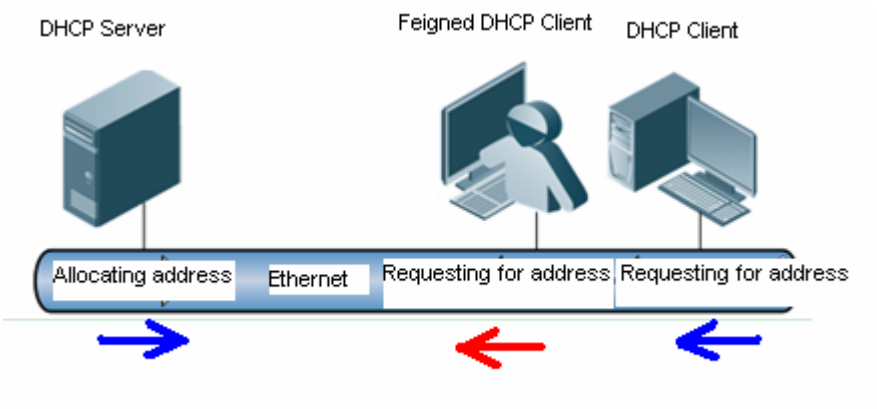
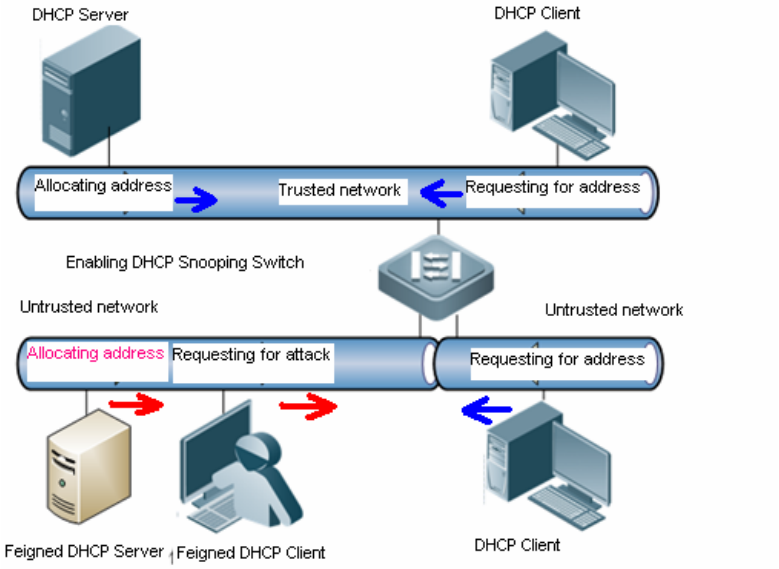


Figure 4 Network protected by DHCP Snooping



By filtering DHCP packets, DHCP Snooping shields feigned servers and block the attacks from the clients. However, it cannot control the users assign IP addresses privately. Those users easily lead to conflict of network addresses and be harm to the management of network addresses. To prevent the clients from assigning addresses privately in the DHCP network, enable IP Source Guard on the device connecting the DHCP server to the DHCP clients. DHCP Snooping-based IP Source Guard ensures that DHCP clients access network resources properly and block the users who assign addresses privately to access.

11.1.2 Understanding IP Source Guard

IP Source Guard maintains a hardware-based IP packet filtering database to filter packets, guaranteeing that only the users matching the database can access network resources.

The hardware-based IP packet filtering database is the key for IP Source Guard to enable efficient security control in DHCP applications. This database is on the basis of DHCP Snooping database. After IP Source Guard is enabled, the DHCP Snooping database is synchronized with the hardware-based IP packet filtering database. In this way, IP Source Guard can strictly filter IP packets from clients on the device with DHCP Snooping enabled.

By default, once IP Source Guard is enabled on a port, all the IP packets traveling through the port (except for DHCP packets) will be checked on the port. Only the users attaining IP addresses through DHCP and the configured static binding users can access the network.

IP Source Guard supports source MAC- and source IP-based filtering or source IP-based filtering. In the former case, IP Source Guard will check the source MAC and source IP addresses of all packets and only allow those packets matching the

hardware-based IP packet filtering database to pass through. In the latter case, IP Source Guard checks the source IP addresses of IP packets.

11.1.3 Other Precautions of Configuring IP Source Guard

IP Source Guard is based on DHCP Snooping, namely port-based IP Source Guard takes effect only on the untrusted port under the control of DHCP Snooping, not on the trusted port or the interfaces in the VLAN not controlled by DHCP Snooping.

11.2 IP Source Guard Configuration

11.2.1 Configuring IP Source Guard on the Interface

By default, IP Source Guard is disabled on the interface and all the users connecting to the interface can use the network. After enabling IP Source Guard on the interface, it will filter the IP packets of the users connecting to the interface according to the hardware-based IP packet filtering database.

Command	Description
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config)# [**no**] **ip verify source** [*port-security*]	Enable IP Source Guard on the interface. Use port-security to set MAC-based filtering.

The following example shows how to enable IP Source Guard on interface1:

```
DES-7200(config)# interface FastEthernet 0/1

DES-7200(config-if)# ip verify source

DES-7200(config-if)# end
```

Caution The application of IP Source Guard is combined with DHCP Snooping. That is to say, port-based IP Source Guard only takes effect on untrusted port under the control of DHCP Snooping.

11.2.2 Configuring Static IP Source Address Binding User

Under certain circumstances, users under certain ports may expect to statically use certain IP addresses. This feature can be realized by adding static user information into the IP source binding database.

Command	Description
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(config)**#** [**no**] **ip source binding mac-address vlan** *vlan_id ip-address* **[interface** *interface-id* **| ip-mac | ip-only]**	Add static IP source binding user into the database. If the interface is not specified, the binding entry will apply to all binding interfaces on the VLAN. interface: bind to interface; ip-mac: global IP+MAC binding; ip-only: global IP binding.

The following example shows how to bind a static user to port 9 of the device:

```
DES-7200# configure terminal

DES-7200(config)# ip source binding 00d0.f801.0101 vlan 1 192.168.4.243 interface
FastEthernet 0/9
```

11.3 Showing IP Source Guard Configuration

11.3.1 Showing IP Source Guard Filtering Entry

Use this command to show IP Source Guard filtering entry.

Command	Description
DES-7200# **show ip verify source** [**interface** *interface*]	Show IP Source Guard filtering entry.

For example:

```
DES-7200 # show ip verify source

Interface         Filter-type Filter-mode Ip-address  Mac-address  VLAN
---------------   ---------   -----------  ----------  ----------- ------
FastEthernet 0/3   ip         active      3.3.3.3                   1
FastEthernet 0/3   ip         active      deny-all
FastEthernet 0/4    ip+mac    active       4.4.4.4   0000.0000.0001   1
```

```
FastEthernet 0/4    ip+mac     active       deny-all
```

11.3.2 Showing Hardware-based IP Packet Filtering Database

Use this command to show the related information of hardware-based IP packet filtering database.

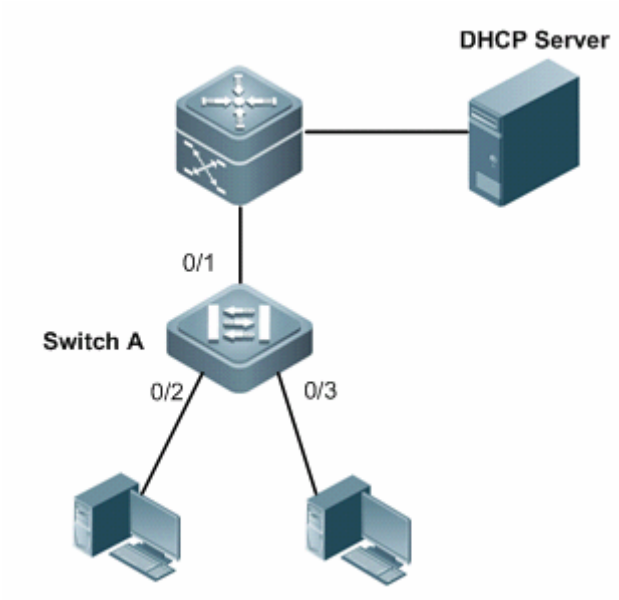
Command	Description
DES-7200# **show ip source binding** [*ip-address*] [*mac-address*] [**dhcp-snooping**] [**static**] [**vlan** *vlan-id*] [**interface** *interface-id*]	Show the hardware-based IP packet filtering database.

For example:

```
DES-7200# show ip source binding

MacAddress     IpAddress    Lease(sec)  Type      VLAN  Interface
-----------    ----------   ----------  -------   ----  ------
0000.0000.0001  1.0.0.1     infinite     static   1     FastEthernet2/1
Total number of bindings: 1
 FastEthernet  0/1

 Total number of bindings: 1
```

11.4 Example of IP Source Guard Configuration

11.4.1 Topological Diagram



DHCP deployment environment

11.4.2 Application Requirements

The user can only use the IP address dynamically allocated by a valid DHCP server or statically allocated by the administrator to access network. IP packets with source IP different from the IP addresses contained in the hardware filtering list of switch will be blocked to ensure network security.

11.4.3 Configuration Tips

Configure IP Source Guard and DHCP Snooping on the access device (Switch A) to meet the requirements:

1. Configure the uplink port (GigabitEthernet 0/1) as trusted port to avoid DHCP server spoofing.
2. Enable IP Source Guard on PC-connecting ports (GigabitEthernet 0/2 and GigabitEthernet 0/3).
3. The user with IP address assigned by the administrator can be configured through IP Source Guard static binding (IP address: 192.168.216.4; MAC address: 0000.0000.0001).

11.4.4 Configuration Steps

Configure Switch A

Step 1: Enable DHCP Snooping.

```
DES-7200#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)#ip dhcp snooping
```

Step 2: Configure the uplink port as the trusted port of DHCP Snooping.

```
DES-7200(config)#interface gigabitEthernet 0/1

DES-7200(config-if-GigabitEthernet 0/1)#ip dhcp snooping trust

DES-7200(config-if-GigabitEthernet 0/1)#exit
```

Step 3: Enable IP Source Guard on the port directly connected with PC

```
DES-7200(config)#interface range gigabitEthernet 0/2-3

DES-7200(config-if-range)#ip verify source port-security

DES-7200(config-if-range)#exit
```

Step 4: Configure static binding user

```
DES-7200(config)#ip source binding 0000.0000.0001 vlan 1 192.168.216.4 interface
gigabitEthernet 0/2
```

11.4.5 Verification

Step 1: Check the configurations of Switch A. Key points: whether DHCP Snooping has been enabled, whether the uplink port has been configured as the trusted port, whether IP Source Guard has been enabled on the user-connecting port, and whether the static binding entries are correct.

```
DES-7200#show running-config

ip dhcp snooping

!

ip source binding 0000.0000.0001 vlan 1 192.168.216.1 interface GigabitEthernet
0/2

!

interface GigabitEthernet 0/1

 ip dhcp snooping trust

!

interface GigabitEthernet 0/2

 ip verify source port-security

!

interface GigabitEthernet 0/3

 ip verify source port-security
```

Step 2: Display DHCP Snooping user binding database

```
DES-7200#show ip dhcp snooping binding

Total number of bindings: 2

MacAddress       IpAddress      Lease(sec)   Type        VLAN  Interface

------------------ --------------- ------------ -------------

0013.2049.9014         192.168.216.4      86233              dhcp-snooping  1
GigabitEthernet 0/3

00e0.4c70.b7e2         192.168.216.3      86228              dhcp-snooping  1
GigabitEthernet 0/2
```

Step 3: Display the IP hardware filtering list jointly generated through DHCP Snooping user binding database and static bindings:

```
DES-7200#show ip source binding

MacAddress        IpAddress      Lease(sec)   Type         VLAN  Interface

------------------ --------------- ------------ -------------

0000.0000.0001         192.168.216.4     infinite         static              1
GigabitEthernet 0/2

0013.2049.9014          192.168.216.4      86176               dhcp-snooping  1
GigabitEthernet 0/3

00e0.4c70.b7e2          192.168.216.3      86171               dhcp-snooping  1
GigabitEthernet 0/2

Total number of bindings: 3
```

Step 4: Display the filtering entries of IP Source Guard:

```
DES-7200#show ip verify source

Interface          Filter-type Filter-mode Ip-address     Mac-address    VLAN

-------------------  -----------  -----------  ---------------  --------------
--------

GigabitEthernet 0/2  ip+mac     active     192.168.216.4   0000.0000.0001  1

GigabitEthernet 0/2  ip+mac     active     192.168.216.3   00e0.4c70.b7e2  1

GigabitEthernet 0/2  ip+mac     active     deny-all       deny-all

GigabitEthernet 0/3  ip+mac     active     192.168.216.4   0013.2049.9014  1

GigabitEthernet 0/3  ip+mac     active
```

12 NFPP Configuration

12.1 NFPP Overview

NFPP is the abbreviation of Network Foundation Protection Policy.

- NFPP Function
- NFPP Principle

12.1.1 NFPP Function

In the network, some malicious attacks put too much burden on the switch. When the packet traffic bandwidth or the packet percent exceeds the limit, it leads to the CPU over-utilization and abnormal operation of the switch.

DoS attack may lead to the consumption of a large amount of the switch memory, entries and other resources, resulting in the system service failure.

A large amount of the packet traffic uses the CPU bandwidth, resulting in the handling failure of the protocol packet and manage packet by the CPU, influencing the data forwarding, the device management of the administrator and the normal device/network running.

In the NFPP-enabled enviroment, it prevents the system from being attacked, releasing the CPU load and ensuring the normal and stable operation of various system services and the whole network.

12.1.2 NFPP Principle

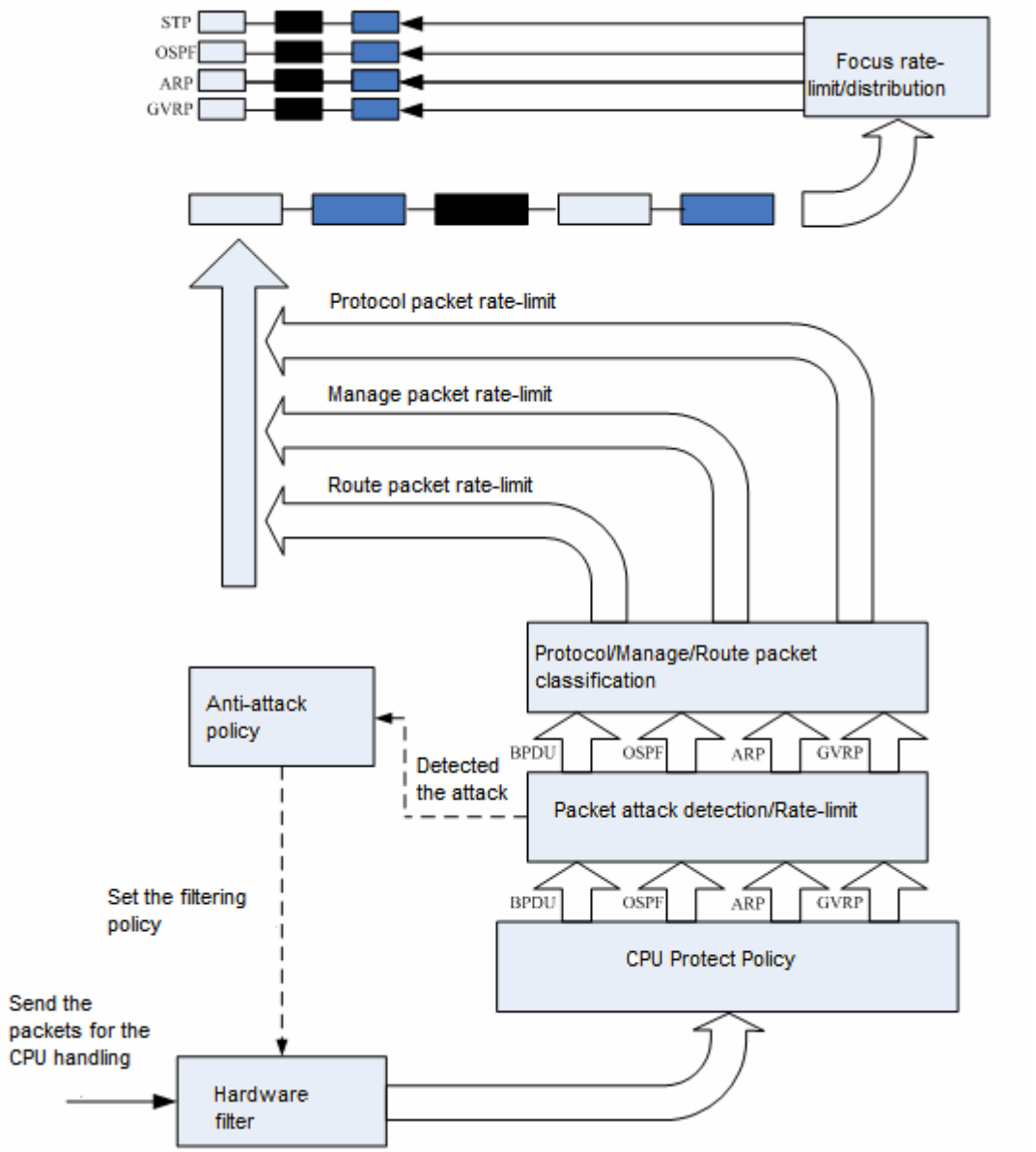
As shown in the Figure-1, the processes of the NFPP datagram processing include hardware filtering、CPU Protect Policy(CPP)、packet attack detection/rate-limit、Protocol/Manage/Route flow classification、focus rate-limit and ultimately the application-layer handling.

1. **CPU Protect Policy(CPP)**

The CPP classification and rate-limit configurations not only classify the CPU datagram according to the CPP service classificaction principle, but also limit the rate of the packet transmission, preventing different packets from competing for the bandwidth and resolving the problem that when a large amount of one packet flow attack occurs, it fails to handle other packets in time. For example, with both the OSPF packet and BPDU packet in the NFPP-enabled device, if the OSPF/BPDU packets consume a large amount of the CPU bandwidth, it will not influence receiving the BPDU/OSPF packets.

Caution

In order to make full use of the NFPP function, you can modify the rate-limit value of each packet in CPU Protect Policy according to specified network environment, you can also use the recommended value displayed after executing the **show cpu-protect summary** command.



2. **Packet attack detection/Rate-limit**

NFPP provides the host-based/port-based attack and rate-limit threshold configuration for the administrator to set in the specific network flexibly to control the rate of receiving the packets based on the host/port. With the attack threshold configured, after detecting the attack, the anti-attack policy implements the attack-warning or the isolation action. For the isolation action,

the anti-attack policy uses the hardware filter in order to make sure that the attack packets will not be sent to the CPU and ensure the normal device operation.

Caution

After detecting an attack, NFPP sends the warning messages to the administrator. However, to avoid the frequent displaying of the warning messages, the warning messages will not be shown again within the continuous 60s after the sending.

Frequently print the syslog consumes the CPU resources, to this end, NFPP writes the syslog on the attack detection to the buffer area and specifies the print rate. No rate-limit is configured for the TRAP message.

Protocol/Manage/Route flow classification

As shown in the Table-1, the packet types are divided into Manage、Route and Protocol packet. Each packet type owns the independent bandwidth. The bandwidth between the different types cannot be shared and the packet flow exceeding the bandwidth threshold will be discarded. The packet flow classification ensures that the set packet type on the device takes the precedence over other types of packet. The administrator can flexibly allocate the bandwidth of the three types of the packet according to the actual network environment and make sure that the protocol and manage packets takes the precendence of being handled for the purpose of normal protocol running and the administrator management, thereby safeguarding the normal operation of each important function on the device and improving the anti-attack capability.

Table-1

Packet Type	Service Type defined in the CPP
Protocol	tp-guard，dot1x，rldp，rerp，slow-packet，bpdu，isis dhcps，gvrp，ripng，dvmrp，igmp，mpls，ospf, pim，pimv6，rip，vrrp，ospf3，dhcp-relay-s，dhcp-relay-c，option82，tunnel-bpdu，tunnel-gvrp
Route	unknown-ipmc，unknown-ipmcv6，ttl1，ttl0, udp-helper，ip4-packet-other，ip6-packet-other，non-ip-packet-other，arp
Manage	ip4-packet-local，ip6-packet-local

3. **Focus rate-limit**

After the classification rate-limit, focus on all the flow classification in a queue.If the process rate of one type of the packets is low, the corresponding packets will accumulate in the queue, and consume the queue resources ultimately. The administrator can configure the packet percent. If the length of the queue for one type of the packet is more than the total queue

length multiplied by the packet percent, the type of packets will be discarded.

12.2 Configuring NFPP

This section describes how to configure the NFPP.

- Default NFPP configuration.
- Configuring the packet traffic bandwidth.
- Configuring the packet percent.
- Anti-attack Protocols

12.2.1 Default NFPP Configuration

The default configurations of NFPP are as follows:

Packet type	Default traffic bandwidth	Default packet percent
Manage	3000PPS	30
Route	3000PPS	25
Protocol	3000PPS	45

12.2.2 Configuring the packet traffic bandwidth

This section describes how to configure the packet traffic bandwidth:

Command	Function
DES-7200(config)# **cpu-protect sub-interface** {**manage|protocol|route**} **pps** *pps_vaule*	Configure the traffic bandwidth threshold of the corresponding packet, in pps, ranging from 1 to 8192, in integer.

For example:

```
DES-7200(config)# cpu-protect sub-interface manage pps 200

DES-7200(config)# end
```

12.2.3 Configuring the packet percent

This section describes how to configure the packet percent:

Command	Function

Command	Function
DES-7200(config)# **cpu-protect sub-interface** {**manage|protocol|route**} **percent** *percent_vaule*	Configure the packet percent. *percent_value*: ranging from 1 to 100, in integer.

For example:

```
DES-7200(config)# cpu-protect sub-interface manage percent 60

DES-7200(config)# end
```

Caution

The valid percent value of one packet must be less than 100% minus the percent value of other two types of packets

12.2.4 Anti-attack Protocols

- ARP-guard
- IP-guard
- ICMP-guard
- DHCP-guard
- DHCPv6-guard
- ND-guard
- NFPP syslog

12.3 ARP-guard

12.3.1 ARP-guard Overview

The IP address is translated into the MAC address by ARP protocol in the local area network(LAN). ARP protocol plays an important role in the network security. ARP DoS attack sends a large amount of illegal ARP packets to the gateway, preventing the gateway from providing the services. To deal with this attack, on one hand, you can configure the rate-limit of the ARP packet, on the other hand, you can detect and isolate the attack source.

The ARP attack detection could be host-based or port-based. Host-based ARP attack detection could be classified into the following two types again: source IP address/VID/port-based and source MAC address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The ARP packet will be

dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

Besides, ARP-guard is able to detect the ARP scan. ARP scan is that the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing. DES-7200 products only support to detect the first ARP scan (the source MAC address on link layer is fixed while the source IP address is changing).

It is worth mentioning that ARP-guard is only for the ARP DoS attack, rather than ARP fraud or dealing with the ARP attack problems in the network.

ARP-guard configuration commands include:

- Enabling arp-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Clearing the monitored hosts
- Clearing the ARP scanning list
- Showing related arp-guard information

12.3.2 Enabling ARP-guard

You can enable arp-guard in the nfpp configuration mode or in the interface configuration mode. By default, the arp-guard is enabled.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)**# nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **arp-guard enable**	Enable the arp-guard. By default, arp-guard is enabled.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-name*	Enter the interface configuration mode.

Command	Function
DES-7200(config-if)# **nfpp arp-guard enable**	Enable the arp-guard on the interface. By default, arp-guard is not enabled on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp arp-guard summary**	Show the configurations.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

With the arp-guard disabled, the monitored hosts and scan hosts are auto-cleared.

12.3.3 Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **arp-guard isolate-period** [*seconds* | **permanent**]	Configure the global isolated time, ranging 0s, 180-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp arp-guard isolate-period** [*seconds* | **permanent**]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.

Command	Function
DES-7200# **show nfpp arp-guard summary**	Show the arp-guard parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the global isolated time to the default value, use the **no arp-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no arp-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

12.3.4 Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the arp-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **arp-guard monitor-period** *seconds*	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp arp-guard summary**	Show the arp-guard parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored time to the default value, use the **no arp-guard monitor-period** command in the nfpp configuration mode.

Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

12.3.5 Configuring the monitored host limit

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **arp-guard monitored-host-limit** *seconds*	Configure the monitored host limit, ranging 1-4294967295. The default value is1000.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp arp-guard summary**	Show the arp-guard parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored host limit to the default value, use the **no arp-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent moniored hosts will not be deleted and it will prompt the message "`%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.`" to notify the administrator of the invalid configuration and removing a part of the monitored hosts.

Caution

It prompts the message that "`% NFPP_ARP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.`" if the monitored host table is full.

12.3.6 Host-based rate-limit and attack detection

For the host-based attack detection, it can be classified into the following two types: source IP address/VID/port-based and source MAC address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The ARP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

ARP-guard supports to detect the ARP scan, which is in 10s, 15s by default. If 15 or more than 15 ARP packets have been received within 10s, and the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing, ARP scan is detected and recorded in the syslog and the TRAP messages are sent.

It prompts the following message if the ARP DoS attack was detected:

```
%NFPP_ARP_GUARD-4-DOS_DETECTED: Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/
1,VLAN=1> was detected.(2009-07-01 13:00:00)
```

The content in brackets is the attack detection time.

The following example shows the describing information included in the sent TRAP messages:

```
ARP DoS attack from host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> wa
s detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_ARP_GUARD-4-ISOLATED:Host <IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VL
AN=1> was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_ARP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=0000.
0000.0004,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1>.
```

It prompts the following message when the ARP scan was detected:

```
%NFPP_ARP_GUARD-4-SCAN: Host<IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VL
AN=1> was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
ARP scan from host< IP=1.1.1.1,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was
  detected.
```

It saves the latest 256 pieces of records in the ARP scan table. When the ARP scan table is full, it prompts:

```
%NFPP_ARP_GUARD-4-SCAN_TABLE_FULL: ARP scan table is full.
```

It prompts the following message to remind the administrator that the configured rate-limit threshold is higher than the attack threshold:

```
%ERROR: rate limit is higher than attack threshold 500pps."
```

It prompts the following message to remind the administrator that the configured attack threshold is smaller than the rate-limit threshold:

```
%ERROR: attack threshold is smaller than rate limit 300pps."
```

Caution

- It sets a policy to the hardware when isolating the attackers. When the hardware resources have been exhausted, it prompts the message to inform the administrator.
- When it fails to allocate the memory to the detected attackers, it prompts the message like "`%NFPP_ARP_GUARD-4-NO_MEMORY: Failed to alloc memory.`" to inform the administrator.
- It contains only the latest 256 pieces of the records in the ARP scan table. When the ARP scan table is full, the newest record will overwrite the oldest one.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.

Command	Function
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **arp-guard rate-limit** {**per-src-ip | per-src-mac**} *pps*	Configure the arp-guard rate-limit, ranging from 1 to 9999, 4 by default. **per-src-ip**: detect the hosts based on the source IP address/VID/port; **per-src-mac**: detect the hosts based on the source MAC address/VID/port.
DES-7200(config-nfpp)# **arp-guard attack-threshold** {**per-src-ip | per-src-mac**} *pps*	Configure the arp-guard attack threshold, ranging from 1 to 9999, 8 by default. When the ARP packet number sent from a host exceeds the attack threshold, the attack is detected and ARP-guard isolates the host, records the message and sends the TRAP packet. **per-src-ip**: detect the hosts based on the source IP address/VID/port; **per-src-mac**: detect the hosts based on the source MAC address/VID/port.
DES-7200(config-nfpp)# **arp-guard scan-threshold** *pkt-cnt*	Configure the arp-guard scan threshold, in 10s, ranging from 1 to 9999, 15 by default. If 15 or more than 15 ARP packets have been received within 10s, and the source MAC address on link layer is fixed while the source IP address is changing, or the source MAC address and source IP address are fixed while the destination IP address is changing, ARP scan is detected and recorded in the syslog and the TRAP messages are sent.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.

Command	Function
DES-7200(config-if)#nfpp arp-guard policy {per-src-ip | per-src-mac} *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. **per-src-ip:** to detect the hosts based on the source IP/VID/port; **per-src-mac:** to detect the hosts based on the source MAC/VID/port on the link layer.
DES-7200(config-if)#nfpp arp-guard scan-threshold *pkt-cnt*	Configure the arp-guard scan threshold value on each interface, the valid range is 1-9999, in 10s. By default, it adopts the global arp-guard scan threshold value.
DES-7200(config-if)**# end**	Return to the privileged EXEC mode.
DES-7200**# show nfpp arp-guard summary**	Show the arp-guard parameter settings.
DES-7200**# copy running-config startup-config**	Save the configurations.

12.3.7 Port-based rate-limit and attack detection

You can configure the arp-guard rate limt and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the ARP packet rate on a port exceeds the limit, the ARP packets are dropped. When the ARP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the ARP DoS attack was detected on a port:

```
%NFPP_ARP_GUARD-4-PORT_ATTACKED: ARP DoS attack was detected on port Gi4/1.
(2009-07-01 13:00:00)
```

The following is additional information of the sent TRAP packet :

```
ARP DoS attack was detected on port Gi4/1.
```

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **arp-guard rate-limit per-port** *pps*	Configure the arp-guard rate-limit of the ARP packet on the port, ranging from 1 to 9999, 100 by default.
DES-7200(config-nfpp)# **arp-guard attack-threshold per-port** *pps*	Configure the arp-guard attack threshold, ranging from 1 to 9999, 200 by default. When the ARP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)**#nfpp arp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp arp-guard summary**	Show the arp-guard parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

MAC address-based rate limit takes precedence over IP address-based rate limit. IP address-based rate limit takes precedence over port-based rate limit.

It is recommended for the administrator to follow the following principle of configuring the host-based rate-limit and attack threshold, in order to perform the best arp-guard function:

Caution

IP address-based rate-limit threshold < IP address-based attack threshold < source MAC address-based rate-limit threshold < source MAC address-based attack threshold.

When configuring the rate limit on the port, you can refer to the user count on this port. For example, if 500 users exist on a port, you can set the rate limit on this port to 500.

12.3.8 Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
DES-7200# **clear nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]	**clear nfpp arp-guard hosts:** Clear all isolated hosts. **clear nfpp arp-guard hosts vlan** *vid*: Clear all isolated hosts in a VLAN. **clear nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Clear all isolated hosts on a interface in a VLAN. **clear nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [**ip-address** | **mac-address**]: An isolated host has been cleared. Use the IP address or the MAC address to identify the hosts.

12.3.9 Clearing the ARP san table

The administrator can use the following command to clear the ARP scan table manually.

Command	Function
DES-7200# **clear nfpp arp-guard scan**	Clear the ARP scan table.

12.3.10 Showing arp-guard

- Showing arp-guard configuration
- Showing monitored host configuration
- Showing arp scan table

12.3.10.1 Showing arp-guard configuration

Use this command to show the arp-guard configurations.

Command	Function
DES-7200# **show nfpp arp-guard summary**	Show the arp-guard configurations.

For example,

```
DES-7200# show nfpp arp-guard summary
（Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-m
ac/per-port.）
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-thresho
ld
Global     Enable  300           4/5/60     8/10/100         15
G 0/1      Enable  180           5/-/-      8/-/-            -
G 0/2      Disable 200           4/5/60     8/10/100         20

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Note

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

12.3.10.2 Showing monitored host configuration

Command	Function
DES-7200# **show nfpp arp-guard hosts statistics**	Show the arp-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
DES-7200#**show nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]	Show the isolated hosts information. **show nfpp arp-guard hosts vlan** *vid*: Show the isolated hosts in a VLAN. **show nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Show the isolated hosts on a interface in a VLAN. **show nfpp arp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [**ip-address** | **mac-address**]: Show the isolated hosts. Use the IP address or the MAC address to identify the hosts.

For example,

```
DES-7200#show nfpp arp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120


DES-7200# show nfpp arp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address   MAC address     remain-time(s)
----  --------   ---------    -----------     -------------
1     Gi0/1      1.1.1.1      -               110
2     Gi0/2      1.1.2.1      -               61
*3    Gi0/3      -            0000.0000.1111  110
4     Gi0/4      -            0000.0000.2222   61
Total：4 hosts

DES-7200# show nfpp arp-guard hosts vlan 1 interface G 0/1 1.1.1.1
If column 1 shows '*', it means "hardware do not isolate user".
VLAN  interface IP address   MAC address     remain-time(s)
---- --------   ---------    -----------     -------------
1    Gi0/1      1.1.1.1      -               110
Total：1 host
```

Note

If the MAC address columm shows "-", it means "the host is identified by the source IP address";

If the IP address columm shows "-", it means "the host is identified by the source MAC address".

12.3.10.3 Showing the ARP scan table

Command	Function
DES-7200# **show nfpp arp-guard scan statistics**	Show the arp-guard scan statistics.
DES-7200#**show nfpp arp-guard scan** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]	Show the arp-guard scan information. **show nfpp arp-guard scan vlan** *vid*: Show the arp-guard scan information in a VLAN. **show nfpp arp-guard scan** [**vlan** *vid*] [**interface** *interface-id*]: Show the arp-guard scan information on a interface in a VLAN. **show nfpp arp-guard scan** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]: Show the arp-guard scan information for a MAC address on a interface in a VLAN.

For example,

```
DES-7200#show nfpp arp-guard scan statistics

ARP scan table has 4 record(s).
```

```
DES-7200# show nfpp arp-guard scan
VLAN    interface   IP address   MAC address      timestamp
----    --------    ----------  -----------      ----------
1       Gi0/1       N/A         0000.0000.0001   2008-01-23 16:23:10
2       Gi0/2       1.1.1.1     0000.0000.0002   2008-01-23 16:24:10
3       Gi0/3       N/A         0000.0000.0003   2008-01-23 16:25:10
4       Gi0/4       N/A         0000.0000.0004   2008-01-23 16:26:10
Total：4 record(s)
```

"timestamp" represents the time when the ARP scan was detected. For example, "2008-01-23 16:23:10" represents that the ARP scan was detected at 16:23:10, Jan 23, 2008.

```
DES-7200# show nfpp arp-guard scan vlan 1 interface G 0/1 0000.0000.0001
```

```
VLAN    interface   IP address   MAC address      timestamp
----    --------    ----------    -----------      ----------
1       Gi0/1       N/A          0000.0000.0001   2008-01-23 16:23:10
Total: 1 record(s)
```

12.4 IP-guard

12.4.1 IP-guard Overview

As is known to all, many hacker attacks and the network virus invasions begin with the network scanning. To this end, a large amount of the scanning packets take up the network bandwidth, leading to the abnormal network communication.

DES-7200 Layer-3 device provides the IP-guard function to prevent the attacks from the hacker and the virus such as “Blaster”, reducing the CPU burden of the layer-3 devices.

There are two types of the IP packet attack:

- **Scanning the destination IP address change:** not only consumes the network bandwidth and increases the device burden, but also is a prelude of the hacker attack.
- **Sending the IP packets to the inexistent destination IP address at the high-rate:** for the layer-3 device, the packets are directly forwarded by the switching chip without the consumption of the CPU resources if the destination IP address exists. While if the destination IP address is inexistent, the ARP request packets are sent from the CPU to ask for the corresponding MAC address for the destination IP address when the IP packets are sent to the CPU. It consumes the CPU resources if many IP packets are sent to the CPU. The workaround for this attack: one one hand, you may configure the IP packet rate-limit; on the other hand, you may detect and isolate the attack source.

The IP attack detection could be host-based or port-based. Host-based ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The IP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ARP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

Caution

It is worth mentioning that the IP-guard is for the attack of the IP packets with the destination IP address not the host IP address. For the IP packet with the destination IP address the host IP address, use the CPP(CPU Protect Policy) to limit the rate.

The IP-guard is supported in the layer-3 switches only.

With the ip-guard enabled on the interface and the non-0 isolated period configured, it isolates the hosts attacked by the IP packets.

IP-guard configuration commands include:

- Enabling ip-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Configuring trusted host
- Showing related ip-guard information

12.4.2 Enabling IP-guard

You can enable ip-guard in the nfpp configuration mode or in the interface configuration mode. By default, the ip-guard is enabled.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **ip-guard enable**	Enable the ip-guard. By default, ip-guard is enabled.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp ip-guard enable**	Enable the ip-guard on the interface. By default, ip-guard is not enabled on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.

Command	Function
DES-7200# **show nfpp ip-guard summary**	Show the configurations.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution With the ip-guard disabled, the monitored hosts are auto-cleared.

12.4.3 Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **ip-guard isolate-period** [*seconds* | **permanent**]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp arp-guard isolate-period** [*seconds* | **permanent**]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp ip-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the global isolated time to the default value, use the **no ip-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no ip-guard isolate-period** command to remove the port-based isolated time

configuration in the interface configuration mode.

12.4.4 Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the ip-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **ip-guard monitor-period** *seconds*	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp ip-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored time to the default value, use the **no ip-guard monitor-period** command in the nfpp configuration mode.

Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

12.4.5 Configuring the monitored host limit

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.

Command	Function
DES-7200(config-nfpp)# **ip-guard monitored-host-limit** *seconds*	Configure the monitored host limit, ranging 1-4294967295. The default value is1000.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp ip-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored host limit to the default value, use the **no ip-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent moniored hosts will not be deleted and it will prompt the message "`%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts.`" to notify the administrator of the invalid configuration and removing a part of the monitored hosts.

Caution

It prompts the message that "`% NFPP_IP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts.`" if the monitored host table is full.

12.4.6 Host-based rate-limit and attack detection

Use the source IP address/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The IP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the IP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

It prompts the following message if the IP DoS attack was detected:

%NFPP_IP_GUARD-4- DOS_DETECTED:Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected. (2009-07-01 13:00:00)

The following example shows the describing information included in the sent TRAP messages:

```
IP DoS attack from host<IP=1.1.1.1,MAC= N/A,,port=Gi4/1,VLAN=1> was detec
ted.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds,

it prompts:

```
%NFPP_IP_GUARD-4-ISOLATED:Host <IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1>
was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

Host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was isolated.

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_IP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=1.1.1.1, MAC=
N/A,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

Failed to isolate host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1>.

It prompts the following message when the IP scan was detected:

%NFPP_IP_GUARD-4-SCAN: Host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was detected. (2009-07-01 13:00:00)

The following example shows the describing information included in the sent TRAP messages:

IP scan from host< IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was detected.

Caution

- It sets a policy to the hardware when isolating the attackers. When the hardware resources have been exhausted, it prompts the message to inform the administrator.
- When it fails to allocate the memory to the detected attackers, it prompts the message like "`%NFPP_IP_GUARD-4-NO_MEMORY: Failed to alloc memory.`" to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **ip-guard rate-limit per-src-ip** *pps*	Configure the ip-guard rate-limit, ranging from 1 to 9999, 20 by default. **per-src-ip**: detect the hosts based on the source IP address/VID/port;

Command	Function
DES-7200(config)# **ip-guard attack-threshold per-src-ip** *pps*	Configure the ip-guard attack threshold, ranging from 1 to 9999, 20 by default. When the IP packet number sent from a host exceeds the attack threshold, the attack is detected and IP-guard isolates the host, records the message and sends the TRAP packet. **per-src-ip**: detect the hosts based on the source IP address/VID/port;
DES-7200(config)# **ip-guard scan-threshold** *pkt-cnt*	Configure the ip-guard scan threshold, in 10s, ranging from 1 to 9999, 100 by default.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)#nfpp ip-guard policy per-src-ip *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. **per-src-ip:** to detect the hosts based on the source IP/VID/port;
DES-7200(config-if)#nfpp ip-guard scan-threshold *pkt-cnt*	Configure the ip-guard scan threshold value on each interface, the valid range is 1-9999, in 10s. By default, it adopts the global arp-guard scan threshold value.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp ip-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

12.4.7 Port-based rate-limit and attack detection

You can configure the ip-guard rate limt and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the IP packet rate on a port exceeds the limit, the IP packets are dropped. When the IP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the IP DoS attack was detected on a port:

%NFPP_IP_GUARD-4-PORT_ATTACKED: IP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

IP DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)**# nfpp**	Enter the nfpp configuration mode.
DES-7200(config)# **ip-guard rate-limit per-port** *pps*	Configure the ip-guard rate-limit of the IP packet on the port, ranging from 1 to 9999, 100 by default.
DES-7200(config)# **ip-guard attack-threshold per-port** *pps*	Configure the ip-guard attack threshold, ranging from 1 to 9999, 200 by default. When the IP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)**#nfpp ip-guard policy per-port** *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.

Command	Function
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp ip-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

The source IP address-based rate limit takes precedence over port-based rate limit.

12.4.8 Configuring the trusted hosts

Use the following commands to set the trusted host to make a host free from monitoring. The IP packets are allowed to be sent to the CPU from the trusted host.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **ip-guard trusted-host** *ip mask*	Configure the IP address range for the trusted hosts. Up to 500 pieces of IP addresses can be configured.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp ip-guard trusted-host**	Show the trusted host settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

In the nfpp configuration mode, use the **no** form of this command to delete a trusted host entry and use the **all** form of this command to delete all trusted hosts.

For example:

The following example shows how to delete all trusted hosts:

DES-7200(config-nfpp)# **no ip-guard trusted-host all**

The following example shows how to delete a trusted host entry:

DES-7200(config-nfpp)# **no ip-guard trusted-host** *1.1.1.1 255.255.255.255*

It prompts that "%ERROR: Attempt to exceed limit of 500 trusted hosts."to inform the administrator of the full trusted host table.

If the IP address for the trusted host entry is the same to the one existing in the untrusted host list, the system will auto-delete the entry according to the IP address.

It prompts that " % ERROR:Failed to delete trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of trusted host removal.

It prompts that "%ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

Caution

It prompts that "%ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "%ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "%ERROR:Trusted host 1.1.1.0 255.255.255.0 has already been configured." to inform the administrator of the exisitence of the trusted host to be added.

It prompts that "%ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator of the inexisitence of the trusted host to be deleted.

It prompts that "%ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator if it fails to allocate the memory for the trusted host.

12.4.9 Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
DES-7200# **clear nfpp ip-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	**clear nfpp ip-guard hosts:** Clear all isolated hosts. **clear nfpp ip-guard hosts vlan** *vid*: Clear all isolated hosts in a VLAN. **clear nfpp ip-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Clear all isolated hosts on a interface in a VLAN. **clear nfpp ip-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]: An isolated host has been cleared. Use the IP address to identify the hosts.

12.4.10 Showing ip-guard

- Showing ip-guard configuration
- Showing monitored host configuration
- Showing trusted host configuration

12.4.10.1 Showing ip-guard configuration

Use this command to show the ip-guard configurations.

Command	Function
DES-7200# **show nfpp ip-guard summary**	Show the ip-guard configurations.

For example,

```
DES-7200# show nfpp ip-guard summary
（Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-m
ac/per-port.）
Interface  Status  Isolate-period Rate-limit Attack-threshold Scan-thresho
ld
Global     Enable  300           4/-/60     8/-/100          15
G 0/1      Enable  180           5/-/-      8/-/-            -
G 0/2      Disable 200           4/-/60     8/-/100          20

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

Note

12.4.10.2 Showing monitored host configuration

Command	Function
DES-7200# **show nfpp ip-guard hosts statistics**	Show the ip-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
DES-7200#**show nfpp ip-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address* | *mac-address*]	Show the isolated hosts information. **show nfpp ip-guard hosts vlan** *vid*: Show the isolated hosts in a VLAN. **show nfpp ip-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Show the isolated hosts on a interface in a VLAN. **show nfpp ip-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [**ip-address** | **mac-address**]: Show the isolated hosts. Use the IP address or the MAC address to identify the hosts.

For example,

```
DES-7200#show nfpp ip-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120


DES-7200# show nfpp ip-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address   MAC address     remain-time(s)
----  --------   ---------    -----------     -------------
1     Gi0/1      1.1.1.1     ATTACK              110
2     Gi0/2      1.1.2.1     SCAN                 61
Total：2 hosts

DES-7200# show nfpp ip-guard hosts vlan 1 interface G 0/1 1.1.1.1
If column 1 shows '*', it means "hardware do not isolate user".
VLAN  interface IP address   MAC address     remain-time(s)
---- --------   ---------    -----------     -------------
1    Gi0/1      1.1.1.1      ATTACK              110
Total：1 host
```

Note

If the MAC address columm shows “-”, it means “the host is identified by the source IP address”;

If the IP address columm shows “-”, it means “the host is identified by the source MAC address”.

12.4.10.3 Showing the trusted host configuration

Command	Function
DES-7200# **show nfpp ip-guard trusted-host**	Show the trusted hosts.

For example,

```
DES-7200#show nfpp ip-guard trusted-host
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

12.5 ICMP-guard

12.5.1 ICMP-guard Overview

The ICMP attack detection could be host-based or port-based. Host-based ICMP protocol is used to diagnose the network trouble. Its basic principle is that the host sends an ICMP echo request packet, and the router/switch sends an ICMP echo reply packet upon receiving the ICMP echo request packet. The “ICMP flood” attack is that the attacker sends a large amount of the ICMP echo request packets to the destination device, resulting in the consumption of the CPU resources and the erroe of the device working. The workaround for the “ICMP flood” attack: one one hand, you may configure the ICMP packet rate-limit; on the other hand, you may detect and isolate the attack source.

ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The ICMP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ICMP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

ICMP-guard configuration commands include:

- Enabling icmp-guard

- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Configuring trusted host
- Clearing monitored host
- Showing related icmp-guard information

12.5.2 Enabling ICMP-guard

You can enable icmp-guard in the nfpp configuration mode or in the interface configuration mode. By default, the icmp-guard is enabled.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **icmp-guard enable**	Enable the icmp-guard. By default, icmp-guard is enabled.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp icmp-guard enable**	Enable the icmp-guard on the interface. By default, icmp-guard is not enabled on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp icmp-guard summary**	Show the configurations.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

With the icmp-guard disabled, the monitored hosts are auto-cleared.

12.5.3 Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **icmp-guard isolate-period** [*seconds* | **permanent**]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp arp-guard isolate-period** [*seconds* | **permanent**]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp icmp-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the global isolated time to the default value, use the **no icmp-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no icmp-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

12.5.4 Configuring the monitored time

Without the global and port-based isolated period configured(including set the interface isolated time 0), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system.

With the global or port-based isolated period configured, the ICMP-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **icmp-guard monitor-period** *seconds*	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp icmp-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored time to the default value, use the **no icmp-guard monitor-period** command in the nfpp configuration mode.

Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

12.5.5 Configuring the monitored host limit

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **icmp-guard monitored-host-limit** *seconds*	Configure the monitored host limit, ranging 1-4294967295. The default value is1000.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp icmp-guard summary**	Show the parameter settings.

Command	Function
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored host limit to the default value, use the **no icmp-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent moniored hosts will not be deleted and it will prompt the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." to notify the administrator of the invalid configuration and removing a part of the monitored hosts.

Caution

It prompts the message that "% NFPP_ICMP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." if the monitored host table is full.

12.5.6 Host-based rate-limit and attack detection

Use the source IP address/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The ICMP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the ICMP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

It prompts the following message if the ICMP DoS attack was detected:

```
%NFPP_ICMP_GUARD-4- DOS_DETECTED:Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLA
N=1> was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
ICMP DoS attack from host<IP=1.1.1.1,MAC= N/A,,port=Gi4/1,VLAN=1> was det
ected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_ICMP_GUARD-4-ISOLATED:Host <IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1
> was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_ICMP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP==1.1.1.1, M
AC= N/A,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1>.
```

Caution When it fails to allocate the memory to the detected attackers, it prompts the message like "`%NFPP_ICMP_GUARD-4-NO_MEMORY: Failed to alloc memory.`" to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **icmp-guard rate-limit per-src-ip** *pps*	Configure the icmp-guard rate-limit, ranging from 1 to 9999, the default value is the half of the port-based global rate-limit. **per-src-ip**: detect the hosts based on the source IP address/VID/port;
DES-7200(config)# **icmp-guard attack-threshold per-src-ip** *pps*	Configure the icmp-guard attack threshold, ranging from 1 to 9999, and the default value is the source IP address-based rate limit. When the ICMP packet number sent from a host exceeds the attack threshold, the attack is detected and ICMP-guard isolates the host, records the message and sends the TRAP packet. **per-src-ip**: detect the hosts based on the source IP address/VID/port;
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.

Command	Function
DES-7200(config)**# interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)#nfpp icmp-guard policy per-src-ip *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. **per-src-ip:** to detect the hosts based on the source IP/VID/port;
DES-7200(config-nfpp)**# end**	Return to the privileged EXEC mode.
DES-7200(config-if)**# show nfpp icmp-guard summary**	Show the parameter settings.
DES-7200**# copy running-config startup-config**	Save the configurations.

12.5.7 Port-based rate-limit and attack detection

You can configure the icmp-guard rate limt and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the ICMP packet rate on a port exceeds the limit, the ICMP packets are dropped. When the ICMP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the ICMP DoS attack was detected on a port:

%NFPP_ICMP_GUARD-4-PORT_ATTACKED: ICMP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

ICMP DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config)# **icmp-guard rate-limit per-port** *pps*	Configure the icmp-guard rate-limit of the ICMP packet on the port, ranging from 1 to 9999. The default values vary with different products: For DES-7200 series, different default values vary with different CMs.
DES-7200(config)# **icmp-guard attack-threshold per-port** *pps*	Configure the icmp-guard attack threshold, ranging from 1 to 9999. The default value is the port-based rate limit. When the ICMP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)#**nfpp icmp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp icmp-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

The source IP address-based rate limit takes precedence over port-based rate limit.

12.5.8 Configuring the trusted hosts

Use the following commands to set the trusted host to make a host free from monitoring. The ping packets are allowed to be sent to the CPU from the trusted host.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **icmp-guard trusted-host** *ip mask*	Configure the IP address range for the trusted hosts. Up to 500 pieces of IP addresses can be configured.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp icmp-guard trusted-host**	Show the trusted host settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

In the nfpp configuration mode, use the **no** form of this command to delete a trusted host entry and use the **all** form of this command to delete all trusted hosts.

For example:

The following example shows how to delete all trusted hosts:

DES-7200(config-nfpp)# **no icmp-guard trusted-host all**

The following example shows how to delete a trusted host entry:

DES-7200(config-nfpp)# **no icmp-guard trusted-host** *1.1.1.1 255.255.255.255*

It prompts that "%ERROR: Attempt to exceed limit of 500 trusted hosts."to inform the administrator of the full trusted host table.

If the IP address for the trusted host entry is the same to the one existing in the untrusted host list, the system will auto-delete the entry according to the IP address.

It prompts that " % ERROR:Failed to delete trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of trusted host removal.

It prompts that "%ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

Caution

It prompts that "%ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "%ERROR:Failed to add trusted host 1.1.1.0 255.255.255.0." to inform the administrator of the failure of adding the trusted host.

It prompts that "%ERROR:Trusted host 1.1.1.0 255.255.255.0 has already been configured." to inform the administrator of the exisitence of the trusted host to be added.

It prompts that "%ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator of the inexisitence of the trusted host to be deleted.

It prompts that "%ERROR:Trusted host 1.1.1.0 255.255.255.0 is not found." to inform the administrator if it fails to allocate the memory for the trusted host.

12.5.9 Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
DES-7200# **clear nfpp icmp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	**clear nfpp icmp-guard hosts:** Clear all isolated hosts. **clear nfpp icmp-guard hosts vlan** *vid*: Clear all isolated hosts in a VLAN. **clear nfpp icmp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Clear all isolated hosts on a interface in a VLAN. **clear nfpp icmp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]: An isolated host has been cleared. Use the IP address to identify the hosts.

12.5.10 Showing icmp-guard

- Showing icmp-guard configuration
- Showing monitored host configuration
- Showing trusted host configuration

12.5.10.1 Showing icmp-guard configuration

Use this command to show the icmp-guard configurations.

Command	Function
DES-7200# **show nfpp icmp-guard summary**	Show the icmp-guard configurations.

For example,

```
DES-7200# show nfpp icmp-guard summary
（Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-m
ac/per-port.）
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            4/-/60     8/-/100
G 0/1      Enable  180            5/-/-      8/-/-
G 0/2      Disable 200            4/-/60     8/-/100

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Note

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

12.5.10.2 Showing monitored host configuration

Command	Function
DES-7200# **show nfpp icmp-guard hosts statistics**	Show the icmp-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
DES-7200#**show nfpp icmp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]	Show the isolated hosts information. **show nfpp icmp-guard hosts vlan** *vid*: Show the isolated hosts in a VLAN. **show nfpp icmp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Show the isolated hosts on a interface in a VLAN. **show nfpp icmp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*]: Show the isolated hosts. Use the IP address to identify the hosts.

For example,

```
DES-7200#show nfpp icmp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120


DES-7200# show nfpp icmp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface IP address      remain-time(s)
----  --------   ---------       -------------
1     Gi0/1      1.1.1.1              110
2     Gi0/2      1.1.2.1               61
Total：2 hosts

DES-7200# show nfpp icmp-guard hosts vlan 1 interface G 0/1 1.1.1.1
If column 1 shows '*', it means "hardware do not isolate user".
VLAN  interface IP address       remain-time(s)
---- --------   ---------         -------------
1    Gi0/1      1.1.1.1               80
Total：1 host
```

12.5.10.3 Showing the trusted host configuration

Command	Function

Command	Function
DES-7200# **show nfpp icmp-guard trusted-host**	Show the trusted hosts.

For example,

```
DES-7200#show nfpp icmp-guard trusted-host
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

12.6 DHCP-guard

12.6.1 DHCP-guard Overview

The DHCP protocol is widely used to dynamically allocate the IP address in the LAN, and plays an important role in the network security. The “DHCP exhaustion” attack occurs in the way of broadcasting the DHCP request packets through faking the MAC address. If there are too many DHCP request packets, the attacker may use up the addresses provided in the DHCP server. To this end, a legal host fails to request for a DHCP IP address and access to the network. The workaround for the “DHCP exhaustion” attack: one one hand, you may configure the DHCP packet rate-limit; on the other hand, you may detect and isolate the attack source.

The DHCP attack detection could be host-based or port-based. Host-based ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The DHCP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

DHCP-guard configuration commands include:

- Enabling dhcp-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit
- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection

- Clearing monitored host
- Showing related dhcp-guard information

12.6.2 Enabling DHCP-guard

You can enable dhcp-guard in the nfpp configuration mode or in the interface configuration mode. By default, the dhcp-guard is enabled.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcp-guard enable**	Enable the dhcp-guard. By default, dhcp-guard is enabled.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp dhcp-guard enable**	Enable the dhcp-guard on the interface. By default, dhcp-guard is not enabled on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcp-guard summary**	Show the configurations.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

With the dhcp-guard disabled, the monitored hosts are auto-cleared.

12.6.3 Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration mode. By default, the isolated time is configured in the global configuration mode.

Command	Function

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcp-guard isolate-period** [*seconds* | **permanent**]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp arp-guard isolate-period** [*seconds* | **permanent**]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcp-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the global isolated time to the default value, use the **no dhcp-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no dhcp-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

12.6.4 Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the DHCP-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.

Command	Function
DES-7200(config-nfpp)# **dhcp-guard monitor-period** *seconds*	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcp-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored time to the default value, use the **no dhcp-guard monitor-period** command in the nfpp configuration mode.

Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

12.6.5 Configuring the monitored host limit

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcp-guard monitored-host-limit** *seconds*	Configure the monitored host limit, ranging 1-4294967295. The default value is1000.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcp-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored host limit to the default value, use the **no dhcp-guard monitored-host-limit** command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent moniored hosts will not be deleted and it will prompt the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." to notify the administrator of the invalid configuration and removing a part of the monitored hosts.

Caution

It prompts the message that "% NFPP_DHCP_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." if the monitored host table is full.

12.6.6 Host-based rate-limit and attack detection

Use the source MAC/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The DHCP packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCP packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

It prompts the following message if the DHCP DoS attack was detected:

```
%NFPP_DHCP_GUARD-4- DOS_DETECTED:Host<IP=N/A,MAC=0000.0000.0001,port=Gi4
/1,VLAN=1> was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
DHCP DoS attack from host<IP= N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>
was detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_DHCP_GUARD-4-ISOLATED:Host <IP= N/A,MAC=0000.0000.0001,port=Gi4/1,
VLAN=1> was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_DHCP_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=000
```

```
0.0000.0001,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```

Caution When it fails to allocate the memory to the detected attackers, it prompts the message like "`%NFPP_DHCP_GUARD-4-NO_MEMORY: Failed to alloc memory.`" to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcp-guard rate-limit per-src-mac** *pps*	Configure the dhcp-guard rate-limit, ranging from 1 to 9999, 5 by default. **per-src-mac**: detect the hosts based on the source MAC address/VID/port;
DES-7200(config)# **dhcp-guard attack-threshold per-src-mac** *pps*	Configure the dhcp-guard attack threshold, ranging from 1 to 9999, 10 by default. When the DHCP packet number sent from a host exceeds the attack threshold, the attack is detected and DHCP-guard isolates the host, records the message and sends the TRAP packet. **per-src-mac**: detect the hosts based on the source MAC address/VID/port;
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.

Command	Function
DES-7200(config-if)#nfpp dhcp-guard policy per-src-mac *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. **per-src-mac:** to detect the hosts based on the source MAC/VID/port;
DES-7200(config-nfpp)**# end**	Return to the privileged EXEC mode.
DES-7200(config-if)**# show nfpp dhcp-guard summary**	Show the parameter settings.
DES-7200**# copy running-config startup-config**	Save the configurations.

12.6.7 Port-based rate-limit and attack detection

You can configure the dhcp-guard rate limt and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the DHCP packet rate on a port exceeds the limit, the DHCP packets are dropped. When the DHCP packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the DHCP DoS attack was detected on a port:

%NFPP_DHCP_GUARD-4-PORT_ATTACKED: DHCP DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

DHCP DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200**# configure terminal**	Enter the global configuration mode.
DES-7200(config)**# nfpp**	Enter the nfpp configuration mode.

Command	Function
DES-7200(config)# **dhcp-guard rate-limit per-port** *pps*	Configure the dhcp-guard rate-limit of the DHCP packet on the port, ranging from 1 to 9999, 150 by default.
DES-7200(config)# **dhcp-guard attack-threshold per-port** *pps*	Configure the dhcp-guard attack threshold, ranging from 1 to 9999, 300 by default. When the DHCP packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)#**nfpp dhcp-guard policy per-port** *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp dhcp-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

The source MAC address-based rate limit takes precedence over port-based rate limit.

12.6.8 Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts manually.

Command	Function
DES-7200# **clear nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	**clear nfpp dhcp-guard hosts:** Clear all isolated hosts. **clear nfpp dhcp-guard hosts vlan** *vid*: Clear all isolated hosts in a VLAN. **clear nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Clear all isolated hosts on a interface in a VLAN. **clear nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]: An isolated host has been cleared. Use the MAC address to identify the hosts.

12.6.9 Showing dhcp-guard

- Showing dhcp-guard configuration
- Showing monitored host configuration

12.6.9.1 Showing dhcp-guard configuration

Use this command to show the dhcp-guard configurations.

Command	Function
DES-7200# **show nfpp dhcp-guard summary**	Show the dhcp-guard configurations.

For example,

```
DES-7200# show nfpp dhcp-guard summary
（Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-ma
c/per-port.）
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable    300            -/5/150     -/10/300
G 0/1      Enable    180            -/6/-       -/8/-
G 0/2      Disable   200            -/5/30      -/10/50

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Note

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

12.6.9.2 Showing monitored host configuration

Command	Function
DES-7200# **show nfpp dhcp-guard hosts statistics**	Show the dhcp-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
DES-7200#**show nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	Show the isolated hosts information. **show nfpp dhcp-guard hosts vlan** *vid*: Show the isolated hosts in a VLAN. **show nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Show the isolated hosts on a interface in a VLAN. **show nfpp dhcp-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]: Show the isolated hosts. Use the MAC address to identify the hosts.

For example,

```
DES-7200#show nfpp dhcp-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120


DES-7200# show nfpp dhcp-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface   MAC address     remain-time(s)

----  --------    -----------     -------------
```

```
*1    Gi0/1      0000.0000.0001  110

2     Gi0/2      0000.0000.2222   61

Total: 2 host(s)
```

```
DES-7200# show nfpp dhcp-guard hosts vlan 1 interface g 0/1 0000.0000.0001
If column 1 shows '*', it means "hardware failed to isolate host".

VLAN  interface   MAC address     remain-time(s)

---- --------    -----------     -------------

 *1    Gi0/1     0000.0000.0001  110

Total: 1 host(s)
```

12.7 DHCPv6-guard

12.7.1 DHCPv6-guard Overview

The DHCPv6 protocol is widely used to dynamically allocate the IPv6 address in the LAN, and plays an important role in the network security. Being similar to the DHCP attack, the DHCPv6 attack occurs in the way of broadcasting the DHCPv6 request packets through faking the MAC address. If there are too many DHCPv6 request packets, the attacker may use up the addresses provided in the DHCPv6 server. To this end, a legal host fails to request for an IPv6 address and access to the network. The workaround for the DHCPv6 attack: one one hand, you may configure the DHCPv6 packet rate-limit; on the other hand, you may detect and isolate the attack source.

The DHCPv6 attack detection could be host-based or port-based. Host-based ARP attack detection adopts the combination of source IP address/VID/port-based. For each attack detection, you can configure the rate-limit threshold and warning threshold. The DHCPv6 packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCPv6 packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message. The host-based attack detection can isolate the attack source.

DHCPv6-guard configuration commands include:

- Enabling dhcpv6-guard
- Configuring the isolated time
- Configuring the monitored time
- Configuring the monitored host limit

- Host-based rate-limit and attack detection
- Port-based rate-limit and attack detection
- Clearing monitored host
- Showing related dhcpv6-guard information

12.7.2 Enabling DHCPv6-guard

You can enable dhcpv6-guard in the nfpp configuration mode or in the interface configuration mode. By default, the dhcpv6-guard is enabled.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcpv6-guard enable**	Enable the dhcpv6-guard. By default, dhcpv6-guard is enabled.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp dhcpv6-guard enable**	Enable the dhcpv6-guard on the interface. By default, dhcpv6-guard is not enabled on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcpv6-guard summary**	Show the configurations.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

With the dhcpv6-guard disabled, the monitored hosts are auto-cleared.

12.7.3 Configuring the isolated time

For the isolated time of the attacker, it can be configured in the global or interface configuration

mode. By default, the isolated time is configured in the global configuration mode.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcpv6-guard isolate-period** [*seconds* | **permanent**]	Configure the global isolated time, ranging 0s, 30-86400s(one day). The default value is 0s, representing no isolation. Permanent represents permanent isolation.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp arp-guard isolate-period** [*seconds* | **permanent**]	Configure the isolated time on the port, ranging 0s, 180-86400s(one day). By default, the isolated time is configured globally. 0s represents no isolation. Permanent represents permanent isolation.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcpv6-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the global isolated time to the default value, use the **no dhcpv6-guard isolate-period** command in the nfpp configuration mode. If the isolated time has been configured on a port, you can use the **no dhcpv6-guard isolate-period** command to remove the port-based isolated time configuration in the interface configuration mode.

12.7.4 Configuring the monitored time

If the isolated time is 0 (that is no isolation), the serviceview monitor will be performed to auto-monitor the attacker according to the configured monitored period, providing the attacker information in the system. If the isolated time is but not 0, the DHCPv6-guard will perform hardware isolation towards the hosts using the serviceview monitor.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.

Command	Function
DES-7200(config-nfpp)# **dhcpv6-guard monitor-period** *seconds*	Configure the monitored time, ranging 180-86400s(one day). The default value is 600s.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcpv6-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored time to the default value, use the **no dhcpv6-guard monitor-period** command in the nfpp configuration mode.

Caution

If the isolated time is 0, the serviceview monitor will be performed to monitor the detected attacker, and the timeout time will be the monitored period. In the process of the serviceview monitor, if the isolated time is but not 0, the hardware isolation will be performed to isolate the attacker, and the timeout time will be the isolated period. Only be the monitored period valid when the isolated period is 0.

Modifying the isolated time from non-0 to 0 removes the attackers from the interface rather than performs the serviceview monitor.

12.7.5 Configuring the monitored host limit

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcpv6-guard monitored-host-limit** *seconds*	Configure the monitored host limit, ranging 1-4294967295. The default value is1000.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcpv6-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

To restore the monitored host limit to the default value, use the **no dhcpv6-guard**

monitored-host-limit command in the nfpp configuration mode.

If the monitored host number has reached the default 1000, and the administrator sets the monitored host limit smaller than 1000, the existent moniored hosts will not be deleted and it will prompt the message "%ERROR: The value that you configured is smaller than current monitored hosts 1000, please clear a part of monitored hosts." to notify the administrator of the invalid configuration and removing a part of the monitored hosts.

Caution

It prompts the message that "% NFPP_DHCPV6_GUARD-4-SESSION_LIMIT: Attempt to exceed limit of 1000 monitored hosts." if the monitored host table is full.

12.7.6 Host-based rate-limit and attack detection

Use the source MAC/VID/port-based method to detect the host-based attack. For each attack detection, you can configure the rate-limit threshold and attack threshold (also called warning threshold). The DHCPv6 packet will be dropped when the packet rate exceeds the rate-limit threshold. When the DHCPv6 packet rate exceeds the warning threshold, it will prompt the warning messages and send the TRAP message.

It prompts the following message if the DHCPv6 DoS attack was detected:

```
%NFPP_DHCPV6_GUARD-4- DOS_DETECTED:Host<IP=N/A,MAC=0000.0000.0001,port=G
i4/1,VLAN=1> was detected. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
DHCPV6 DoS attack from host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>
 was detected.
```

If the isolated time is not set as 0 by the administrator, when the hardware isolation succeeds, it prompts:

```
%NFPP_DHCPV6_GUARD-4-ISOLATED:Host <IP= N/A,MAC=0000.0000.0001,port=Gi4/
1,VLAN=1> was isolated. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1> was isolated.
```

When it fails to isolate the hardware due to a lack of memory or hardware resources, it prompts:

```
%NFPP_DHCPV6_GUARD-4-ISOLATE_FAILED: Failed to isolate host <IP=N/A,MAC=0
000.0000.0001,port=Gi4/1,VLAN=1>. (2009-07-01 13:00:00)
```

The following example shows the describing information included in the sent TRAP messages:

```
Failed to isolate host<IP=N/A,MAC=0000.0000.0001,port=Gi4/1,VLAN=1>.
```

Caution When it fails to allocate the memory to the detected attackers, it prompts the message like "`%NFPP_DHCPV6_GUARD-4-NO_MEMORY: Failed to alloc memory.`" to inform the administrator.

This section shows the administrator how to configure the host-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **dhcpv6-guard rate-limit per-src-mac** *pps*	Configure the dhcpv6-guard rate-limit, ranging from 1 to 9999, 5 by default. **per-src-mac**: detect the hosts based on the source MAC address/VID/port;
DES-7200(config)# **dhcpv6-guard attack-threshold per-src-mac** *pps*	Configure the dhcpv6-guard attack threshold, ranging from 1 to 9999, 10 by default. When the DHCPv6 packet number sent from a host exceeds the attack threshold, the attack is detected and DHCPv6-guard isolates the host, records the message and sends the TRAP packet. **per-src-mac**: detect the hosts based on the source MAC address/VID/port;
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.

Command	Function
DES-7200(config-if)#nfpp dhcpv6-guard policy per-src-mac *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value. **per-src-mac:** to detect the hosts based on the source MAC/VID/port;
DES-7200(config-nfpp)**# end**	Return to the privileged EXEC mode.
DES-7200(config-if)**# show nfpp dhcpv6-guard summary**	Show the parameter settings.
DES-7200**# copy running-config startup-config**	Save the configurations.

12.7.7 Port-based rate-limit and attack detection

You can configure the dhcpv6-guard rate limt and attack threshold on the port. The rate limit value must be less than the attack threshold value. When the DHCPv6 packet rate on a port exceeds the limit, the DHCPv6 packets are dropped. When the DHCPv6 packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

It prompts the following message when the DHCPv6 DoS attack was detected on a port:

%NFPP_DHCPV6_GUARD-4-PORT_ATTACKED: DHCPV6 DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

DHCPV6 DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200**# configure terminal**	Enter the global configuration mode.
DES-7200(config)**# nfpp**	Enter the nfpp configuration mode.

Command	Function
DES-7200(config)# **dhcpv6-guard rate-limit per-port** *pps*	Configure the dhcpv6-guard rate-limit of the DHCPV6 packet on the port, ranging from 1 to 9999, 150 by default.
DES-7200(config)# **dhcpv6-guard attack-threshold per-port** *pps*	Configure the dhcpv6-guard attack threshold, ranging from 1 to 9999, 300 by default. When the DHCPV6 packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)#**nfpp dhcpv6-guard policy per-port** *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999 and by default, it adopts the global rate-limit threshold value. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999 and by default, it adopts the global attack threshold value.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp dhcpv6-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

The source MAC address-based rate limit takes precedence over port-based rate limit.

12.7.8 Clearing the monitored hosts

The isolated hosts can be recovered automatically after a period of the time. The administrator can use the following command to clear the isolated hosts

manually.

Command	Function
DES-7200# **clear nfpp dhcpv6-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	**clear nfpp dhcpv6-guard hosts:** Clear all isolated hosts. **clear nfpp dhcpv6-guard hosts vlan** *vid*: Clear all isolated hosts in a VLAN. **clear nfpp dhcpv6-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Clear all isolated hosts on a interface in a VLAN. **clear nfpp dhcpv6-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]: An isolated host has been cleared. Use the MAC address to identify the hosts.

12.7.9 Showing dhcpv6-guard

- Showing dhcpv6-guard configuration
- Showing monitored host configuration

12.7.9.1 Showing dhcpv6-guard configuration

Use this command to show the dhcpv6-guard configurations.

Command	Function
DES-7200# **show nfpp dhcpv6-guard summary**	Show the dhcpv6-guard configurations.

For example,

```
DES-7200# show nfpp dhcpv6-guard summary
（Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-m
ac/per-port.）
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable    300           -/5/150     -/10/300
G 0/1      Enable    180           -/6/-       -/8/-
G 0/2      Disable   200           -/5/30      -/10/50

Maximum count of monitored hosts: 1000
Monitor period：300s
```

Note

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of source IP address-based rate-limit threshold / source MAC address-based rate-limit threshold / port-based rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

12.7.9.2 Showing monitored host configuration

Command	Function
DES-7200# **show nfpp dhcpv6-guard hosts statistics**	Show the dhcpv6-guard hosts statistics, including total host amount, isolated host amount and non-isolated host amount.
DES-7200#**show nfpp dhcpv6-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]	Show the isolated hosts information. **show nfpp dhcpv6-guard hosts vlan** *vid*: Show the isolated hosts in a VLAN. **show nfpp dhcpv6-guard hosts** [**vlan** *vid*] [**interface** *interface-id*]: Show the isolated hosts on a interface in a VLAN. **show nfpp dhcpv6-guard hosts** [**vlan** *vid*] [**interface** *interface-id*] [*mac-address*]: Show the isolated hosts. Use the MAC address to identify the hosts.

For example,

```
DES-7200#show nfpp dhcpv6-guard hosts statistics
success    fail    total
-------    ----    -----
100        20       120


DES-7200# show nfpp dhcpv6-guard hosts
If column 1 shows '*', it means "hardware do not isolate user" .
VLAN  interface   MAC address     remain-time(s)
```

```
----  --------    -----------     -------------

*1    Gi0/1       0000.0000.0001  110

2     Gi0/2       0000.0000.2222   61

Total: 2 host(s)


DES-7200# show nfpp dhcpv6-guard hosts vlan 1 interface g 0/1 0000.0000.0001
If column 1 shows '*', it means "hardware failed to isolate host".

VLAN  interface   MAC address     remain-time(s)

---- --------    -----------     -------------

 *1    Gi0/1     0000.0000.0001  110

Total: 1 host(s)
```

12.8 ND-guard

12.8.1 ND-guard Overview

ND, the abbreviation of “Neighbor Discovery”, is responsible for the address resolution、router discovery、prefix discovery and the redirection. ND uses the following 5 types of the ND packets: Neighbor Solicitation、Neighbor Advertisement、Router Solicitation、Router Advertisement and Redirect, which are abbreviated as the NS、NA、RS and RA.

ND Snooping monitors the ND packets in the network, filters the illegal ND packets and associates the monitored IPv6 users with the interface to prevent the IPv6 address from being stolen. ND Snooping shall send the ND packets to the CPU at the configured rate-limit to implement the ND-guard function, for sending the ND packets at the high rate leads to the CPU attack.

ND-guard classifies the ND packets into the following three types: 1) NS-NA: the Neighbor Solicitation and the Neighbor Advertisement, used for the address resolution; 2) RS: the Router Solicitation, used for the gateway discovery by the host; 3) RA and Redirect: the Router Advertisement and Redirect, used to advertise the gateway and prefix, and the better next-hop.

At present, only the port-based ND packet attack detection is implemented. You may configure the rate-limit threshold and the attack threshold for the ND packets.

When the ND packet rate on a port exceeds the limit, the ND packets are dropped. When the ND packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

ND-guard configuration commands include:

- Enabling ND-guard
- Port-based rate-limit and attack detection
- Showing related dhcpv6-guard information

12.8.2 Enabling ND-guard

You can enable ND-guard in the nfpp configuration mode or in the interface configuration mode. By default, the ND-guard is enabled.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **nd-guard enable**	Enable the nd-guard. By default, nd-guard is enabled.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp nd-guard enable**	Enable the nd-guard on the interface. By default, nd-guard is not enabled on the interface.
DES-7200(config-if)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp dhcpv6-guard summary**	Show the configurations.
DES-7200# **copy running-config startup-config**	Save the configurations.

Caution

With the nd-guard disabled, the monitored hosts are auto-cleared.

12.8.3 Port-based rate-limit and attack detection

You can configure the ND-guard rate-limit and attack threshold on the port. The rate-limit value must be less than the attack threshold value. When the ND packet rate on a port exceeds the limit, the ND packets are dropped. When the ND packet rate on a port exceeds the attack threshold limit, the CLI prompts and the TRAP packets are sent.

ND Snooping divides the port into the untrusted port and the trusted port, which connect to the host and the gateway respectively. The rate-limit threshold for the trusted port shall be higher than the one for the untrusted port because the traffic for the trusted port is generally higher than the one for the untrusted port. With the ND Snooping enabled, the ND Snooping advertises the ND-guard to set the rate-limit threshold and the attack threshold of the ND packets on the trusted port as 800pps and 900pps respectively.

For the rate-limit threshold configured by the ND Snooping and the one configured by the administrator, the latter configured threshold value overwrites the former configured one.

When the administrator saves the settings, the rate-limit threshold configured by the ND Snooping saved into the configuration file.

It prompts the following message when the **NS-NA DoS attack** was detected on a port:

%NFPP_ND_GUARD-4-PORT_ATTACKED: **NS-NA** DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

NS-NA DoS attack was detected on port Gi4/1.

It prompts the following message when the **RS DoS attack** was detected on a port:

%NFPP_ND_GUARD-4-PORT_ATTACKED: RS DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

RS DoS attack was detected on port Gi4/1.

It prompts the following message when the **RA-REDIRECT DoS attack** was detected on a port:

%NFPP_ND_GUARD-4-PORT_ATTACKED: **RA-REDIRECT** DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The following is additional information of the sent TRAP packet :

RA-REDIRECT DoS attack was detected on port Gi4/1.

This section shows the administrator how to configure the port-based rate-limit and attack detection in the nfpp configuration mode and in the interface configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config)# **nd-guard rate-limit per-port [ns-na | rs | ra-redirect]** *pps*	Configure the rate-limit of the ND packets on the port, ranging from 1 to 9999, 15 by default.
DES-7200(config)# **nd-guard attack-threshold per-port [ns-na | rs | ra-redirect]** *pps*	Configure the attack threshold, ranging from 1 to 9999, 30 by default. When the ND packet number on a port exceeds the attack threshold, the CLI prompts and the TRAP packets are sent.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-name*	Enter the interface configuration mode.
DES-7200(config-if)# **nfpp nd-guard policy per-port [ns-na | rs | ra-redirect]** *rate-limit-pps attack-threshold-pps*	Configure the rate-limit and attack threshold on the specified interface. *rate-limit-pps:* set the rate-limit threshold. The valid range is 1-9999. *attack-threshold-pps:* set the attack threshold. The valid range is 1-9999.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200(config-if)# **show nfpp nd-guard summary**	Show the parameter settings.
DES-7200# **copy running-config startup-config**	Save the configurations.

12.8.4 Showing dhcpv6-guard

- Showing ND-guard configuration

12.8.4.1 Showing ND-guard configuration

Use this command to show the ND-guard configurations.

Command	Function
DES-7200# **show nfpp nd-guard summary**	Show the ND-guard configurations.

For example,

```
DES-7200# show nfpp nd-guard summary
（Format of column Rate-limit and  Attack-threshold is NS-NA/RS/RA-REDIRECT.）
Interface  Status  Rate-limit Attack-threshold
Global     Enable  20/5/10    40/10/20
G 0/1      Enable  15/15/15   30/30/30
G 0/2      Disable -/5/30      -/10/50
```

Note

Field	Description
Interface	Global refers to the global configuration.
Status	Enable/disable the arp-guard.
Rate-limit	In the format of NS-NA rate-limit threshold / RS rate-limit threshold / RA-redirect rate-limit threshold.
Attack-threshold	In the same format of the Rate-limit.
-	No configuration.

12.9 Defined-guard

12.9.1 Defined-guard Overview

There are a great variety of network protocols, including such routing protocols as OSPF, BGP, RIP and etc. Protocol communication is realized by exchanging packets between different devices, and the exchange packets must be delivered to the CPU in order to be processed by respective protocols. Once a protocol is running on the network device, a "window" is opened to potential attackers. If the attacker sends excessive protocol packets to the network device, the CPU resource of the device will be heavily consumed, and the device may not work properly.

Given the diversity of network protocols and the fact that different protocols may be used under different user environment during sustainable development, DES-7200 devices have provided the feature of Defined Guard to allow users to define guard against various attacks, so as meet different attack protection needs.

12.9.1.1 Define-guard Policy

The administrator can define a guard policy in NFPP configuration mode. Defined Guard requires that the user must configure packet type, rate-limiting threshold, attack threshold and how to identify such basic information. The type of Defined Guard will only take effect after configuring the basic information.

The user-defined packet type may include Ethernet link layer type (etype), source MAC address (smac), destination MAC address (dmac), IPv4/v6 protocol number (protocol), source IPv4/v6 address (sip), destination IPv4/v6 address (dip), source transport layer port (sport) and destination transport layer port (dport).

Defined Guard must configure how to take classified statistics of the data rate of defined type of packets, including source IP/VID/port based data rate statistics, source MAC/VID/port based data rate statistics and port-based data rate statistics, or any combination thereof. You must configure the corresponding rate-limiting threshold and attack threshold for these classes. The class will only take effect after configuring the rate-limiting threshold and attack threshold for such class.

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.
DES-7200(config-nfpp)#define *name*	Configure the name of defined guard type
DES-7200(config-nfpp-define)# match [etype *type***] [src-mac** *smac* **[src-mac-mask** *smac_mask***]] [dst-mac** *dmac* **[dst-mac-mask** *dst_mask***]] [protocol** *protocol* **] [src-ip** *sip* **[src-ip-mask** *sip-mask***]] [src-ipv6** *sipv6* **[src-ipv6-masklen** *sipv6-masklen***]] [dst-ip** *dip* **[dst-ip-mask** *dip-mask***]] [dst-ipv6** *dipv6* **[dst-ipv6-masklen** *dipv6-masklen***]][src-port** *sport***] [dst-port** *dport***]**	Configure the packet fields to be matched by the defined guard type. By default, **src-mac-mask, dst-mac-mask, src-ip-mask** and **dst-ip-mask** are all 1, and **src-ipv6-masklen** and **dst-ipv6-masklen** are all 128. **Protocol** will only take effect when **etype** is ipv4 or ipv6; **src-ip** and **dst-ip** will only take effect when **etype** is ipv4; **src-ipv6** and **dst-ipv6** will only take effect when **etype** is ipv6; **src-port** and **dst-port** will only take effect when **protocol** is tcp or udp.

DES-7200(config-nfpp-define)# define-policy {per-src-ip | per-src-mac | per-port} *rate-limit-pps attack-threshold-pps*	Configure host-based or port-based rate-limiting threshold and attack threshold. **per-src-ip** means to take statistics of data rate as per source IP/VID/port; **per-src-mac** means to take statistics of data rate as per source MAC/VID/port. **per-port** means to take statistics of data rate as per each packet-receiving physical port. You must configure any of **per-src-ip, per-src-mac** and **per-port**, or else the policy won't take effect. **per-src-ip** will only take effect when **etype** is ipv4 or ipv6. *Rate-limit-pps* means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded. *Attack-threshold-pps* means the attack threshold (1-9999). By default, no rate limiting will be implemented. The attack threshold must be greater than or equal to the rate-limiting threshold.
DES-7200#show nfpp define summary *name*	Verify configurations.
DES-7200#copy running-config startup-config	Save configurations.

To delete the defined guard type, execute "**no nfpp define name**" in NFPP configuration mode. Deleting defined guard type will delete all related configurations, including global and interface based configurations and all isolated hosts.

The name of defined guard type cannot be repeated. The field and value to be matched cannot be completely same or be same with the guard type of arp, icmp, dhcp, ip, or dhcpv6. When the configured type is repeated, the system will prompt configuration failure.

When the match type and value of defined guard are completely the same with the existing defined guard type, the following prompting message will be displayed: "%ERROR: the match type and value are the same with define name (name of the existing defined guard type)", indicating that the configuration has failed.

Caution

When protocol has been configured for the match field but etype is neither IPv4 or IPv6, the following prompting message will be displayed: "%ERROR：protocol is valid only when etype is IPv4 (0x0800) or IPv6 (0x86dd)."

When src-ip and dst-ip have been configured for the match field but etype is not IPv4, the following prompting message will be displayed: "%ERROR：IP address is valid only when etype is IPv4 (0x0800)."

When src-ipv6 and dst-ipv6 have been configured for the match field but etype is not IPv6, the following prompting message will be displayed: "%ERROR：IPv6 address is valid only when etype is IPv6 (0x86dd)."

When src-port and dst-port have been configured for the match field but protocol is not TCP or UDP, the following prompting message will be displayed: "%ERROR：Port is valid only when protocol is TCP (6) or UDP (17)."

12.9.1.2 Common Define-guard Policy

The following table shows the guard policies corresponding to certain commonly used network protocols. The corresponding rate-limiting threshold and attack threshold can meet the needs in most application scenarios. The network administrator shall configure effective rate-limiting threshold and attack threshold according to the actual application scenario.

Protocol	match	policy per-src-ip	policy per-src-mac	policy per-port
RIP	etype 0x0800 protocol 17 dst-port 520	rate-limit 100 attatch-threshold 150	Not applicable	rate-limit 300 attatch-threshold 500

RIPng	etype 0x86dd protocol 17 dst-port 521	rate-limit 100 attatch-threshold 150	Not applicable	rate-limit 300 attatch-threshold 500
BGP	etype 0x0800 protocol 6 dst-port 179	rate-limit 1000 attatch-threshold 1200	Not applicable	rate-limit 2000 attatch-threshold 3000
BPDU	dst-mac 0180.c200.0000	Not applicable	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
RERP	dst-mac 01d0.f800.0001	Not applicable	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
REUP	dst-mac 01d0.f800.0007	Not applicable	rate-limit 20 attatch-threshold 40	rate-limit 100 attatch-threshold 100
BGP	etype 0x0800 protocol 6 dst-port 179	Not applicable	Not applicable	Not applicable
OSPFv2	etype 0x0800 protocol 89	rate-limit 800 attatch-threshold 1200	Not applicable	rate-limit 2000 attatch-threshold 3000
OSPFv3	etype 0x86dd protocol 89	rate-limit 800 attatch-threshold 1200	Not applicable	rate-limit 2000 attatch-threshold 3000
VRRP	etype 0x0800 protocol 112	rate-limit 64 attatch-threshold 100	Not applicable	rate-limit 1024 attatch-threshold 1024

IPv6 VRRP	etype 0x86dd protocol 112	rate-limit 64 attatch-threshold 100	Not applicable	rate-limit 1024 attatch-threshold 1024
SNMP	etype 0x0800 protocol 17 dst-port 161	rate-limit 1000 attatch-threshold 1200	Not applicable	rate-limit 2000 attatch-threshold 3000
RSVP	etype 0x0800 protocol 46	rate-limit 800 attatch-threshold 1200	Not applicable	rate-limit 1200 attatch-threshold 1500
LDP (UDP hello)	etype 0x0800 protocol 17 dst-port 646	rate-limit 10 attatch-threshold 15	Not applicable	rate-limit 100 attatch-threshold 150

Caution

Defined guard is intended to furthest include existing protocol types and facilitate new protocol type extension. It allows free combinations of type fields. If improperly configured, it will result in abnormal network. Therefore, the network administrator shall have a good command of network protocols. This table shows the effective configurations for popular protocols, and the administrator can configure accordingly. For other protocols which have been listed in the table, configurations shall be made with caution.

12.9.1.3 Configuring Attacker Isolation Period

By default, the attacker isolation period is 0, namely the attacker won't be isolated.

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.
DES-7200(config-nfpp)#define *name*	Enter defined guard configuration mode

DES-7200(config-nfpp)#isolate-period {*seconds* | **permanent**}	Configure attacker isolation period Range: 0 and 30-86400 seconds (i.e., one day); default value is 0 second, meaning no isolation; **permanent** means permanent isolation.
DES-7200(config-nfpp)#end	Return to privilege mode.
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#interface *interface-name*	Enter interface configuration mode.
DES-7200(config-if)# nfpp define *name* **isolate-period** {*seconds* | **permanent**}	Configure attacker isolation period on the port. Range: 0 and 180-86400 seconds (i.e., one day). By default, the local isolation period is not configured, and the global isolation period will be used. The value of 0 means no isolation, and **permanent** means permanent isolation.
DES-7200(config-if)#end	Return to privileged mode.
DES-7200#show nfpp define summary *name*	Verify configurations.
DES-7200#copy running-config startup-config	Save configurations.

To restore global isolation period to the default value, execute "**no isolate-period**" command in NFPP defined guard configuration mode. If one port has been configured with local isolation period and it is now expected to apply the global isolation period, execute "**no nfpp define** *name* (name of defined guard) **isolate-period**" in interface configuration mode to delete the configuration of local isolation period.

12.9.1.4 Configuring Attacker Monitoring Period

If the isolation period is 0 (i.e., no isolation), the guard module will automatically monitor the attacker as per the monitoring period configured and provide information about the existing attackers in the system. When the isolation period is configured to a non-zero value, the guard module will automatically isolate the host being monitored.

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.
DES-7200(config-nfpp)#define *name*	Enter defined guard configuration mode

DES-7200(config-nfpp)# monitor-period *seconds*	Configure attacker monitoring period. Range: 180-86400 seconds (i.e., one day); default value is 600 seconds.
DES-7200(config-nfpp)#end	Return to privileged mode.
DES-7200#show nfpp define summary *name*	Verify configurations.
DES-7200#copy running-config startup-config	Save configurations.

To restore the monitoring period to default value, execute "**no monitor-period**" command in NFPP defined guard configuration mode.

Caution

When an attacker is detected and if the isolation period is 0, the attacker will be monitored, and the timeout timer is the monitoring period. During the process of software monitoring, when the isolation period is configured to a non-zero value, the attacker being monitored will be automatically isolated at hardware layer, and the timeout timer is the isolation period. The monitoring period will only make sense when the isolation period is 0.

Changing isolation period from a non-zero value to zero will directly delete the attackers on the relevant port instead of implementing software monitoring.

12.9.1.5 Configuring the Maximum Number of Monitored Hosts

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.
DES-7200(config-nfpp)#define *name*	Enter defined guard configuration mode
DES-7200(config-nfpp)#monitored-host-limit *number*	Configure the maximum number of monitored hosts Range: 1-4294967295. By default, the maximum number of monitored hosts is 1000.
DES-7200(config-nfpp)#end	Return to privileged mode.
DES-7200#show nfpp define summary *name*	Verify configurations.
DES-7200#copy running-config startup-config	Save configurations.

To restore the maximum number of monitored hosts to default value, execute "**no monitored-host-limit**" command in NFPP defined guard configuration mode.

If the maximum number of monitored hosts has reached the default value of 1000 and the administrator configures a value lower than 1000 by this time, the existing hosts being monitored won't be deleted, but the following message will be displayed to remind the administrator to clear a certain part of monitored hosts in order to effect the configuration: "%ERROR: The value that you configured is smaller than current monitored hosts 1000 (number of monitored hosts configured), please clear a part of monitored hosts."

Caution

When the table of monitored hosts is full, the following message will be displayed to remind the administrator: "% NFPP_DEFINE-4-SESSION_LIMIT: Attempt to exceed limit of name (name of defined guard type)'s 1000 (number of monitored hosts configured) monitored hosts."

12.9.1.6 Configuring the Trusted Hosts Exempt from Monitoring

If the administrator expects not to monitor a host (i.e., the host is trusted), the command can be configured. IP packets from trusted hosts are allowed to be sent to the CPU. Trusted hosts can only be added after configuring the match rule.

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.
DES-7200(config-nfpp)#define *name*	Enter NFPP defined guard configuration mode
DES-7200(config-nfpp-define)#trusted-host {*mac mac_mask* | *ip mask* | *IPv6/prefixlen*}	Configure trusted hosts exempt from monitoring. You can configure up to 500 entries.
DES-7200(config-nfpp-define)#end	Return to privileged mode.
DES-7200# show nfpp define trusted-host *name*	Display the trusted hosts configured.
DES-7200#copy running-config startup-config	Save configurations.

In NFPP defined guard configuration mode, execute the corresponding "no" command to delete one entry of trusted host. Use "no" form of this command and "all" option to delete all trusted hosts.

To delete all trusted hosts:

DES-7200(config-nfpp-define)# **no trusted-host all**

Or to delete one trusted host:

DES-7200(config-nfpp)# **no trusted-host** *1.1.1.1 255.255.255.255*

When match rule is not configured, the following prompting message will be displayed: "%ERROR: Please configure match rule first."

While adding an IPv4 trusted host but the etype of match rule is not IPv4, the following prompting message will be displayed: "%ERROR: Match type can't support IPv4 trusted host."

While adding an IPv6 trusted host but the etype of match rule is not IPv6, the following prompting message will be displayed: "%ERROR: Match type can't support IPv6 trusted host."

When the table of trusted hosts is full, the following prompting message will be displayed: "％ERROR: Attempt to exceed limit of 500 trusted hosts.".

When the table of monitored hosts contains an entry matching a trusted host (with same IP address), the system will automatically delete the corresponding entry of this IP address.

Caution

When it is failed to delete a trusted host, the following prompting message will be displayed "％ERROR: Failed to delete trusted host 1.1.1.0 255.255.255.0 (the trusted host configured)."

When it is failed to add a trusted host, the following prompting message will be displayed "％ERROR: Failed to add trusted host 1.1.1.0 255.255.255.0 (the trusted host configured)."

When a trusted host to be added exists already, the following prompting message will be displayed "％ERROR: Trusted host 1.1.1.0 255.255.255.0 (the trusted host configured) has already been configured."

When a trusted host to be deleted doesn't exist, the following prompting message will be displayed "％ERROR: Trusted host 1.1.1.0 255.255.255.0 (the trusted host configured) is not found."

When it is unable to allocate memory for a trusted host, the following message will be displayed "％ERROR: Failed to allocate memory."

12.9.1.7 Host-based rate-limit and attack detection

The host detection method shall be determined according to the guard policy, including host detection based on source IP/VID/Port (per-src-ip) and host detection based on source MAC/VID/Port (per-src-mac). These two methods can apply or not at the same time. To effect host detection, the user must configure the rate-limiting threshold and attack threshold for such method. Each host has rate-limiting threshold and attack threshold (also called the alert threshold), and the rate-limiting threshold shall be lower than the attack threshold. When the data rate of defined type of packets from a single host exceeds the rate-limiting threshold, the excessive packets will be discarded. If the data rate of defined type of packets from a single host exceeds the attack threshold, the host will be isolated and logged, and the Trap will be sent as well.

When attack is detected, the following log information will be displayed:

%NFPP_DEFINE_GUARD-4- DOS_DETECTED: Host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> was detected by name(name of defined guard). (2009-07-01 13:00:00)

The Traps sent will include the following descriptive information:

Name (guard name) DoS attack from host<IP=1.1.1.1, MAC= N/A,port=Gi4/1,VLAN=1> was detected.

If the administrator sets the isolation period to a non-zero value, the following log information will be displayed when hardware isolation is successful:

%NFPP_DEFINE_GUARD-4-ISOLATED: Host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> was isolated by name (name of defined guard). (2009-07-01 13:00:00)

The Traps sent will include the following descriptive information:

Host<IP=1.1.1.1,MAC=N/A,port=Gi4/1,VLAN=1> was isolated by name (name of defined guard).

If hardware isolation is failed (generally due to insufficient memory of insufficient hardware resources), the following log information will be displayed:

%NFPP_DEFINE_GUARD-4-ISOLATE_FAILED:Failed to isolate host<IP=1.1.1.1, MAC= N/A ,port=Gi4/1,VLAN=1> by name (name of defined guard).(2009-07-01 13:00:00)

The Traps sent will include the following descriptive information:

Failed to isolate host<IP=1.1.1.1,MAC= N/A,port=Gi4/1,VLAN=1> by name (name of defined guard).

The administrator can configure in NFPP defined guard configuration mode and interface

configuration mode:

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.
DES-7200(config-nfpp)#define *name*	Enter NFPP defined guard configuration mode.
DES-7200(config-nfpp-define)# define-policy {per-src-ip | per-src-mac} *rate-limit-pps attack-threshold-pps*	Configure host-based rate-limiting threshold and attack threshold. **per-src-ip** means to take data rate statistics of the host detected as per source IP/VID/port, while **per-src-mac** means to take data rate statistics of the host detected as per source MAC/VID/port. *Rate-limit-pps* means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded. *Attack-threshold-pps* means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent and the user will be isolated as per the isolation period configured. By default, no rate limiting will be implemented. The attack threshold must be greater than or equal to the rate-limiting threshold.
DES-7200(config-nfpp)#end	Return to privileged mode.
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#interface *interface-name*	Enter interface configuration mode.

DES-7200(config-if)#nfpp define *name* **policy {per-src-ip | per-src-mac}** *rate-limit-pps attack-threshold-pps*	The local rate-limiting threshold and attack threshold configured will only apply to the associated port. **per-src-ip** means to take data rate statistics of the host detected as per source IP/VID/port, while **per-src-mac** means to take data rate statistics of the host detected as per source MAC/VID/port. *Rate-limit-pps* means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded. *Attack-threshold-pps* means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent and the user will be isolated as per the isolation period configured. By default, the globally configured rate-limiting threshold and attack threshold will be used. The attack threshold must be greater than or equal to the rate-limiting threshold.
DES-7200(config-if)#end	Return to privileged mode.
DES-7200#show nfpp define summary *name*	Verify configurations.
DES-7200#copy running-config startup-config	Save configurations.

Caution

The priority of source MAC/VID/port based rate limiting is higher than that of source IP/VID/port based rate limiting.

The policy of port-based host detection shall be same with the global policy.

If per-src-ip policy is not configured globally, when configuring per-src-ip policy on the port, the following message will be displayed to remind the administrator that the configuration has failed: "%ERROR: name (name of defined guard) has not per-src-ip policy."

If per-src-mac policy is not configured globally, when configuring per-src-mac policy on the port, the following message will be displayed to remind the administrator that the configuration has failed: "%ERROR: name (name of defined guard) has not per-src-mac policy."

When it is unable to allocate memory for the attacker detected, the following message will be displayed to remind the administrator: "%NFPP_DEFINE_GUARD-4-NO_MEMORY: Failed to allocate memory."

12.9.1.8 Port-based rate-limit and attack detection

You can configure port-based rate-limiting threshold and attack threshold for the guard policy, and the rate-limiting threshold shall be lower than the attack threshold. When the data rate of defined type of packets from certain port exceeds the rate-limiting threshold, the excessive packets will be discarded. If the data rate of defined type of packets from certain port exceeds the attack threshold, the port will be logged and the Trap will be sent as well.

When the port is subject to ARP DoS attack, the following alert message will be displayed:

%NFPP_DEFINE_GUARD-4-PORT_ATTACKED: name (name of defined guard) DoS attack was detected on port Gi4/1. (2009-07-01 13:00:00)

The Traps sent will include the following descriptive information:

Name (name of defined guard) DoS attack was detected on port Gi4/1.

The administrator can configure in NFPP defined guard configuration mode and interface configuration mode:

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.

DES-7200(config-nfpp)#define *name*	Enter NFPP defined guard configuration mode
DES-7200(config-nfpp-define)# define-policy per-port *rate-limit-pps attack-threshold-pps*	Configure host-based rate-limiting threshold and attack threshold. **per-port** means to take data rate statistics as per the physical port receiving packets. *Rate-limit-pps* means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded. *Attack-threshold-pps* means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent and the user will be isolated as per the isolation period configured. By default, the globally configured rate-limiting threshold and attack threshold will be used. The attack threshold must be greater than or equal to the rate-limiting threshold.
DES-7200(config-nfpp)#end	Return to privileged mode.
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#interface *interface-name*	Enter interface configuration mode.

DES-7200(config-if)#nfpp define *name* **policy per-port** *rate-limit-pps attack-threshold-pps*	The local rate-limiting threshold and attack threshold configured will only apply to the associated port. **per-port** means to take data rate statistics as per the physical port receiving packets. *Rate-limit-pps* means the rate-limiting threshold (1-9999). By default, no rate limiting will be implemented. Packets exceeding the rate-limiting threshold will be discarded. *Attack-threshold-pps* means the attack threshold (1-9999). When the packets of defined type exceed the attack threshold, an attack is considered existing and will be logged. The traps will be sent. By default, no rate limiting will be implemented. The attack threshold must be greater than or equal to the rate-limiting threshold.
DES-7200(config-if)#end	Return to privileged mode.
DES-7200#show nfpp define summary *name*	Verify configurations.
DES-7200#copy running-config startup-config	Save configurations.

Caution	The priority of host-based rate limiting is higher than that of port-based rate limiting. If per-port policy is not configured globally, when configuring per-port policy on the port, the following message will be displayed to remind the administrator that the configuration has failed: "%ERROR: name (name of defined guard) has not per-port policy."

12.9.1.9 Applying Defined-guard

The administrator can apply defined guard in NFPP configuration mode or interface configuration mode. This feature is disabled by default.

Command	Function
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#nfpp	Enter NFPP configuration mode.
DES-7200(config-nfpp)# define *name* **enable**	Globally enable defined guard. By default, defined guard is enabled on all ports.
DES-7200(config-nfpp)#end	Return to privileged mode.
DES-7200#configure terminal	Enter global configuration mode.
DES-7200(config)#interface *interface-name*	Enter interface configuration mode.
DES-7200(config-if)#nfpp define *name* **enable**	Enable defined guard attack on the port. By default, the local switch is not configured on the port, and the global switch will be adopted.
DES-7200(config-if)#end	Return to privileged mode.
DES-7200#show nfpp define summary *name*	Verify configurations.
DES-7200#copy running-config startup-config	Save configurations.

To disable defined guard, execute "no define name enable" command in NFPP configuration mode to globally disable the feature of defined guard, or execute "no define name enable" command in interface configuration mode to disable defined guard configured on the interface (to restore defined guard on interface, enable defined guard globally).

Caution

When defined guard policy is not fully configured, the defined guard cannot be enabled, and the system will remind the user of the corresponding absent policy configurations.

When the name of defined attack doesn't exist, the following prompting message will be displayed: "%ERROR: The name is not exist."

When match type is not configured for the defined guard, the following prompting message will be displayed: "%ERROR: name (name of defined guard) doesn't match any type."

When the policy is not configured for the defined guard, the following prompting message will be displayed: "%ERROR: name (name of defined guard) doesn't specify any policy."

12.9.1.10 Clearing Monitored Hosts

Isolated hosts will be released after certain period. To manually clear this host, the administrator can execute the following commands in the privileged mode.

Command	Function
DES-7200# clear nfpp define hosts *name* [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]	The parameters define the specific hosts to be cleared.

12.9.1.11 Showing Defined-guard

12.9.1.11.1 Showing defined guard configuration

Execute "**show nfpp define summary**" command to display defined guard configurations:

Command	Function
DES-7200#show nfpp define summary [*name*]	Display defined guard configurations. If "name" is not specified, the configurations of all defined guard policies will be displayed.

An example is shown below:

```
DES-7200# show nfpp define summary tcp
Define tcp summary:
match etype 0x0800 protocol 0x06
Maximum count of monitored hosts: 1000
Monitor period: 300s
(Format of column Rate-limit and  Attack-threshold is per-src-ip/per-src-ma
c/per-port.)
Interface  Status  Isolate-period Rate-limit Attack-threshold
Global     Enable  300            -/5/150    -/10/300
G 0/1      Enable  180            -/6/-      -/8/-
G 0/2      Disable 200            -/5/30     -/10/50
```

12.9.1.11.2 Showing information about monitored hosts

Command	Function
DES-7200# show nfpp define hosts *name* [**statistics** | [**vlan** *vid*] [**interface** *interface-id*] [*ip-address*] [*mac-address*]]]	Display hosts detected to be under attack. If no parameter is specified, all hosts detected to be under attack will be displayed. The parameters define the specific hosts to be displayed.

An example is shown below:

```
DES-7200#show nfpp define hosts tcp statistics
Define tcp:
```

```
success    fail    total
-------    ----    -----
100         20       120
Meaning: Totally 120 hosts are isolated, including 100 successful hosts and
20 failed hosts.

DES-7200#show nfpp define hosts tcp
Define tcp:
If column 1 shows '*', it means "hardware do not isolate host" .
VLAN  interface    IP address  remain-time(s)
----    --------   ---------    -------------
1     Gi0/1        1.1.1.1    110
*2     Gi0/2        1.1.2.1    61
Total: 2 host(s)
```

Note

The above fields mean VLAN ID, port, IP address, MAC address and remaining time of isolation.

If "*" is displayed before the first column of fine line, it means that this host is currently subject to software monitoring or the hardware isolation has failed due to insufficient resources. When etype is IPv6, source IP based host isolation users will be displayed in the form of IPv6 address, and source MAC based host isolation users will be displayed in the form of MAC address.

12.9.1.11.3 Showing trusted hosts exempt from monitoring

Execute "**show nfpp define trusted-host**" to display trusted hosts exempt from monitoring.

Command	Function
DES-7200#show nfpp define trusted-host *name*	Display trusted hosts exempt from monitoring.

An example is shown below:

```
DES-7200# show nfpp define trusted-host tcp
Define tcp:
IP address      mask
---------       ------
1.1.1.0         255.255.255.0
1.1.2.0         255.255.255.0
Total: 2 record(s)
```

12.10 NFPP Syslog

12.10.1 NFPP Syslog Overview

A NFPP log is generated in the NFPP syslog buffer area after detecting the attack. Use the NFPP log to generate the syslog at the specified rate and delete the NFPP log from the NFPP syslog buffer area.

NFPP syslog configuration commands include:

- Configuring NFPP log-buffer entry number
- Configuring the rate of generating NFPP syslog
- Configuring NFPP log filtering
- Clearing NFPP syslog
- Showing NFPP syslog

12.10.2 Configuring NFPP log-buffer entry number

The administrator can configure the NFPP log-buffer entry number in the nfpp configuration mode.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **log-buffer entries** *number*	Configure the NFPP log-buffer area size(in the range of 0-1024), 256 by default.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp log summary**	Show the configurations.

12.10.3 Configuring the rate of generating NFPP syslog

The administrator can configure the rate of generating the NFPP syslog in the nfpp configuration mode.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.
DES-7200(config-nfpp)# **log-buffer logs** *number_of_message* **interval** *length_in_seconds*	Set the rate of generating the syslog from the NFPP syslog buffer area. *number_of_message /length_in_seconds:* The rate of generating the syslog. The correspondent information in the NFPP syslog buffer area will be removed while generating the syslog. *number_of_message:* The valid range is 0-1024, the default value is 1. 0 indicates that all syslogs are recorded in the NFPP syslog buffer area and the syslog is not generated. *length_in_seconds:* The valid range is 0-86400s(one day), the default value is 30s. 0 indicates to generate the syslog immediately. Setting the *number_of_message* and the *length_in_seconds* 0 indicates to generate the syslog immediately.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp log summary**	Show the configurations.

12.10.4 Configuring NFPP syslog filtering

The administrator can filter the NFPP syslog and record the syslog in the specific VLAN or on the specific interface.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **nfpp**	Enter the nfpp configuration mode.

Command	Function
DES-7200(config-nfpp)# **logging vlan** *vlan-range* DES-7200(config-nfpp)# **logging interface** *interface-id*	Specify the syslog recorded in the VLAN; Specify the syslog recorded on the port. By default, all syslogs are recorded.
DES-7200(config-nfpp)# **end**	Return to the privileged EXEC mode.
DES-7200# **show nfpp log summary**	Show the configurations.

12.10.5 Clearing NFPP syslog

Command	Function
DES-7200# clear nfpp log	Clear the NFPP syslog in the log-buffer area.

12.10.6 Showing NFPP syslog

Command	Function
DES-7200# show nfpp log summary	Show the NFPP syslog configuration.
DES-7200# show nfpp log buffer [**statistics**]	Show the NFPP syslog in the log-buffer area. The parameter **statistics** shows the log number in the log-buffer area.

The following example shows the NFPP syslog configuration:

```
DES-7200#show nfpp log summary
Total log buffer size : 10
Syslog rate : 1 entry per 2 seconds
Logging:
    VLAN  1-3, 5
    interface Gi 0/1
    interface Gi 0/2
```

The following example shows the NFPP syslog number in the log-buffer area:

```
DES-7200#show nfpp log buffer statistics
```

```
There are 6 logs in buffer.
```

The following example shows the NFPP syslog buffer area:

```
DES-7200#show nfpp log buffer
Protocol VLAN  Interface IP address MAC address    Reason         Timestamp
------- ----  --------  ---------  -----------    ------         ---------
ARP     1     Gi0/1     1.1.1.1     -             DoS            2009-05-30 16:23:10
ARP     1     Gi0/1     1.1.1.1     -             ISOLATED       2009-05-30 16:23:10
ARP     1     Gi0/1     1.1.1.2     -             DoS            2009-05-30 16:23:15
ARP     1     Gi0/1     1.1.1.2     -             ISOLATE_FAILED 2009-05-30 16:23:15
ARP     1     Gi0/1     -         0000.0000.0001  SCAN           2009-05-30 16:30:10
ARP     -     Gi0/2     -         -               PORT_ATTACKED  2009-05-30 16:30:10
```

Field	Description
Protocol	Includes ARP、IP、ICMP、DHCP、DHCPv6、NS-NA、RS、RA-REDIRECT
Reason	Includes DoS、ISOLATED、ISOLATED_FAILED、SCAN、PORT_ATTACKED.

Caution

If the syslog buffer area is full, the subsequent syslog will be discarded and an entry with all attributes "-" will be shown in the syslog buffer area. The administrator shall increase the capacity of the syslog buffer area or improve the rate of generating the syslog.

The syslog that generated from the syslog buffer area carries with the event timestamp, for example:

```
%NFPP_ARP_GUARD-4-DOS_DETECTED:
Host<IP=N/A,MAC=0000.0000.0004,port=Gi4/1,VLAN=1> was
detected.(2009-07-01 13:00:00)
```

DES-7200

ACL&QoS Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)
Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 Access Control List Configuration

1.1 Overview

As part of our security solution, ACL is used to provide a powerful data flow filtering function. At present, our product supports the following access lists:

- IP access control list(Standard/Extended)
- MAC extended access control list
- Expert extended access control list
- IPV6 extended access control list

Depending on the conditions of networks, you can choose different access control lists to control data flows.

1.1.1 Access Control List Introduction

ACLs is the shortened form of Access Control Lists, or Access Lists. It is also popularly called firewall, or packet filtering in some documentation. ACL controls the messages on the device interface by defining some rules: Permit or Deny. According to usage ranges, they can be divided into ACLs and QoS ACLs.

By filtering the data streams, you can restrict the communication data types in the network and restrict the users of the network and the device they can use. When data streams pass the switch, ACLs classify and filter them, that is, check the data streams input from the specified interface and determine whether to permit or deny them according to the matching conditions.

To sum up, the security ACL is used to control which dataflow is allowed to pass through the network device. The QoS policy performs priority classification and processing for the dataflow.

ACLs consist of a series of entries, known as Access Control Entry (ACE). Each entry specifies its matching condition and behavior.

Access list rules can be about the source addresses, destination addresses, upper layer protocols, time-ranges or other information of data flows.

1.1.2 Why to Configure Access Lists

There are many reasons why we need configure access lists. Some of them are as follows:

- Restrict route updating: Control where to send and receive the route updating information.
- Restrict network access: To ensure network security, by defining rules, make users unable to access some services. (When a user only need access the WWW and E-mail services, then other services like TELNET are disabled). Or, allow users to access services only during a given period or only allow some hosts to access networks.

Figure 1 is a case. In the case, only host A is allowed to access Finance Network, while Host B is disallowed to do so. See Figure 1.

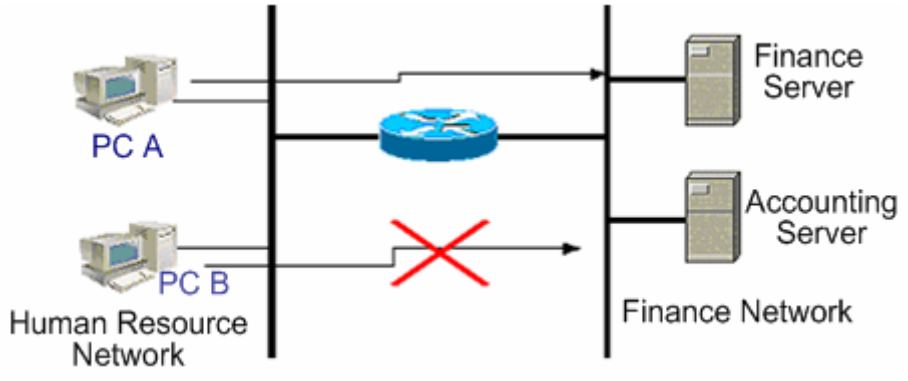


Figure 1 Using Access List to Control Network Access

1.1.3 When to Configure Access Lists

Depending on your requirements, you can select the basic access list or dynamic access list. In general, the basic access list can meet the security requirement.However, experienced hackers may use some software spoof source address and cheat the devices so as to gain accesses. Before the user can access the network, the dynamic access list requires the pass of authentication so that the hackers are difficult to invade the network. So, in some sensitive areas the dynamic access list can be used to ensure the network security.

Note

A inherent problem of all access lists is electric spoofing, the behavior of providing spoof source addresses to deceive switches Even you use the dynamic list, a spoofing problem occurs. During the valid access period of an authenticated user, a hacker may use a counterfeit user address and accesses the network. There are two methods to resolve the problem. One method is to set free time for a user to access the network as little as possible, making it hard for a hacker to attack the network. Another method is to use the IPSEC encryption protocol to encrypt network data, ensuring that all the data entering switches are encrypted.

Access lists are usually configured in the following locations of network devices:

- Devices between the inside network and outside network (such as the Internet)
- Devices at the borders of two parts in a network
- Devices on the access control port

The execution of the ACL statements must follow the order in the table strictly. Starting from the first statement, once the header of a packet matches a conditional judge statement in the table, the sequential statements are ignored.

1.1.4 Input/Output ACL, Filtering Domain Template and Rule

When a device interface receives a message, the input ACL checks whether the message matches an ACE of the ACL input on the interface. When a device interface is ready to output a message, the output ACL checks whether the message matches an ACE of the ACL output on the interface.

When detailed filtering rules are formulated, all or some of the above eight items may be used. As long as the message matches one ACE, the ACL processes the message as the ACE defined (permit or deny). The ACE of an ACL identifies Ethernet messages according to some fields of Ethernet messages. The fields include the following:

Layer-2 fields:

- 48-bit source MAC address (all the 48 bits must be declared)
- 48-bit destination MAC address (all the 48 bits must be declared)
- 16-bit layer-2 type field

Layer 3 fields:

- Source IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)
- Destination IP address field (you can specify all the 32 bits of the IP address, or specify a type of streams of the defined subnet)

- Protocol type fields

Layer-4 fields:

- You can specify one UDP source port, destination port, or both
- You can specify one UDP source port, destination port, or both

The filtering domain consists of the fields in the packets based on which the packets are identified and classified when you create an ACE. A filtering domain template is the definition formed by these fields. For example, when one ACE is generated, you want to identify and classify messages according to the destination IP field of a message. When another ACE is generated, you want to identify and classify messages according to the source IP address field of a message and the source port field of UDP. In this way, these two ACEs use different filtering domain templates.

Rules refer to the values of the ACE mask. For example, one ACE is:

permit tcp host *192.168.12.2* **any eq telnet**

In this ACE, the filtering domain template is a collection of the following fields: Source IP Address Fields, IP Protocol Fields and Destination TCP Port Fields. Corresponding values (rules) are respectively as follows: Source IP Address=host 192.168.12.2; IP Protocol=tcp; TCP Destination Port=telnet.

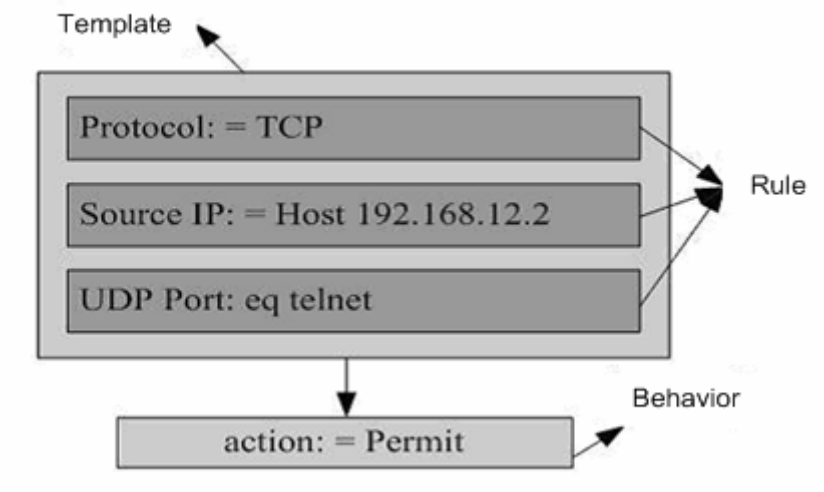


Figure 2 Analysis of the ACE: permit tcp host 192.168.12.2 any eq telnet

Note

A filtering domain template can be the collection of L3 fields (Layer 3 Field) and L4 fields (Layer 4 Field) or the collection of multiple L2 fields (Layer 2 Field). However, the filtering domain templates of a standard and extended ACL cannot be the collection of L2 and L3, L2 and 4, L2 and L3, or L4 fields. To use the combination of L2, L3 and L4 fields, it is possible to apply the Expert ACLs.

1. When associating SVI with the ACL at the outbounding direction, you should note that:

- Standard IP ACL, extended IP ACL, extended MAC ACL and expert ACL are supported.
- There are some limits on matching the destination IP address and the destination MAC address in an ACL. When you configure to match the destination MAC address in an extended MAC ACL or expert ACL and then apply this ACL to the outbounding direction of SVI, the entry will be set, but will not take effect. If you need to match the destination IP address not in the subnet IP range of the associated SVI in the standard IP ACL, extended IP ACL or expert ACL, this ACL will not take effect. For example, VLAN 1's IP address is 192.168.64.1 255.255.255.0. Now you create an ACL with the ACE of **deny udp any 192.168.65.1 0.0.0.255 eq 255** and apply this ACL at the egress of VLAN 1. This ACL will not function for the destination IP address is not in the subnet IP range of VLAN 1. If the ACE is **deny udp any 192.168.64.1 0.0.0.255 eq 255**, this ACL will take effect.

Caution

2. For the DES-7200 series, with the input ACL and DOT1X, global IP+MAC binding, port security and IP Source Guard co-used, the Permit and default Deny ACEs are ineffective and other Deny ACEs take effect.

3. For the DES-7200 series, with the input ACL and QOS co-used, the Permit ACEs are ineffective while other Deny ACEs take effect. The default Deny ACE behind the QoS entry takes effect.

4. For the 7200-24, 7200-24G, 7200-48, 7200-48P, 7200-2XG, 7200-4XG and 7200-24P line cards of DES-7200, after applying the ACL to the incoming direction of the multi-SVIs and increasing the ACEs in the ACL, it may fail to configured the ACLs on the SVI due to the insufficient hardware capacity after configuration save and device reload.

5. When configuring the expert ACL and applying it to the outbounding direction of the interface, if some ACEs in the ACL contains the layer-3 matching information(such as IP, L4 port), it leads to the failure of controlling the non-IP packets transmitted on the interface by the ACL permit and deny rules.

6. When applying the ACL, if the ACEs in the ACL(including IP access list and expert extended access list) match with the non-L2 field(such as SIP, DIP), the tagged MPLS packet matching is invalid.

1.2 Configuring IP Access List

To configure access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the protocols that can use numbers to specify access lists and the number ranges of access lists that can be used by each protocol.

Protocol	Number Range
Standard IP	1-99, 1300 - 1999
Extended IP	100-199, 2000 - 2699

1.2.1 Guide to configure IP Access List

When you create an access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

Basic Access Lists include standard access lists and extended access lists. The typical rules defined in access lists are the following:

- Source address
- Destination address
- Upper layer protocol
- Time range

Standard IP access lists (1 – 99, 1300 – 1999) forward or block packets according to source addresses. Extended IP access lists (100 – 199, 2000 – 2699) use the above four combinations to forward or block packets. Other types of access lists forward or block packets according to related codes.

A single access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list. However, the more the used sentences are, the more difficult to read and understand an access list.

1.2.1.1 Implicating “Deny Any Data Flow” Rule Sentence

The ending part of each access list implicates a “Deny any data flow” rule sentence. Therefore, if a packet matches no rule, then it is denied, as shown in the following example:

```
access-list 1 permit host 192.168.4.12
```

This list allows only the message of host 192.168.4.12 and denies any other host. This is because the list contains the following rule statement at the end: **access-list 1 deny any**

Here is another example:

```
access-list 1 deny host 192.168.4.12
```

If the list contains the only statement above, the messages from any host will be denied on the port.

Caution

1. It is required to consider the routing update message when defining the access list. Since the end of the access list “denies all dataflow”, this may cause all routing update messages blocked.

1.2.1.2 Order to Input Rule Sentences

Each added rule is appended to the access list. If a sentence is created, then you cannot delete it separately and can only delete the whole access list. Therefore, the order of access list sentences is very important. When deciding whether to forward or block packets, a switch compares packets and sentences in the order of sentence creation. After finding a matching sentence, it will not check other rule sentences.

If you have created a sentence and it allows all data flows to pass, then the following sentences will not be checked, as shown in the following example:

```
access-list 101 deny ip any any
access-list 101 permit tcp 192.168.12.0 0.0.0.255  eq  telnet any
```

Because the first rule sentence denies all IP messages, the host telnet message of the 192.168.12.0/24 network will be denied. Because the switch discover that the messages match the first rule sentence, it will not check other rule sentences.

1.2.2 Configuring IP Access List

The configuration of the basic access list includes the following steps:

1. Define a basic access list

2. Apply the access list to a specific interface.

There are two methods to configure a basic access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **access-list id** {**deny** | **permit**} {**src** *src-wildcard* | **host src** | **any** | *interface idx*} [**time-range** *tm-rng-name*]	Define an access list
DES-7200(config)# **interface** *interface*	Select the interface to which the access list is to be applied.

Command	Function
DES-7200(config-if)# **ip access-group** id { **in** | **out** } **[unreflect]**	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DES-7200(config)# **ip access-list** { **standard** | **extended** } { *id* | *name* }	Enter the access list configuration mode
DES-7200 (config-xxx-nacl)# [**sn**] { **permit** | **deny** } {**src** *src-wildcard* | **host src** | **any** } [**time-range** *tm-rng-name*]	Add table entries for ACL. For details, please see command reference.
DES-7200(config-xxx-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(config-if)# **ip access-group** *id* { **in** | **out** } **[unreflect]**	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (in the devices that support ACE priority levels).

By default, the reflected ACL is enabled on the IP ACL port. Use the **unreflect** command to disable the reflected ACL.

(The following introduces the operation principle of the reflected ACL:

a. Router auto-generates a temporary access list according to the L3, L4 information of the beginning traffic in the internal network based on the principles of protocol is constant, the source and destination IP addresses, and the source and destination ports are rigidly exchanged.

b. Routers allows the traffic to flow into the internal network only when the L3, L4 information of returned traffic is matched with the one in the temporary access list previously created based on the outputting traffic.)

1.2.3 Showing IP ACL

To monitor access lists, run the following command the in privileged user mode:

Command	Function

Command	Function
DES-7200# **show access-lists** [*id* | *name*]	Show the basic access list.

1.2.4 IP ACL Example

■ **Configuration requirements:**

There are two devices Switch A and Switch B, as shown in Figure 3:

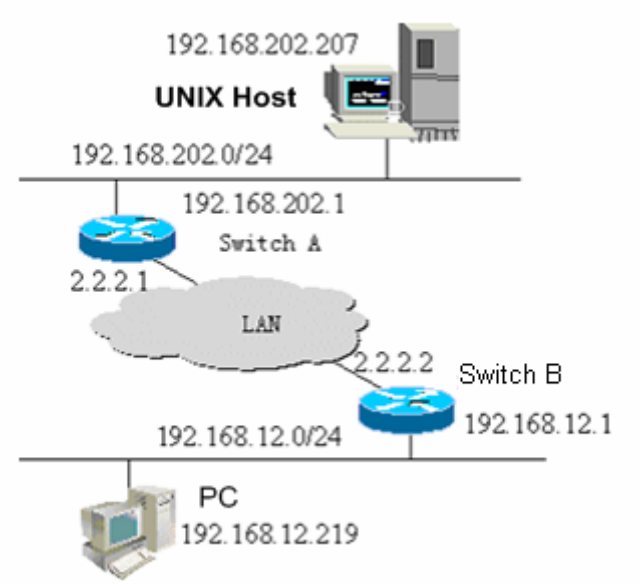


Figure-3 Basic Access List Example

It is required to implement the following security functions by configuring access lists on Switch B.

1. Hosts at the 192.168.12.0/24 network section can only access the remote UNIX host TELNET service during the normal working time period and deny the PING service.
2. On the Switch B console, access to any of the services of hosts at the 192.168.202.0/24 network section is denied.

Note

The above case simplifies the application in the bank system. Namely, it only allows the hosts on the Local Area Network of branches or savings agencies to access the central host and disallows accessing the central host on the device.

■ **Equipment Configuration**

Switch B configuration:

```
DES-7200(config)# interface GigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.12.1 255.255.255.0
DES-7200(config-if)# exit
```

```
DES-7200(config)# interface GigabitEthernet 0/2
DES-7200(config-if)# ip address 2.2.2.2 255.255.255.0
DES-7200(config-if)# ip access-group 101 in
DES-7200(config-if)# ip access-group 101 out
```

According to requirements, configure an extended access list numbered 101

```
access-list 101 permit tcp 192.168.12.0 0.0.0.255 any eq telnet time-range check
DES-7200(config)# access-list 101 deny icmp 192.168.12.0 0.0.0.255 any
DES-7200(config)# access-list 101 deny ip 2.2.2.0 0.0.0.255 any
DES-7200(config)# access-list 101 deny ip any any
```

Configure the time range

```
DES-7200(config)# time-range check
DES-7200(config-time-range)# periodic weekdays 8:30 to 17:30
```

Note

For access list 101. the lat rule sentence ”access-list 101 deny ip any any” is not needed, for the ending part of the access list implicates a “deny any” rule sentence.

For DES-7200, the extended IP ACL does not support the neq matching of TCP/UDP at L4 port.

Switch A configuration:

```
DES-7200(config)# hostname DES-7200
DES-7200(config)# interface GigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.202.1 255.255.255.0
DES-7200(config)# interface GigabitEthernet 0/2
DES-7200(config-if)# ip address 2.2.2.1 255.255.255.0
```

1.3 Configuring Extended MAC Address-based Access Control List

To configure MAC address-based access control lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol. The following table lists the range of the numbers that can be used to specify MAC access lists.

Protocol	Number Range
Extended MAC Access List	700-799

1.3.1 Configuration Guide of Extended MAC Address-based Access Control List

When you create an expert access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in MAC access lists are the following:

- Source MAC address
- Destination MAC address
- Ethernet protocol type
- Time-range

The MAC extended access list (number 700 – 799) forwards or blocks the packets based on the source and destination MAC addresses, and can also match the Ethernet protocol type.

A single MAC access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

1.3.2 Configuring Extended MAC Address-based Access Control List

The configuration of an MAC access list includes the following steps:

1. Define an MAC access list
2. Apply the access list to a specific interface

There are two methods to configure an MAC access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **access-list** id {**deny** | **permit**}{**any** | **host** *src-mac-addr*} {**any** | **host** dst-mac-addr} [*ethernet-type*] [**cos** *cos*]	Define an access list. For details about commands, please see command reference.
DES-7200(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7200(config-if)# **mac access-group** *id* { **in** | **out** }	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DES-7200(config)# **mac access-list extended** {*id* | *name*}	Enter the access list configuration mode
DES-7200 (config-mac-nacl)# [sn] { **permit** | **deny** }{**any** | **host** *src-mac-addr*} {**any** | **host** *dst-mac-addr*} [*ethernet-type*] [**cos** *cos*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7200(config-mac-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(config-if)# **mac access-group** {*id* | *name*} { **in** | **out**}	Apply the access list to the specific interface

Note Method 1 only configures the numerical value ACL. Method 2 can configure names and numerical value ACL and specify the priorities of table entries (they support priority ACE products).

1.3.3 Showing Configuration of MAC Extended Access List

To monitor access lists, please run the following command the in privileged mode:

Command	Function
DES-7200# **show access-lists** [*id* | *name*]	Show the basic access list.

1.3.4 MAC Extended Access List Example

It is required to implement the following security functions by configuring MAC access lists:

1. The 0013.2049.8272 host using the ipx protocol cannot access the giga 0/1 port of a device.
2. It can access other ports.

Configure an Ethernet port, apply the access list 101 on the Ethernet port and check all the messages passing in and out on the port.

```
DES-7200> enable
DES-7200# configure terminal
```

```
DES-7200(config)# mac access-list extended mac-list
DES-7200(config-mac-nacl)# deny host 0013.2049.8272 any ipx
DES-7200(config-mac-nacl)# permit any any
DES-7200(config-mac-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# mac access-group mac-list in
DES-7200(config-if)# end
DES-7200# show access-lists
mac access-list extended mac-list
deny host 0013.2049.8272 any ipx
permit any any
DES-7200#
```

Note

For access lists, ”permit any any” cannot be discarded, for the ending part of an access list implicates a “deny any” rule sentence.

1.4 Configuring Expert Extended Access List

To configure expert extended access lists on a device, you must specify unique names or numbers for the access lists of a protocol to uniquely identifying each access list inside the protocol.The table below lists the number range of the Expert access list.

Protocol	Number Range
Expert extended access list	2700-2899

1.4.1 Configuration Guide of Expert Extended Access List

When you create an expert extended access list, defined rules will be applied to all packet messages on a switch. The switch decides whether to forward or block a packet messages by judging whether the packet matches a rule.

The typical rules defined in expert access lists are the following:

All information in basic access lists and MAC extended access lists

VLAN ID

Expert extended access lists (2700 – 2899) are the syntheses of basic access lists and MAC extended access lists and can filter VLAN IDs.

A single expert access list can use multiple separate access list sentences to define multiple rules. Where, all sentences use a same number or name to bind these sentences to a same access list.

1.4.2 Configuring Extended Expert ACL

The configuration of an expert access list includes the following steps:

1. Define an expert access list
2. Apply the access list to a specific interface (application particular case)

There are two methods to configure an expert access list.

Method 1: Run the following command in the global configuration mode:

Command	Function
DES-7200 (config)# **access-list** *id* {**deny** | **permit**} [*prot* | {[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*] {**src** *src-wildcard* | **host** *src* | **interface** *idx*} {**host** *src-mac-addr* | **any**} {**dst** *dst-wildcard* | **host** *dst* | **any**}{**host** *dst-mac-addr* | **any**}] [**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragment**] [**time-range** *tm-rng-name*]	Define an access list. For details about commands, please see command reference.
DES-7200(config)# **interface** *interface*	Select the interface to which the access list is to be applied.
DES-7200(config-if)# **expert access-group** *id* {**in** | **out** } **[unreflect]**	Apply the access list to the specific interface

Method 2: Run the following command in the ACL configuration mode:

Command	Function
DES-7200(config)# **expert access-list extended** {*id*|*name*}	Enter the access list configuration mode
DES-7200 (config-exp-nacl)# [*sn*]{ **permit** | **deny** }[*prot* | {[*ethernet-type*] [**cos** *cos*]}] [**VID** *vid*] {**src** *src-wildcard* | **host** *src* | **interface** *idx*}{**host** *src-mac-addr* | **any**} {**dst** *dst-wildcard* | **host** *dst* | **any**} {**host** *dst-mac-addr* | **any**}][**precedence** *precedence*] [**tos** *tos*] [**dscp** *dscp*] [**fragment**] [**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7200(config-exp-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(config-if)# **expert access-group** {*id*|*name*} {**in**|**out**} **[unreflect]**	Apply the access list to the specific interface

Note

Method 1 only configures the numerical value ACL. Method 2 can configure names and the numerical value ACL. In a version supporting priority table entries, method 2 can also specify the priorities of table entries (the [*sn*] option in a command).

Note

For DES-7200, the extended Expert ACL does not support the neq matching of TCP/UDP at L4 port.

By default, with the IP extend ACL applied on the interface, the reflect ACL is enabled. You can use the **unreflect** command to disable the reflect ACL.

1.4.3 Showing Configuration of Extended Expert ACL

To monitor access lists, please run the following command the in privileged user mode:

Command	Function
DES-7200# **show access-lists** [*id* | *name*]	Show the expert access list.

1.4.4 Expert Extended Access List Example

It is required to implement the following security functions by configuring expert access lists:

The 0013.2049.8272 host using vlan 20 cannot access the giga 0/1 port of a device.

It cannot access other ports.

```
DES-7200> enable
DES-7200# config terminal
DES-7200(config)# expert access-list extended expert-list
DES-7200(config-exp-nacl)# permit ip vid 20 any host 0013.2049.8272 any any
DES-7200(config-exp-nacl)# deny any any any any
DES-7200(config-exp-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# expert access-group expert-list in
DES-7200(config-if)# end
DES-7200# show access-lists
expert access-list extended expert-list
petmit ip vid 20 any host 0013.2049.8272 any any
deny any any
```

1.5 Configuring IPv6-based Extended Access List

1.5.1 Configuring IPv6 Extended Access List

The configuration of an IPv6-based access list includes the following steps:

1. Define an IPv6 access list
2. Apply the access list to a specific interface (application particular case)

There is the following method to configure a basic access list. Run the following command in the ACL configuration mode:

Command	Function
DES-7200(config)# **ipv6 access-list** *name*	Enter the access list configuration mode
DES-7200 (config-ipv6-nacl)# [sn] **{permit | deny** } prot {*src-ipv6-prefix/prefix-len* | **host** *src-ipv6-addr* | **any**} *{dst-ipv6-pfix/pfix-len* | **any | host** *dst-ipv6-addr*} [**dscp** *dscp*] [**flow-label** *flow-labe*l] [**time-range** *tm-rng-name*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7200(config-exp-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(config-if)# **ipv6 traffic-filter** *name* {**in** | **out**}	Apply the access list to the specific interface

1.5.2 Showing Configuration of IPv6Extended Access List

To monitor access lists, please run the following command the in privileged user mode:

Command	Function
DES-7200# **show access-lists** [*name*]	Show the basic access list.

1.5.3 IPv6 Extended Access List Example

It is required to implement the following security functions by configuring access lists:

The 192.168.4.12 host can access the gi 0/1 port of a device.

It cannot access other ports.

```
DES-7200> enable
DES-7200# config terminal
DES-7200(config)# ipv6 access-list v6-list
DES-7200(config-ipv6-nacl)# permit ipv6 ::192:68:4:12/24 any
DES-7200(config-ipv6-nacl)# deny ipv6 any any
DES-7200(config-ipv6-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ipv6 traffic-filter v6-list in
DES-7200(config-if)# end
DES-7200# show access-lists
ipv6 access-list extended v6-list
permit ipv6 ::192.168.4.12 any
deny any any
DES-7200#
```

Caution

1. For DES-7200 series, IPv6 ACL supports the following matching areas:

Protocol, sip, l4_src,dip, l4_dst, dip, dscp, flow_label.

An IPv6 ACL supports any one of the following three matching areas:

- sip, dip
- protocol, sip, l4_src, l4_dst, dscp, flow_label, range
- protocol, dip, l4_src, l4_dst, dscp, flow_label, range

An ACL cannot match all the above areas. Besides, the IPv6 ACL does not support the fragment matching.

Besides, when an ACL match sip and dip at the same time, it can not support the matching of type code of icmp or source and destination port.

1.6 Configuring ACL80

The ACL80 is also call the custom access list, which means matching the first 80 bytes of the message to filter the messages. A message consists of a series of byte flows. The ACL80 enables the user to perform match filtering by bits in the specified 16 bytes of the first 80 bytes in the message.

Note

The SMAC/DMAC/SIP/DIP/ETYPE of the packets are not contained in any fields. In other words, you can select to match the above fields or other 16 bytes.

For any 16-byte field, it is possible to compare or not the configured value by bits. In other words, it allows setting any bit of those 16 bytes as 0 or 1. There are two factors in filtering any byte: filtering rule and filter domain template. The bits of the both are one-to-one corresponding. The filtering rule specifies the value of the field to be filtered. The filter domain template specifies whether to filter the related fields in the filtering

rule (“1” indicates matching the bit in the corresponding filtering rule, 0 for not). Therefore, when it is time to match a bit, it is required to set 1 for the corresponding bit in the filter domain template. If the filter domain template bit is set as 0, no match will be done no matter what the corresponding bit is in the filtering rule.

For example,

```
DES-7200(config)# expert access-list advanced name
DES-7200(config-exp-dacl)# permit 00d0f8123456 ffffffffffff 0
DES-7200(config-exp-dacl)# deny 00d0f8654321 ffffffffffff 6
```

The user custom access control list matches any byte of the first 80 bytes in the layer-2 data frames according to the user definitions, and then performs corresponding processing for the messages. To use the user custom access control list correctly, it is necessary to have in-depth knowledge about the structure of layer-2 data frame. The following illustrates the first 64 bytes in a layer-2 data frame (each letter indicates a hexadecimal number, and each two letters indicate a byte).

AA AA AA AA AA AA BB BB BB BB BB BB CC CC DD DD

DD DD EE FF GG HH HH HH II II JJ KK LL LL MM MM

NN NN OO PP QQ QQ RR RR RR RR SS SS SS SS TT TT

UU UU VV VV VV VV WW WW WW WW XY ZZ aa aa bb bb

In the figure above, the meaning of each letter and the value of offset are shown below:

Letter	Meaning	Offset	Letter	Meaning	Offset
A	Destination MAC	0	O	TTL field	34
B	Source MAC	6	P	Protocol ID	35
C	VLAN tag field	12	Q	IP checksum	36
D	Data frame length field	14	R	Source IP address	38
E	DSAP field	18	S	Destination IP address	42
F	SSAP field	19	T	TCP source port	46
G	Ctrl field	20	U	TCP destination port	48
H	Org Code field	21	V	Sequential number	50
I	Encapsulated data type	24	W	Confirmation field	54
J	IP version No.	26	XY	IP header length and reservation bits	58
K	TOS field	27	Z	Reservation bit and flags bit	59
L	IP packet length	28	a	Windows size field	60
M	ID	30	b	Others	62
N	Flags field	32			

As shown in the above table, the offset of each field is it offset in the SNAP+tag 802.3 data frame. In the user custom access control list, the user can use two parameters, the rule mask and offset, to abstract any byte from the first 80 bytes of the data frame, and then compare it with the user defined rule to filter the matched data frame for corresponding processing. The user defined rule can be some fixed attributes of the data. For example, the user wants to filter all the TCP messages by defining the rule as “06”, rule mask as “FF” and offset as 35. Here, the rule mask and offset work together to abstract the contents of the TCP protocol ID field in the received data frame, and compare it with the rule to filter all TCP messages.

ACL80 is supported on DES-7200 series.

ACL80 supports matching against Ethernet packets, 803.3 SNAP packets, and 802.311c packets. If the value for matching DSAP to the cnt1 field is set to AAAA03, it indicates to match the 803.3 SNAP packets. If the value is set to E0E003, it indicates to match the 803.311c packets. This field cannot be set to match Ethernet packets.

Note:

1. For DES-7200 series, 3 bytes of AAAA03 must be configured to match the 803.3snap packets(other bytes of AAAA03 shall not be configured). Besides, when using the non-24SFP line card to configure the matched snap packets, if the first byte of the org code filed of the packet is 0, the packet will be dropped. Only if the first byte of the org code is not 0, the packet can be matched. You shall pay special attention to that using this function.

Note

Configuration note:

The ACL180 has only 16 bytes for matching. If the 16 bytes are used, no fields other than the 16 bytes can be matched. For example:

```
DES-7200(config)# expert access-list advanced name
DES-7200(config-exp-dacl)# permit 11223344556677889900aabbccd
deeff ffffffffffffffffffffffffffff 50
```

If you use the following command to add another ACE:

```
DES-7200(config-exp-dacl)#permit 11223344556677889900aabbccd
deeff ffffffffffffffffffffffffffff 54
```

The configuration will fail because the 16 bytes are used by the first ACE. To match the second ACE, you must firstly delete the first ACE.

1.7 Configuring TCP Flag Filtering Control

The TCP Flag filtering feature provides a flexible mechanism. At present, TCP Flag filtering control supports the match-all option. Namely, when the TCP Flags in a received message exactly match those defined in the ACL table entry, the message

will be checked by the ACL rule. A user can define any combination of TCP Flags to filter some messages with specific TCP Flags.

For example,

```
permit tcp any any match-all rst
```

Allow the messages with a TCP Flag RST set and 0 in other positions to pass

Note

When the protocol number of the naming ACL and numerical value configuration is TCP, you can select to configure this filtering feature. MAC extended and IP standard ones do not have this function.

Please configure a TCP Flag by following these steps:

Command	Function
DES-7200(config)# **ip access-list extended** { id | *name* }	Enter the access list configuration mode
DES-7200(config-ext-nacl)# [*sn*] [**permit** | **deny**] **tcp source** *source-wildcard* [**operator port** *[port]*] **destination** *destination-wildcard* [**operator port** *[port]*] [**match-all** *flag-name*][**precedence** *precedence*]	Add table entries for ACL. For details about commands, please see command reference.
DES-7200(config-exp-nacl)# **exit** DES-7200(config)# **interface** *interface*	Exit from the access control list mode and select the interface to which the access list is to be applied.
DES-7200(config-if)# **ip access-group** {*id* | *name*} {**in** | **out**}	Apply the access list to the specific interface

The following example explains how to configure a TCP Flag

Enable permission and password

```
DES-7200> enable
DES-7200#
```

Enter the global configuration mode.

```
DES-7200# configure terminal
```

Enter the ACL configuration mode.

```
DES-7200(config)# ip access-list extended test-tcp-flag
```

Add an ACL entry

```
DES-7200(config-ext-nacl)# permit tcp any any match-all rst
```

Add a deny entry

```
DES-7200(config-ext-nacl)# deny tcp any any match-all fin
```

Adding/delete entries repeatedly.

end

```
DES-7200(config-ext-nacl)# end
```

Show

```
DES-7200# show  access-list test-tcp-flag
ip access-lists extended test-tcp-flag
10 permit tcp any any match-all rst
20 deny tcp any any match-all fin
```

1.8 Configuring ACL Entries by Priority

To embody the ACE priority, there are standards for each ACL to normalize the ACE arranging method under the ACL by using the numbered start point – increment mode, as detailed below:

- ACE is sorted in the ascend order in the chain table by the sequential numbers.
- Starting from the start point number, if no number is specified, it increases by step on the basis of the previous ACE number.
- To specify number, the ACE is inserted in sorting mode, and the increment ensures new ACE can be inserted between two adjacent ACEs.
- The ACL specifies the start point number and the number increment.

The **ip access-list resequence** {*acl-id*| *acl-name*} *sn-start sn-inc* command is available, with details in the related command reference.

Whenever the above command is run, the ACEs will be re-sorted under the ACL list. For example, the ACE numbers under the ACL named tst_acl is as follows:

In the beginning

```
ace1: 10
ace2: 20
ace3: 30
```

The ACE numbers are as follows after "**ip access-list resequence** *tst_acl 100 3*" is run:

```
DES-7200(config)# ip access-list resequence tst_acl 100 3
ace1: 100
ace2: 103
ace3: 106
```

When adding ace4 without entering sn-num, the numbers are as follows:

```
DES-7200(config-std-nacl)# permit …
ace1: 100
ace2: 103
ace3: 106
ace4: 109
```

When adding ace5 by entering seq-num = 105, the numbers are as follows:

```
DES-7200(config-std-nacl)# 105 permit …
ace1: 100
ace2: 103
ace5: 105
ace3: 106
ace4: 109
```

The reference of the numbers is to implement the priority adding ace mode in step 4.

Delete ACE

```
DES-7200(config-std-nacl)# no 106
ace1: 100
ace2: 103
ace5: 105
ace4: 109
The above numbers can also facilitate deleting ACE.
```

1.9 Configuring ACL Based on Time-range

You can run the ACLs based on time, for example, make the ACL take effect during certain periods in a week. For this purpose, you must first set a Time-Range.

Time-Range implementation depends on the system clock. If you want to use this function, you must assure that the system has a reliable clock.

In the privileged configuration mode, you can create a time-range by performing the following steps:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **time-range** *time-range-name*	Identify a time-range by using a meaningful display character string as its name
DES-7200(config-time-range)# **absolute** [**start time** *date*] **end time** *date*	Set the absolute time range (optional). For details, see the configuration guide of time-range.
DES-7200(config-time-range)# **periodic day-of-the-week time to** [*day-of-the-week*] **time**	Set the periodic time range (optional). For details, see the configuration guide of time-range.
DES-7200# **show time-range**	Verify the configurations.
DES-7200# **copy running-config startup-config**	Save the configuration.

Command	Function
DES-7200(config)# **ip access-list extended** *101*	Enter the ACL configuration mode.
DES-7200(config-ext-nacl)# **permit ip any any time-range** *time-range-name*	Configure the ACE of a time-range.

Note

The length of the name should be 1-32 characters, which should not include any space.

You can set one absolute time range at most. The application based on time-ranges will be valid only in this time range.

You can set one or more periodic intervals. If you have already set a running time range for the **time-range**, the application takes effect at periodic intervals in that time range.

The following example shows how to deny HTTP data streams during the working hours in a week by using the ACLs as example:

```
DES-7200(config)# time-range no-http
DES-7200(config-time-range)# periodic weekdays 8:00 to 18:00
DES-7200(config)# end
DES-7200(config)# ip access-list extended limit-udp
DES-7200(config-ext-nacl)# deny tcp any any eq www time-range no-http
DES-7200(config-ext-nacl)# exit
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip access-group no-http in
DES-7200(config)# end
```

Example of displaying time range:

```
DES-7200# show time-range
time-range entry: no-http(inactive)
periodic Weekdays 8:00 to 18:00
time-range entry: no-udp
periodic Tuesday 15:30 to 16:30
```

1.10 Configuring Security Tunnel

Applying a secure ACL globally means that the ACL is a security tunnel. A general ACL is installed on a port or port map; a security tunnel is installed on an interface or globally. The difference between them arises in priority. The security tunnel takes precedence over port security (that is the IP binding under port security), 802.1x and secure ACL. The global security tunnel takes effect for all ports, unless you set a port as an exception port.

Note

1 A security tunnel supports permit and deny rules.

2 The global security tunnel takes no effect for an exception port.

3 The security tunnel policies enabled on an interface take precedence over the global security tunnel.

4 Without IP authorization, using a security tunnel in 802.1x will reduce the permitted authentication number at large extent, which is in accordance with the one under IP authorization.

5 It is strongly recommended to configure a security tunnel before authentication, so as to avoid the case that resource exhaustion causes the authenticated users cannot access the Interface due to the configuration of security tunnel midway.

6 If MAC-IP binding and MAC related binding under port security are enabled on DES-7200 series, the related IP and MAC policies configured on other ports do not function.

You can use an exist ACL to configure a security tunnel

In the privileged configuration mode, execute the following commands to configure a global security tunnel:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **security global access-group** *acl-name*	Configure a global security tunnel.

In the privileged configuration mode, execute the following commands to set an exception port:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config)# **security uplink enable**	Set the interface as an exception port..

If a security tunnel is configured under the interface, remove the security tunnel and then set the interface as the exception port.

In the privileged configuration mode, execute the following commands to configure a security tunnel on the interface:

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **interface** *interface-id*	Enter the interface configuration mode.

Command	Function
DES-7200(config)# **security access-group** *acl-name*	Configure a security tunnel on the interface.

If the interface is set as an exception port, remove the setting and then configure the security tunnel on the interface.

The following example configures a security tunnel.

Set port 4 as security port and bind IP address and MAC address

```
DES-7200(config)#interface FastEthernet 0/4
DES-7200(config-if)#switchport port-security
DES-7200(config-if)#switchport port-security mac-address 0000.0000.0011
ip-address 192.168.6.3
```

Only the packets whose source IP address is 192.168.6.3 and MAC address is 0000.0000.0011 can flow in the switch from port 4. To receive IPX packets, set a security tunnel as follows:

```
DES-7200#configure
DES-7200(config)#expert access-list extended safe_channel
DES-7200(config-exp-nacl)#permit ipx any any
DES-7200(config-exp-nacl)#exit
DES-7200(config)#security global access-group safe_channel
```

Or configure a security tunnel on the interface:

```
DES-7200#configure
DES-7200(config)#expert access-list extended safe_channel
DES-7200(config-exp-nacl)#permit ipx any any
DES-7200(config-exp-nacl)#exit
DES-7200(config)#interface FastEthernet 0/4
DES-7200(config-if)#security access-group safe_channel
```

1.11 Configuring SVI Router ACLs

1.11.1 Understanding SVI Router ACLs

The ACL applied to layer 3 interface is called Router ACLs, which only apply to the routing messages forwarded at layer 3. On layer 3 switches of DES-7200, the ACL applied to SVI also applies to intra-VLAN bridge forwarding messages and inter-VLAN routing messages, resulting in the abnormal communication between users on the VLAN.

To realize the features of Router ACLs on SVI ACL, SVI Router ACLs enabling command is provided on DES-7200 switches. After enabling this command, the ACL applied to SVI will only apply to the layer 3 packets forwarded between VLANs, and will not apply to the bridge forwarded packets within the VLAN.

1.11.2 Default Configuration

By default, SVI Router ACLs is disabled. SVI ACL applies to both inter-VLAN layer 3 packets and intra-VLAN bridge-forwarded packets.

1.11.3 Enabling SVI Router ACLs

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200# **[*no*] svi router-acls enable**	Enable/Disable the SVI Router ACLs.

1.12 Configuration Examples

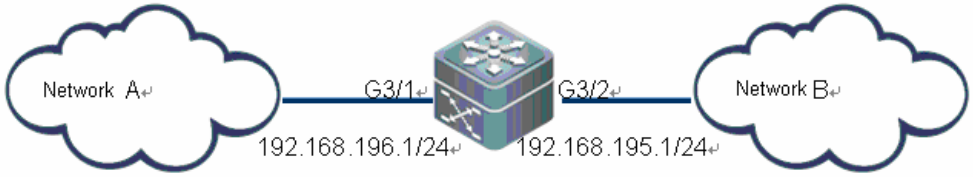
1.12.1 Configuring Unidirectional TCP Connection

Configure TCP Flag filtering to enable unidirectional ACL.

1.12.1.1 Configuration Requirements

For the security of network A, the hosts in network A are allowed to originate the TCP connection request to the hosts in network B. However, the hosts of network B are not allowed to originate the TCP communication requests to network A.

1.12.1.2 Topology View



As shown in the above figure, two networks are connected through a layer 3 switch. Network A connects to the G3/1 port of the switch and network B connects to the G3/2 port of the switch.

1.12.1.3 Analysis

By filtering the packets of TCP connection request originated by network B on the G3/2 port of the switch, you can block the TCP connection request from hosts in network B to network A. Accoding to the analysis of TCP connection, the SYN of the flag field in the TCP header of the initial TCP request packet is reset and the ACK is set to 0. Therefore, to enable network A to access network B in the one-way direction, configure the Match-all option of the extended ACL to set the SYN of the TCP header to 1 and ACK to 0 on the inbounding direction of theG3/2 port.

1.12.1.4 Configuration Steps

1) Define an Access Control List (ACL)

Enter the configuration mode of the switch

```
DES-7200# configure terminal
```

Create the extended ACL101 in the configuration mode

```
DES-7200(config)# ip access-list extended 101
```

Deny the packets whose SYN is 1 and permit other packets whose SYN is 0 (including ACK)

```
DES-7200(config-ext-nacl)# deny tcp any any match-all SYN
```

Permit other IP packets

```
DES-7200(config-ext-nacl)# permit ip any any
```

2) Apply the ACL at the interface

Exit ACL mode

```
DES-7200(config-ext-nacl)# exit
DES-7200(config)# interface vlan 1
DES-7200(config)# ip address 1.1.1.1 255.255.255.0
```

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)#ip access-group ifaddr in
```

Enter the G3/2 port on which the ACL is applied

```
DES-7200(config)# interface gigabitEthernet 3/2
```

Apply ACL 101 to the packet filtering at the inlet of G3/2

```
DES-7200(config-if)# ip access-group 101 in
```

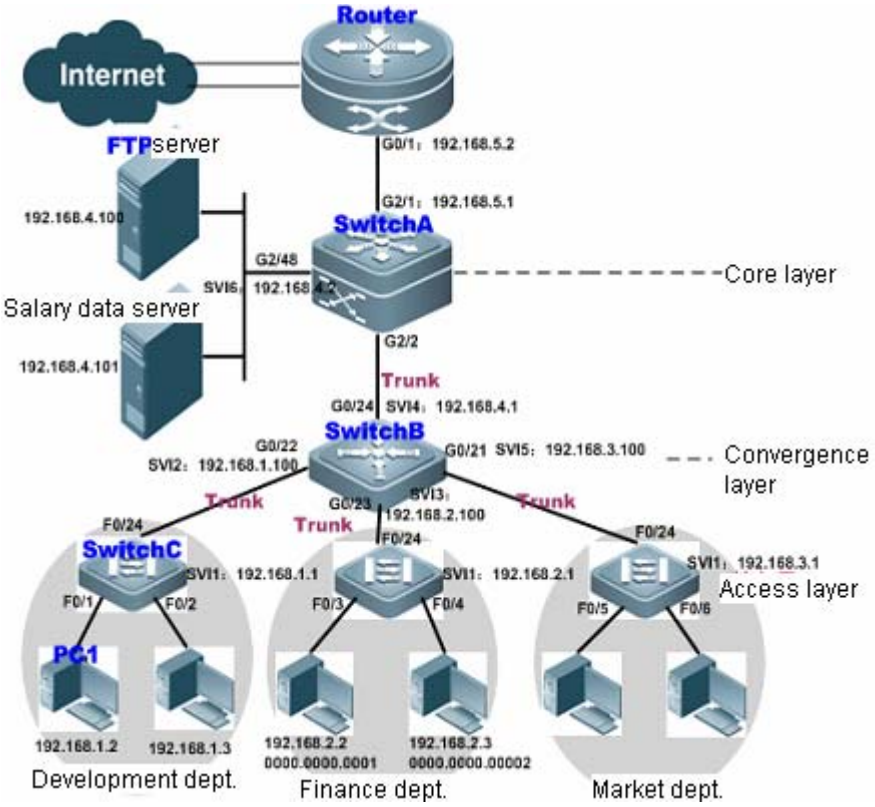
3) Show the configuration of ACL

In the privileged mode, use the **Show** command to display related configuration of ACL

```
DES-7200# show access-lists 101
ip access-list extended 101
 10 deny tcp any any match-all syn
 20 permit ip any any
```

1.12.2 Typical Application of Intranet ACL

1.12.2.1 Networking Diagram



The above diagram shows the typical topology of an Intranet:

The access switch (SwitchC) connecting PCs of respective departments is connected to the convergence switch through 1000M optical fiber cable (trunk mode).

The convergence switch (SwitchB) assigns one VLAN for each department and is connected to the core switch through 10G optical fiber cable (trunk mode).

The core switch (SwitchA) is connected with multiple servers, such as FTP, HTTP server and etc, and is connected to Internet through firewall.

1.12.2.2 Application Requirements

The above scenario of Intranet ACL application mainly involves the following needs:

1. Internet viruses are almost everywhere. Various vulnerable ports must be blocked in order to guarantee Intranet security.
2. Only the internal PCs can access the servers. External PCs are not allowed to access the servers.
3. PCs other than the finance department cannot access PCs of finance department; PCs other than the development department cannot access PCs of development department.
4. QQ, MSN and other IM applications cannot be used by the staff of development department during working hours (namely 9:00-18:00).

1.12.2.3 Configuration Tips

1. The viruses can be avoided by configuring extended ACL on the router-connecting port (G2/1) of core switch (SwitchA) to filter packets destined for relevant ports.
2. As for the requirement that internal PCs can access the servers while external PCs are not allowed to access these servers, we can define the IP extended ACL and apply to ports (G2/2, SVI2) of the core switch (SwitchA) that connect with the convergence switch and server.
3. As for the requirement that specific departments cannot access each other, we can define the IP extended ACL (apply IP extended ACL to G0/22 and G0/23 of Switch B).
4. Configuring time & IP based extended ACL can prevent development departments from suing QQ/MSN and other IM application during a specific period (applying time & IP based extended ACL to SVI2 of SwitchB).

1.12.2.4 Configuration Steps

- Configure the core switch: SwitchA

Step 1: Define the virus-blocking ACL of "Virus_Defence"

☞

Configuration Guide

The worms viruses on the network will create a TFTP server on the local port of "udp/69" in order to transmit the binary virus program to other infected systems. While selecting the destination IP address, the worms will generally select the IP of subnet to which the infected system belongs, and then randomly select the attack target on Internet as per certain algorithm. Once the connection is established, the worms will send attack data to TCP ports (135, 445, 593, 1025, 5554, 9995, 9996), UDP ports (136, 445, 593, 1433, 1434) and UDP/TCP ports (135, 137, 138, 139) of targets. If the attack is successful, TCP/4444 port of target system will be used as the backdoor port. After that, worms will connect to this port and send tftp command in order to transmit virus file to the target system and run the file. The infected server will send substantive invalid data packets to the network, thus wasting network bandwidth and even causing failure of network devices and the network. In such a case, the extended ACL can be used to filter data packets destined for these ports.

```
SwitchA#configure terminal
SwitchA(config)#ip access-list extended Virus_Defence
! Block packets destined for internal and external TCP ports which may have
been used by viruses
SwitchA(config-ext-nacl)#deny tcp any any eq 135
SwitchA(config-ext-nacl)#deny tcp any eq 135 any
SwitchA(config-ext-nacl)#deny tcp any any eq 136
SwitchA(config-ext-nacl)#deny tcp any eq 136 any
SwitchA(config-ext-nacl)#deny tcp any any eq 137
SwitchA(config-ext-nacl)#deny tcp any eq 137 any
……! The configuration is the same for other ports.
SwitchA(config-ext-nacl)#deny tcp any any eq 9996
SwitchA(config-ext-nacl)#deny tcp any eq 9996 any
! Block packets destined for internal and external UDP ports which may have
been used by viruses
SwitchA(config-ext-nacl)#deny udp any any eq 69
SwitchA(config-ext-nacl)#deny udp any eq 69 any
SwitchA(config-ext-nacl)#deny udp any any eq 135
SwitchA(config-ext-nacl)#deny udp any eq 135 any
SwitchA(config-ext-nacl)#deny udp any any eq 137
SwitchA(config-ext-nacl)#deny udp any eq 137 any
……! The configuration is the same for other ports.
SwitchA(config-ext-nacl)#deny udp any any eq 1434
SwitchA(config-ext-nacl)#deny udp any eq 1434 any
! Block ICMP packets
SwitchA(config-ext-nacl)#deny icmp any any
```

```
! Permit all other IP packets
SwitchA(config-ext-nacl)#permit ip any any
SwitchA(config-ext-nacl)#exit
```

Step 2: Apply ACL "Virus_Defence" to the router-connecting interface of core switch

```
SwitchA(config)#interface gigabitEthernet 2/1
SwitchA(config-if)#no switchport
SwitchA(config-if)#ip address 192.168.5.1 255.255.255.0
! Apply ACL "Virus_Defence" to the in direction of G2/1 to block virus packets
from external network
SwitchA(config-if)#ip access-group Virus_Defence in
SwitchA(config-if)#exit
```

Step 3: Define the ACL of "access_server" to only permit Intranet PCs to access the server

```
SwitchA(config)#ip access-list extended access_server
! Only permit Intranet PCs to access the server (IP address being
192.168.4.100).
SwitchA(config-ext-nacl)#permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
SwitchA(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
SwitchA(config-ext-nacl)#permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
SwitchA(config-ext-nacl)#deny ip any any
```

Step 4: Apply ACL "access_server" to the interface connecting with convergence switch and server

```
SwitchA(config)#interface gigabitEthernet 2/2
SwitchA(config-if)#switch mode trunk
! Apply to the in direction on the interface of convergence switch
SwitchA(config-if)#ip access-group access_server in
SwitchA(config-if)#exit
! Create VLAN
SwitchA(config)#vlan 2
SwitchA(config-vlan)#exit
SwitchA(config)#interface gigabitEthernet 2/48
! The server-connecting interface of G2/48 belongs to vlan2
SwitchA(config-if)#switch access vlan 2
SwitchA(config-if)#exit
! Apply to the in direction of server-connecting interface
SwitchA(config)#interface vlan 2
SwitchA(config-if-VLAN 2)# ip access-group access_server in
SwitchA(config-if-VLAN 2)# ip address 192.168.4.2 255.255.255.0
SwitchA(config-ext-nacl)#end
```

- **Configure the convergence switch: SwitchB**

Step 1: Create vlan2-4

```
SwitchB#configure terminal
! Create vlan2-4
SwitchB(config)#vlan range 2-4
SwitchB(config-vlan-range)#exit
```

Step 2: Define ACL

! Define IP extended ACL (vlan_access1 and vlan_access2)

```
SwitchB(config)#ip access-list extended vlan_access1
```

! Prohibit finance department and market department from accessing the development department

```
SwitchB(config-ext-nacl)#deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
SwitchB(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
SwitchB(config-ext-nacl)#permit ip any any
SwitchB(config)#ip access-list extended vlan_access2
```

! Prohibit development department and market department from accessing the finance department

```
SwitchB(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
SwitchB(config-ext-nacl)#deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
SwitchB(config-ext-nacl)#permit ip any any
SwitchB(config-ext-nacl)#exit
```

Step 3: Apply ACLs of "vlan_access1" and "vlan-access2" to the corresponding interfaces

```
! Configure G0/22 as a trunk port and apply vlan_access1
SwitchB(config)#interface GigabitEthernet 0/22
SwitchB(config-if)#switchport mode trunk
SwitchB(config-if)#ip access-group vlan_access1 in
! Configure G0/23 as a trunk port and apply vlan_access2
SwitchB(config)# interface GigabitEthernet 0/23
SwitchB(config-if)# switchport mode trunk
SwitchB(config-if)# ip access-group vlan_access2 in
! Configure G0/24 as a trunk port
SwitchB(config)#interface GigabitEthernet 0/24
SwitchB(config-if)#switchport mode trunk
! Configure IP address of SVI2.
SwitchB(config)#interface vlan 2
SwitchB(config-if)#ip address 192.168.1.100 255.255.255.0
! Configure IP address of SVI3.
SwitchB(config)#interface vlan 3
SwitchB(config-if)#ip address 192.168.2.100 255.255.255.0
! Configure IP address of SVI4.
SwitchB(config)#interface vlan 4
SwitchB(config-if)#ip address 192.168.4.1 255.255.255.0
```

Step 4: Specify time range

```
! Define the time range of 9:00-18:00 from Monday to Friday
SwitchB#configure terminal
SwitchB(config)#time-range worktime
SwitchB(config-time-range)#periodic weekdays 9:00 to 18:00
```

Step 5: Specify the traffic rule of development department

```
SwitchB#configure terminal
```

! Create the extended ACL of "yanfa" in configuration mode

```
SwitchB(config)#ip access-list extended yanfa
```

! Prohibit all hosts of development department from using QQ, MSN and other IM applications during 9:00-18:00 of every working day.

```
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8000 any
time-range worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 8001 any
time-range worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range
worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 1863 any
time-range worktime
SwitchB(config-ext-nacl)#deny tcp 192.168.1.0 0.0.0.255 eq 4000 any
time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 8000 any
time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 1429 any
time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6000 any
time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6001 any
time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6002 any
time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6003 any
time-range worktime
SwitchB(config-ext-nacl)#deny udp 192.168.1.0 0.0.0.255 eq 6004 any
time-range worktime
```

! Permit all other IP traffic

```
SwitchB(config-ext-nacl)#permit ip any any
```

! Apply ACL to the in direction of SVI2

```
SwitchB(config)#interface vlan 2
SwitchB(config-if)#ip access-group yanfa in
```

1.12.2.5 Verifications

Step 1: Verify whether ACE entries are correct. The key is that whether the precedence order of entries is correct and whether entries are effective.

```
SwitchA#show access-lists
ip access-list extended Virus_Defence
 10 deny tcp any any eq 135
 20 deny tcp any eq 135 any
 30 deny tcp any eq 4444 any
 40 deny tcp any any eq 5554
 50 deny tcp any eq 5554 any
 60 deny tcp any any eq 9995
 70 deny tcp any eq 9995 any
 80 deny tcp any any eq 9996
 90 deny tcp any eq 9996 any
 100 deny udp any any eq tftp
```

```
 110 deny udp any eq tftp any
 120 deny udp any any eq 135
 130 deny udp any eq 135 any
 140 deny udp any any eq netbios-ns
 150 deny udp any eq netbios-ns any
 160 deny udp any any eq netbios-dgm
 170 deny udp any eq netbios-dgm any
 180 deny udp any any eq netbios-ss
 190 deny udp any eq netbios-ss any
 200 deny udp any any eq 445
 210 deny udp any eq 445 any
 220 deny udp any any eq 593
 230 deny udp any eq 593 any
 240 deny udp any any eq 1433
 250 deny udp any eq 1433 any
 260 deny udp any any eq 1434
 270 deny udp any eq 1434 any
 280 deny tcp any any eq 136
 290 deny tcp any eq 136 any
 300 deny tcp any any eq 137
 310 deny tcp any eq 137 any
 320 deny tcp any any eq 138
 330 deny tcp any eq 138 any
 340 deny tcp any any eq 139
 350 deny tcp any eq 139 any
 360 deny tcp any any eq 445
 370 deny tcp any eq 445 any
 380 deny tcp any any eq 593
 390 deny tcp any eq 593 any
 400 deny tcp any eq 1025 any
 410 deny tcp any any eq 4444
420 deny icmp any any
 430 permit tcp any any
 440 permit udp any any
 450 permit ip any any

ip access-list extended access_server
 10 permit ip 192.168.2.0 0.0.0.255 host 192.168.4.100
 20 permit ip 192.168.1.0 0.0.0.255 host 192.168.4.100
 30 permit ip 192.168.3.0 0.0.0.255 host 192.168.4.100
 40 deny ip any any
SwitchB#show access-lists
ip access-list extended vlan_access1
 10 deny ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255
 30 permit ip any any

ip access-list extended vlan_access2
 10 deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255
 20 deny ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
 30 permit ip any any

ip access-list extended yanfa
```

```
 10 deny tcp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 20 deny tcp 192.168.1.0 0.0.0.255 eq 8001 any time-range worktime (active)
 30 deny tcp 192.168.1.0 0.0.0.255 eq 443 any time-range worktime (active)
 40 deny tcp 192.168.1.0 0.0.0.255 eq 1863 any time-range worktime (active)
 50 deny tcp 192.168.1.0 0.0.0.255 eq 4000 any time-range worktime (active)
 60 deny udp 192.168.1.0 0.0.0.255 eq 8000 any time-range worktime (active)
 70 deny udp 192.168.1.0 0.0.0.255 eq 1429 any time-range worktime (active)
 80 deny udp 192.168.1.0 0.0.0.255 eq 6000 any time-range worktime (active)
 90 deny udp 192.168.1.0 0.0.0.255 eq 6001 any time-range worktime (active)
 100 deny udp 192.168.1.0 0.0.0.255 eq 6002 any time-range worktime (active)
 110 deny udp 192.168.1.0 0.0.0.255 eq 6003 any time-range worktime (active)
 120 deny udp 192.168.1.0 0.0.0.255 eq 6004 any time-range worktime (active)
```

Step 2: Verify whether ACL configurations are complete. The key is that whether the correct ACL has been applied to the specified interface.

SwitchA:

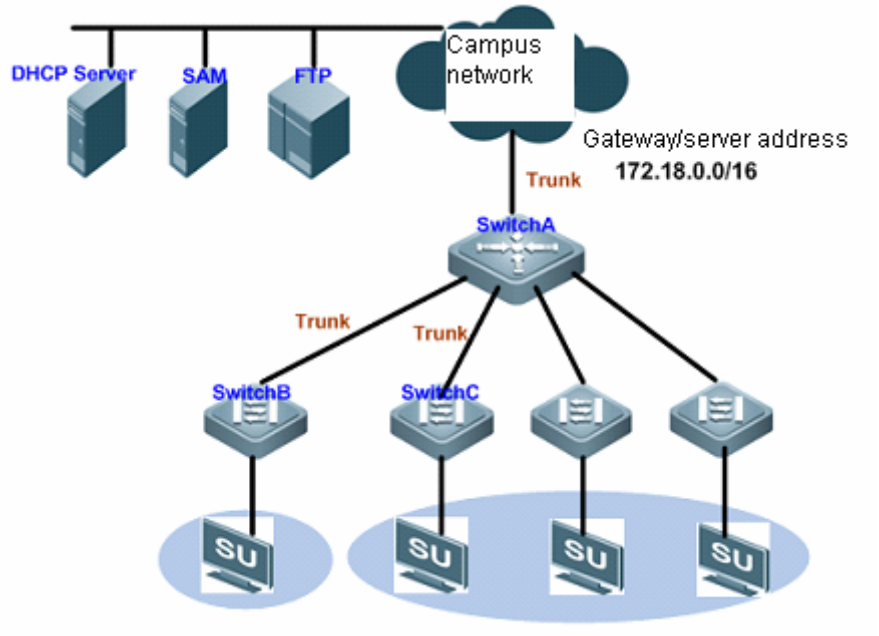
```
SwitchA#show run
interface GigabitEthernet 2/1
 no switchport
 no ip proxy-arp
 ip access-group Virus_Defence in
 ip address 192.168.5.1 255.255.255.0
!
interface GigabitEthernet 2/2
 switchport mode trunk
 ip access-group access_server in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group access_server in
 ip address 192.168.4.2 255.255.255.0
```

SwitchB:

```
SwitchB#show run
!
interface GigabitEthernet 0/22
 switchport mode trunk
 ip access-group vlan_access1 in
!
interface GigabitEthernet 0/23
 switchport mode trunk
 ip access-group vlan_access2 in
!
interface VLAN 2
 no ip proxy-arp
 ip access-group yanfa in
 ip address 192.168.1.100 255.255.255.0
```

1.12.3 Application of expert ACL & ACL80

1.12.3.1 Networking Diagram



The above figure shows the simplified topology of campus network:

SwitchA is the convergence device assigning one VLAN for each faculty and is connected to the campus network through 10G optical fiber cable (trunk mode).

SwitchB and SwitchC are access devices connecting PCs of respective faculties, and are connected to the convergence switch through 1000M optical fiber cable (trunk mode).

SU client must be installed on each PC, which can only access network after passing 802.1x authentication.

1.12.3.2 Application Requirements

SU software is not embedded in Windows. You must download and install SU client on the PC in order to pass authentication. However, the PC cannot download software without 802.1x authentication. To solve this problem, the following requirements must be met:

1. IP packets and ARP packets accessing the segment address of gateway/server (172.18.0.0/16) are allowed to pass through without authentication, so that the user PC can download software from the specified server or access gateway before authentication.

2. DHCP packets (UDP port number being 67/68) are allowed to pass through without authentication, so that the user PC can acquire the IP address in order to proceed with authentication.

1.12.3.3 Configuration Tips

Configure ACL80 or expert ACL on the access device (SwitchB/SwitchC) and combine the feature of secure tunnel to permit certain packets without authentication.

In this case, ACL80 is configured on SwitchB and expert ACL is configured on SwitchC.

1.12.3.4 Configuration Steps

SwitchB

☞ **Configuration Guide**	The customized ACL allows the user to define 64 bytes out of the first 80 bytes of packets to perform per-bit matching and filtering. The user-defined string will be compared with the string extracted from packet (1 means match and 0 means no match), so as to determine further action.

Step 1: Configure the customized ACL

```
SwitchB#configure terminal
```

! Create a customized ACL named "tongdao"

```
SwitchB(config)#expert access-list advanced tongdao
```

! Permit all ARP packets (protocol number being 0800, offset being 24) with source IP (the offset in the source IP of ARP packets is 40) falling within the network segment of 172.18.0.0 (hexadecimal value being ac12)

```
SwitchB(config-exp-dacl)#permit 0806 ffff 24 ac12 ffff 40
```

! Permit all IP packets (protocol number being 0800, offset being 24) with source IP (the offset in the source IP of IP packets is 38) falling within the network segment of 172.18.0.0 (hexadecimal value being ac12)

```
SwitchB(config-exp-dacl)#permit 0800 ffff 24 ac12 ffff 38
```

! Permit DHCP packets with UDP port being 67 (Bootstrap Protocol Server) and 68 (Bootstrap Protocol Client) (offset in protocol number being 35; hexadecimal value of 11 to indicate UDP; offset in port being 46; hexadecimal value of 43/44 corresponding to 67 and 68).

```
SwitchB(config-exp-dacl)# permit 11 ff 35 00440043 ffffffff 46
SwitchB(config-exp-dacl)#exit
```

Step 2: Globally configure the ACL for secure tunnel application

! Configure ACL "tongdao" for secure tunnel application

```
SwitchB(config)# security global access-group tongdao
```

SwitchC

Step 1: Configure expert ACL

```
SwitchC#configure terminal
```

! In configuration mode, create an expert ACL named "tongdao1"

```
SwitchC(config)#expert access-list extended tongdao1
```

! Permit all IP packets with source IP falling within the network segment of 172.18.0.0

```
SwitchC(config-exp-dacl)#permit ip 172.18.0.0 0.0.255.255 any any any
```

! Permit all packets with UDP port number being 67 (Bootstrap Protocol Server) and 68 (Bootstrap Protocol Client)

```
SwitchC(config-exp-dacl)# permit udp any any eq bootpc any any eq bootps
SwitchC(config-exp-dacl)#exit
```

Step 2: Globally configure the ACL for secure tunnel application

! Configure ACL "tongdao1" for secure tunnel application

```
SwitchC(config)# security global access-group tongdao1
```

1.12.3.5 Verifications

Step 1: Verify whether ACE entries are correct. The key is that whether the precedence order of entries is correct and whether entries are effective.

```
SwitchB# show access-lists
expert access-list advanced tongdao
 10 permit 0806 FFFF 24 AC12 FFFF 40
 20 permit 0800 FFFF 24 AC12 FFFF 38
 30 permit 11 FF 35 00440043 FFFFFFFF 46
SwitchC# show access-lists
expert access-list extended tongdao1
 10 permit ip 172.18.0.0 0.0.255.255 any any any
 20 permit udp any any eq bootpc any any eq bootps
```

Execute the above command to verify whether the corresponding ACE entries are correct.

Step 2: Verify whether ACL configurations are complete. The key is that whether the correct ACL has been applied in the global configuration mode:

```
SwitchB#show run
!
expert access-list advanced tongdao
!
security global access-group tongdao
!
!
SwitchC#show run
!
expert access-list advanced tongdao1
!
```

```
security global access-group tongdao1
!
!
```

2 QoS Configuration

2.1 QoS Overview

The fast development of the Internet results in more and more demands for multimedia streams. Generally, people have different service quality requirements for different multimedia, which requires the network to be able to allocate and dispatch resources according to the user demands. As a result, the traditional "best effort" forwarding mechanism cannot meet the user demands. So the QoS emerges.

The QoS (Quality of Service) is used to evaluate the ability for the service provider to meet the customer demands. In the Internet, the QoS mechanism is introduced to improve the network service quality, where the QoS is used to evaluate the ability of the network to deliver packets. The commonly-mentioned QoS is an evaluation on the service ability for the delay, jitter, packet loss and more core demands.

2.1.1 Basic Framework of QoS

The devices that have no QoS function cannot provide the capability of transmission quality service, and will not ensure special forwarding priority for certain dataflow. When bandwidth is abundant, all the traffic can be well processed. But when congestion occurs, all traffic could be discarded. This kind of forwarding policy is otherwise called the service of best effect, since the device now is exerting its performance of data forwarding and the use of its switching bandwidth is maximized.

The device of this module features the QoS function to provide transmission quality service. This makes it possible to select specific network traffic, prioritize it according to its relative importance, and use congestion-management and congestion-avoidance techniques to provide preferential treatment. The network environment with QoS configured is added with predictability of network performance and allocates network bandwidth more effectively to maximize the use of network resources.

The QoS of this device is based on the DiffServ (Differentiated Serve Mode) of the IETF Internet Engineering Task Force. According to the definitions in the DiffServ architecture, every transmission message is classified into a category in the network, and the classification information is included in the IP packet header. The first 6 bits in the ToS (Type of Service) field for IPv4 packet header or the Traffic Class field for Ipv6 packet header carry the classification information of the message. The classification information can also be carried in the Link layer packet header. Below shows the special bits in the packet:

- Carried by the first 3 bits in the Tag Control Information of 802.1Q frame header, which contains the priority information of one of the 8 categories. These three bits are generally called User Priority bits.
- Carried by the first 3 bits of the ToS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called IP precedence value; or carried by the first 6 bits of the ToS field for IPv4 packet header or Traffic Class field for IPv6 packet header, called Differentiated Services Code Point (DSCP) value.

In a DiffServ-compliant network, every device has the same transmission service policy for the messages with the same classification information, and vice versa. The class information in the packet can be assigned by all the systems along the way, such as hosts, devices, or other network devices. It's based on a policy set by a manager, or contents in the packet, or both. The assignment of class information in order to identify packets usually consumes enormous resources of the network device. To reduce the processing overhead on the backbone network, such assignment is often used on the network edge. Based on the class information, the devices can provide different priorities for different traffic, or limit the amount of resources allocated per traffic class, or appropriately discard the packets of less important, or perform other operations as appropriate. This behavior of these independent devices is call per-hop behavior in the DiffServ architecture.

If all devices in the network are providing consistent per-hop behavior, this network forms the end-to-end QoS solution for the DiffServ architecture.

2.1.2 QoS processing flow

2.1.2.1 Classifying

The process of classifying involves putting the messages to the dataflow indicated with CoS value according to the trust policy or the analysis of the message contents. As a result, the core task of classifying is to determine the CoS value of a message. It happens when the port is receiving the inbound messages. When a port is associated with a policy-map that represents a QoS policy, the classification will take effect and be applied on all the messages input through that port.

For general non-IP messages, the switch classifies the messages according to the following criteria:

- If the message itself does not contain any QoS information, which means the layer-2 packet header has no User Priority bits, it gets the QoS information of the message by using the default CoS value of the message input port. Like the User Priority bits of the message, the default CoS value of the port ranges 0~7.
- If the message itself contains QoS information, which means the layer-2 packet header has User Priority bits, it gets the CoS information directly from the message.

Note

The above criteria take effect only when the QoS trust mode of the port is enabled. Enabling the QoS trust mode of a port does not mean getting the QoS information directly from the message or the input port of the message without analyzing the message contents.

- If the policy-map associated with the port is using the ACL classifying based on the MAC access-list extended, the associated ACLs will be matched by getting the source MAC address, destination MAC address and Ethertype domain of the message on that port, to determine the DSCP value of the message. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will assign the priority for the messages of this classification by performing the default behavior: following the priority information contained in the layer-2 packet header of the message or the default priority of the port.

Note

The above three criteria may apply simultaneously on the same port. In this case, they will take effect according to the sequence 3, then 2 and then 1. In other words, the ACLs work first for the classifying operation. When it fails, the criteria 2 will be used, and so on. Here, if the QoS trust mode of the port is enabled, criteria 2 and 1 will be used to get the QoS information directly from the message or the port; otherwise, default DSCP value 0 will be assigned for the messages failing the classifying operation.

For IP messages, the switch classifies the messages according to the following criteria:

- If the port trust mode is Trust ip-precedence, it extracts from the ip precedence field (3 bits) of the IP message and fills the CoS field (3 bits) of the output message.
- If the port trust mode is Trust cos, it extracts directly the CoS field (3 bits) of the message and overwrite the ip precedence field (3 bits) of the message. There are the following two cases. Case 1 is that the layer-2 packet header does not contain User Priority bits, and now the CoS value is got from the default CoS value of the message input port. Case 2 is that the layer-2 packet header contains User Priority bits, and now the CoS is got directly from the packet header.
- If the Policy-map associated with the port is using the ACLs classifying based on the ip access-list (extended), the associated ACLs will be matched by getting the source IP address, destination IP address, Protocol field and layer-4 TCP/UDP port field of the message, to determine the DSCP value of the message, and the CoS value is determined according to the mapping from DSCP to CoS. Note that, if a port is associated with a policy-map but has no DSCP value set for it, the switch will use the above criteria 1 and 2 to determine the priority.

Just like the criteria for non-IP message classifying, the above classifying criteria can apply on the same port at the same time. In this case, they will take effect according to the sequence 3, then 2 and then 1.

For the details of the CoS-to-DSCP map and IP-precedence-to-DSCP map, see the descriptions below.

2.1.2.2 Policing

The Policing action happens after the data classifying is completed. It is used to constrain the transmission bandwidth occupied by the classified dataflow. The Policing action will check every message in the classified dataflow. If the message is occupying more bandwidth as allowed by the police that applies on that dataflow, the message will be treated specially, either to be discarded or assigned with another DSCP value.

In the QoS processing flow, the Policing action is optional. If no Policing action is enabled, the DSCP value of messages in the classified dataflow will remain unchanged, and no message will be discarded before the message is sent for the Marking action.

2.1.2.3 Marking

After the Classifying and Policing actions, the Marking action will write the QoS information for the message to ensure the DSCP value of the classified message can be transferred to the next hop device in the network. Here, the QoS ACLs can be used to change the QoS information of the message, or the QoS information is reserved in the Trust mode. For example, the Trust DSCP can be selected to reserve the DSCP information in the IP packet header.

2.1.2.4 Queuing

The Queuing action is responsible for transferring the messages in the dataflow to an output queue of the port. The messages in different output queues will have transmission service policies of different levels and qualities.

Each port has 8 output queues. The two mapping tables DSCP-to-CoS Map and Cos-to-Queue Map configured on the switch convert the DSCP value of the message into output queue number so as to determine which output queue to transfer the messages into.

2.1.2.5 Scheduling

The Scheduling action is the last cycle in the QoS process. After the messages are transferring into different output queues of the port, the switch works with WRR or another algorithm to transmit the messages in those 8 queues.

It is possible to set the weight in the WRR algorithm to configure the amount of messages to be transmitted in every cycle of message output, thus affecting the transmission bandwidth. Alternatively, it is possible to set the weight in the DRR algorithm to configure the amount of message bytes to be transmitted in every cycle of message output, thus affecting the transmission bandwidth.

2.1.3 QoS Logic Interface Group

A series of interface, which could be APs, or the physical ports, can be specified as one QoS logic interface group, and association the logic interface group with Policy-map for the QoS processing. Take the rate-limit for example, the packets that corresponds to the rate-limit condition share the bandwidth value limited by Policy-map on all ports within the same logic interface group.

Note

The member ports join the logic interface group must be physical ports or Aggregate Port.

For DES-7200 series, the member of the logic interface group must be in the same line card. If there are 48 ports in the line card, all member ports must be distributed in the former 24 ports or the latter 24 ports.

The supported logic interface group number is up to 128.

2.2 QoS Configuration

2.2.1 Default QoS configuration

Make clear the following points of QoS before starting the configuration:

- One interface can be associated with at most one policy-map.
- One policy-map can have multiple class-maps.
- One class-map can be associated at most one ACL, and all ACEs in that ACL must have the same filter domain template.
- The amount of ACEs associated with one interface meets the constraint described in the section "Configuring secure ACL".

By default, the QoS function is disabled. That is, the device treats all messages equally. When you associate a Policy Map with a port and set the trust mode of the port, the QoS function of that port is enabled. To disable the QoS function of a port, you may remove the Policy Map setting and set the trust mode of the port as Off. Below is the default QoS configuration:

Default CoS value	0
Number of Queues	8
Queue Scheduling	WRR

QueueWeight	1:1:1:1:1:1:1:1
WRR Weight Range	1:15
DRR Weight Range	1:15
Trust mode	No Trust
Switch Buffer Management Mode	FC

Default mapping table from CoS value to queue

CoS Value	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Default mapping table from CoS to DSCP

CoS Value	0	1	2	3	4	5	6	7
DSCP value	0	8	16	24	32	40	48	56

Default mapping table from IP-Precedence to DSC

IP-Precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

Default mapping table from DSCP to CoS

DSCP	0	8	16	24	32	40	48	56
CoS	0	1	2	3	4	5	6	7

2.2.2 Configure the QoS trust mode of the interface

By default, the QoS trust mode of an interface is disabled.

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)# **interface interface**	Enter the interface configuration mode.
DES-7200(config-if)#**mls qos trust {cos | ip-precedence | dscp}**	Configure the QoS trust mode of the interface CoS, dscp or ip-precedence

Command	Description
DES-7200(config-if)#**no mls qos trust**	Restore the QoS trust mode of the interface to default

The command below set the trust mode of interface gigabitEthernet 0/4 to DSCP:

```
DES-7200(config)# interface gigabitEthernet 0/4
DES-7200(config-if)# mls qos trust dscp
DES-7200(config-if)# end
DES-7200# show mls qos interface g0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 0
DES-7200#
```

2.2.3 Configuring the Default CoS Value of an Interface

You may configure the default CoS value for every interface through the following steps.

By default, the CoS value of an interface 0.

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)# **interface interface**	Enter the interface configuration mode.
DES-7200(config-if)#**mls qos cos default-cos**	Configure the default CoS value of the interface, where default-cos is the desired default CoS value, ranging 0~7.
DES-7200(config-if)#**no mls qos cos**	Restore to the default CoS value.

The example below set the default CoS value of interface g0/4 to 6:

```
DES-7200# configure terminal
DES-7200(config)# interface g 0/4
DES-7200(config-if)# mls qos cos 6
DES-7200(config-if)# end
DES-7200# show mls qos interface g 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map:
Default COS: trust dscp
Default COS: 6
DES-7200#
```

2.2.4 Configuring the Logic Interface Group

To configure the logic interface group, run the following command in the interface configuration mode:

Command	Description
DES-7200(config-if)#**virtual-group** *virtual-group-number*	Add an interface to the logic interface group. *virtual-group-number:* the goup number of the logic interfaces.

Use the **no virtual-group** *virtual-group-number* command to make a physical port to exit from the logic interface group.

The example below set the interface g0/1 to the member of logic interface group 5:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# virtual-group 5
DES-7200(config-if-range)# end
```

2.2.5 Configuring Class Maps

You may create and configure Class Maps through the following steps:

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)#**ip access-list extended**{*id*|*name*} … DES-7200(config)#**ip access-list standard** {*id*|*name*} … DES-7200(config)#**mac access-list extended** {id|*name*} … DES-7200(config)#**expert access-list extended{***id*|*name*} … DES-7200(config)#**ipv6 access-list extended name** … DES-7200(config)#**access-list id**[…]	Create ACL Please refer to the chapter of ACL

Command	Description
DES-7200(config)# **[no] class-map** *class-map-name*	Create and enter into the class map configuration mode, where class-map-name is the name of the class map to be created. The no option will delete an existing class map
DES-7200(config-cmap)# **[no] match access-group** {*acl-num* | *acl-name }*	Set the matching ACL, where a*cl-name* is the name of the created ACL, acl-num is the ID of the created ACL; the no option delete that match.

For example, the following steps creates a class-map named class1, which is associated with a ACL:acl_1. This class-map will classify all TCP messages with port 80.

```
DES-7200(config)# ip access-list extended acl_1
DES-7200(config-ext-nacl)# permit tcp any any eq 80
DES-7200(config-ext-nacl)# exit
DES-7200(config)# class-map class1
DES-7200(config-cmap)# match access-group acl_1
DES-7200(config-cmap)# end
```

2.2.6 Configuring Policy Maps

You may create and configure Policy Maps through the following steps:

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)# **[no] policy-map** *policy-map-name*	Create and enter into the policy map configuration mode, where policy-map-name is the name of the policy map to be created. The **no** option will delete an existing policy map
DES-7200(config-pmap)# **[no] class** *class-map-name*	Create and enter into the data classifying configuration mode, where class-map-name is the name of the class map to be created. The **no** option deletes that data classification
DES-7200(config-pmap-c)# **[no]set ip dscp** *new-dscp*	Set new ip dscp value for the IP messages in the dataflow; it does not take effect for non-IP messages. *new-dscp* is the new DSCP value to be set, whose range varies with the specific product.
DES-7200(config-pmap-c)#**police** *rate-bps burst-byte* **[exceed-action** {**drop** | **dscp** *dscp-value*}]	Limit the bandwidth of the dataflow and specify the action for the excessive bandwidth part, where *rate-bps* is the limited bandwidth per second (kbps), *burst-byte* is the limited burst bandwidth

Command	Description
	(Kbyte), **drop** means dropping the message of the excessive bandwidth part, **dscp** *dscp-value* means changing the DSCP value of the message in excessive bandwidth part, and *dscp-value* value range varies with specific products. The effective range of the *burst-byte* is 4 to 2097152.
DES-7200(config-pmap-c)# **no police**	Cancel to limit the bandwidth of the dataflow and specify the action for the excessive bandwidth part

Note

1. For DES-7200 series, changing the DSCP value for the excessive bandwidth part will not change the corresponding COS value.

2. The DENY action in the ACL, matched with the CLASS MAP will be ignored.

3. Changing the CoS value will change the corresponding DSCP value at the same time. With the non-tos option enabled, changing the CoS value will not change the corresponding DSCP value.

4. For DES-7200 series and the device with v1.x linecard inserted, up to 128 ACEs in the ACL associated with Class Map share the bandwidth; For the device with v2.x linecard inserted, up to 256 ACEs in the ACL associated with Class Map share the bandwidth.

For example, the following steps create a policy-map named policy1 and associate it with interface Gigabitethernet 1/1.

```
DES-7200(config)# policy-map policy1
DES-7200(config-pmap)# class class1
DES-7200(config-pmap-c)# set ip dscp 48
DES-7200(config-pmap-c)# exit
Router(config-pmap)# exit
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# switchport mode trunk
DES-7200(config-if)# mls qos trust cos
DES-7200(config-if)# service-policy input policy1
```

2.2.7 Applying Policy Maps on the Interface

You may apply the Policy Maps to a port through the following steps:

Command	Description
configure terminal	Enter the configuration mode

Command	Description
Interface *interface*	Enter the interface configuration mode.
[no] service-policy {**input** | **output** *policy-map-name}*	Apply the created policy map to the interface, where the *policy-map-name* is the name of the created policy map, **input** is the input rate limit and **output** is the output rate limit.

Note

DES-7200 series support applying the policy map to the out direction only for 24sfp or 48gt/4sfp_poeII linecard. Because it is necessary to associate the class map with acl, all restrictions of the acl configuration are applicable for the qos configuration. For the details, see the *ACL Configuration*.

For DES-7200 series, with the AP applied to the police, the configured bandwidth limit can be shared by all AP members if the AP member port address the following requirements:

a) if the number of ports of the linecard or device is less than 48 ports, all Aggregate Port members must on the linecard or the device port.

b) If the number of ports of the linecard or device is equal to or more than 48 ports, all Aggregate Port members must on the linecard or the former 24 ports or latter 24 ports on the device.

2.2.8 Applying Policy Maps to the Logic Interface Group

To apply Policy Maps to the logic interface group, run the following commands:

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)#**virtual-group** *virtual-group-number*	**Enter the logic interface group configuration mode.**
DES-7200(config)# [**no**] **service-policy** {**input** | **output**} *policy-map-name*	**Apply the created Policy Maps to the logic interface group.** ***policy-map-name:*** **the name of created policy map;** input***:*** **the input rate-limit;** output***:*** **the output rate-limit.**

Note

This function is not supported. Because it is necessary to associate the class map with acl, all restrictions of the acl configuration are applicable for the qos configuration. For the details, see the *ACL Configuration*.

2.2.9 Configuring the Output Queue Scheduling Algorithm

You may schedule the algorithms for the output queue of a port: WRR, SP, RR and DRR. By default, the output queue algorithm is WRR (Weighted Round-Robin).

You may set the port priority queue scheduling method through the following steps. For details of the algorithm, see the overview of QoS.

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)#**mls qos scheduler** {**sp** | **rr** | **wrr** | **drr**}	Set the port priority queue scheduling method, where **sp** is absolute priority scheduling, **rr** is round-robin, **wrr** is weighted round-robin with frame quantity, and **drr** weighted round-robin with frame length
DES-7200(config)#**no mls qos scheduler**	Restore the default **wrr** scheduling

For example, the following steps set the port output algorithm to SP:

```
DES-7200# configure terminal
DES-7200(config)# mls qos scheduler sp
DES-7200(config)# end
DES-7200# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DES-7200#
```

2.2.10 Configuring Output Round-Robin Weight

You may set the output round-robin weight through the following steps:

Command	Description
DES-7200# **configure terminal**	Enter the configuration mode
DES-7200(config)#{**wrr-queue** | **drr-queue**} **bandwidth** *weight1...weightn*	weight1...weightn are the weight values specified for the output queues. For the count and value range, see the default QoS settings

Command	Description
DES-7200(config)# **no** {**wrr-queue** | **drr-queue**} **bandwidth**	The no option restores the default weight value.

Note

The following table lists the mapping relationship of DES-7200 Series port drr output round-robin weight and bytes:

drr	0	1	2	3	4	5	6	7
bytes	0k	2k	4k	6k	8k	10k	12k	14k

drr	8	9	10	11	12	13	14	15
bytes	16k	18k	20k	22k	24k	26k	28k	30k

The example below sets the wrr scheduling weight as 1:2:3:4:5:6:7:8

```
DES-7200# configure terminal
DES-7200(config)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
DES-7200(config)# end
DES-7200# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
DES-7200(config)#
```

2.2.11 Configuring Cos-Map

You may set cos-map to change which queue to select for the messages in output. The default value of cos-map is provided in the default QoS configuration section.

Command	Description
DES-7200# **configure terminal**	Enter the configuration mode
DES-7200(config)#**priority-queue Cos-Map qid cos0** [**cos1** [**cos2** [**cos3** [**cos4** [**cos5** [**cos6** [**cos7**]]]]]]]	*qid* is the queue id; *cos0..cos7* are the CoS values associated with that queue.
DES-7200(config)#**no priority-queue cos-map**	Restore default of cos-map

Below is the example of configuring CoS Map

```
DES-7200# configure terminal
DES-7200(config)# priority-queue Cos-Map 1 2 4 6 7 5
DES-7200(config)# end
DES-7200# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1

wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

2.2.12 Configuring CoS-to-DSCP Map

CoS-to-DSCP Map is used to map the CoS value to internal DSCP value. You may follow these steps to set CoS-to-DSCP Map. The default value of CoS-to-DSCP is provided in the default QoS configuration section.

Command	Description
DES-7200# **configure terminal**	Enter the configuration mode
DES-7200(config)#**mls qos map cos-dscp** *dscp1...dscp8* DES-7200(config)# **no mls qos map cos-dscp**	Change the CoS-to-DSCP Map settings, where dscp1...dscp8 are the DSCP values corresponding to CoS values 0 ~ 7. The DSCP value range varies with specific products.

For Example:

```
DES-7200# configure terminal
DES-7200(config)# mls qos map cos-dscp 56 48 46 40 34 32 26 24
DES-7200(config)# end
DES-7200# show mls qos maps cos-dscp
cos dscp
--- ----
0   56
1   48
2   46
3   40
4   34
5   32
6   26
7   24
```

2.2.13 Configuring DSCP-to-CoS Map

DSCP-to-CoS is used to map internal DSCP value to CoS value so that it is possible to select output queue for messages.

The default value of DSCP-to-CoS Map is provided in the default QoS configuration section. You may follow these steps to set DSCP-to-CoS Map:

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)# **mls qos map dscp-cos** *dscp-list* **to** *cos*	Set DSCP to COS Map, where dscp-list is the list of DSCP values to be set, DSCP values delimited by spaces, value range varying with specific products, cos means the CoS values corresponding to the DSCP values, ranging 0~7
DES-7200(config)# **no mls qos map dscp-cos**	Restore default

For example, the following steps set the DSCP values 0, 32 and 56 to map 6:

```
DES-7200# configure terminal
DES-7200(config)# mls qos map dscp-cos 0 32 56 to 6
```

```
DES-7200(config)# show mls qos maps dscp-cos
dscp cos    dscp cos   dscp cos   dscp cos
---- ---    ---- ---   ---- ---   ---- ---
 0   6       1   0      2   0      3   0
 4   0       5   0      6   0      7   0
 8   1       9   1     10   1     11   1
12   1      13   1     14   1     15   1
16   2      17   2     18   2     19   2
20   2      21   2     22   2     23   2
24   3      25   3     26   3     27   3
28   3      29   3     30   3     31   3
32   6      33   4     34   4     35   4
36   4      37   4     38   4     39   4
40   5      41   5     42   5     43   5
44   5      45   5     46   5     47   5
48   6      49   6     50   6     51   6
52   6      53   6     54   6     55   6
56   6      57   7     58   7     59   7
60   7      61   7     62   7     63   7
```

2.2.14 Configuring Port Rate Limiting

You may follow these steps to limit the port rate:

Command	Description
DES-7200#**configure terminal**	Enter the configuration mode
DES-7200(config)#**interface** *interface*	Enter the interface configuration mode.
DES-7200(config-if)# **rate-limit output** *bps burst-size*	Port rate limit, where output is the output rate limit, bps is the bandwidth limit per second (kbps), and burst-size is the burst bandwidth limit (Kbyte)
DES-7200(config-if)# **no rate-limit**	Cancel port rate limiting

Note DES-7200 series do not support input rate limit on a port.

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/4
DES-7200(config-if)# rate-limit output 64 1024
DES-7200(config-if)# end
DES-7200#
```

2.2.15 Configuring IPpre to DSCP Map

IPpre-to-Dscp is used to map the IPpre values of message to internal DSCP values. The default settings of IPpre-to-DSCP Map are provided in the default QoS configuration section. you may follow these steps to configure IPpre-to-Dscp Map:

Command	Description
DES-7200# **configure terminal**	Enter the configuration mode
DES-7200(config)# **mls qos map ip-precedence-dscp** *dscp1...dscp8*	Modify the setting of IP-Precedence-to-Dscp Map, where dscp1...dscp8 are the DSCP values corresponding to IP-Precedence values 0~7
DES-7200(config)# **no mls qos map ip-prec-dscp**	Restore default

For Example:

```
DES-7200# configure terminal
DES-7200(config)# mls qos map ip-precedence-dscp 56 48 46 40 34 32 26 24
DES-7200(config)# end
DES-7200# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0     56
1     48
2     46
3     40
4     34
5     32
6     26
7     24
```

2.3 QoS Displaying

2.3.1 Showing class-map

You may show the contents of class-map through the following steps:

Command	Description
show class-map [*class-name*]	Show the contents of the class map entity

For example,

```
DES-7200# show class-map
Class Map cc
```

```
Match access-group 1
DES-7200#
```

2.3.2 Showing policy-map

You may show the contents of policy-map through the following steps:

Command	Description
show policy-map [*policy-name* [**class** *class-name*]]	Show QoS policy map, *policy-name* is the selected name of policy map, specified as **class** Show the class map bound with the policy map in case of *class-name*

For example,

```
DES-7200# show policy-map
Policy Map pp
Class cc
DES-7200#
```

2.3.3 Showing mls qos interface

You may show the QoS information of all ports through the following steps:

Command	Description
show mls qos interface [*interface*| *policers*]	Show the QoS information of the interface, The **Policers** option shows the policy map applied on the interface.

For example,

```
DES-7200# show mls qos interface gigabitEthernet 0/4
Interface GigabitEthernet 0/4
Attached input  policy-map: pp
Default COS: trust dscp
Default COS: 6
DES-7200#show mls qos interface policers
Interface: GigabitEthernet 0/4
Attached input  policy-map: pp
DES-7200#
```

2.3.4 Showing mls qos queueing

You may show the QoS queue information through the following steps:

Command	Description

Command	Description
Show mls qos queueing	Show the QoS queue information, CoS-to-queue map, wrr weight and drr weight;

For example:

```
DES-7200# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   1
3   4
4   1
5   1
6   1
7   1
wrr bandwidth weights:
qid weights
--- -------
0   1
1   2
2   3
3   4
4   5
5   6
6   7
7   8
```

2.3.5 Showing mls qos scheduler

You may show the QoS scheduling method through the following steps:

Command	Description
Show mls qos scheduler	Show the port priority queue scheduling method.

For example:

```
DES-7200# show mls qos scheduler
Global Multi-Layer Switching scheduling
Strict Priority
DES-7200#
```

2.3.6 Showing mls qos maps

You may show the MLS QoS maps table through the following steps:

Command	Description

Command	Description
show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp**]	Show MLS QoS map.

For example:

```
DES-7200# show mls qos maps cos-dscp
cos dscp
--- ----
0   0
1   8
2   16
3   24
4   32
5   40
6   48
7   56
DES-7200# show mls qos maps dscp-cos
dscp cos   dscp cos   dscp cos   dscp cos
---- ---   ---- ---   ---- ---   ---- ---
 0   6      1   0      2   0      3   0
 4   0      5   0      6   0      7   0
 8   1      9   1     10   1     11   1
12   1     13   1     14   1     15   1
16   2     17   2     18   2     19   2
20   2     21   2     22   2     23   2
24   3     25   3     26   3     27   3
28   3     29   3     30   3     31   3
32   6     33   4     34   4     35   4
36   4     37   4     38   4     39   4
40   5     41   5     42   5     43   5
44   5     45   5     46   5     47   5
48   6     49   6     50   6     51   6
52   6     53   6     54   6     55   6
56   6     57   7     58   7     59   7
60   7     61   7     62   7     63   7
DES-7200# show mls qos maps ip-prec-dscp
ip-precedence dscp
------------- ----
0     56
1     48
2     46
3     40
4     34
5     32
6     26
7     24
```

2.3.7 Showing mls qos rate-limit

You may show the port rate limiting information through the following steps:

Command	Description
show mls qos rate-limit [**interface** *interface*]	Show the rate limit of [port]

```
DES-7200# show mls qos rate-limit
Interface GigabitEthernet 0/4
rate limit input bps = 100 burst = 100
```

2.3.8 Showing the virtual-group

You can show the virtual-group configuration by performing following steps

Command	Function
show virtual-group [*virtual-group-number* | **summary**]	Showing the logic interface group information.

```
DES-7200#show virtual-group 1

 virtual-group       member

  -------------       -------------------------

  1                   Gi0/2 Gi0/3 Gi0/4 Gi0/5

                      Gi0/6 Gi0/7 Gi0/8 Gi0/9 Gi0/10

DES-7200#show virtual-group summary

  virtual-group       member

  -------------       -------------------------

  1                   Gi0/1 Gi0/2 Gi0/3 Gi0/4

                      Gi0/5 Gi0/6 Gi0/7 Gi0/8 Gi0/9

  2                   Gi0/11 Gi0/12 Gi0/13 Gi0/14

                      Gi0/15 Gi0/16 Gi0/17 Gi0/18 Gi0/19
```

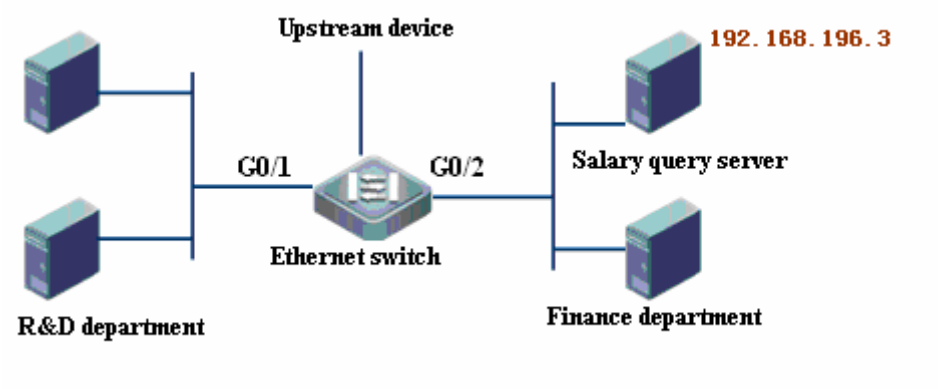
2.4 QoS Configuration Examples

2.4.1 Classified Packets-based Rate Limit

2.4.2 Configuration Requirements

Various departments are interconnected through Ethernet switches in the Intranet, where the finance department is connected through G0/2. For some reason, it is required to limit the maximum outgoing traffic from the salary query server to no more than 512Kbps. The ones exceeding the limit will be dropped.

2.4.3 Topology View



2.4.4 Configuration Procedure

Note

Below shows only the configuration commands associated with QoS ACL.

Enter the global configuration mode.

```
DES-7200# configure
Enter configuration commands, one per line. End with CNTL?Z
```

Define a standard ACL named salary_acl.

```
DES-7200(config)# ip access-list standard salary_acl
```

Define a rule to permit the traffic from the salary server.

```
DES-7200(config-std-nacl)# permit host 192.168.217.223
```

Exit to the global configuration mode.

```
DES-7200(config-std-nacl)# exit
```

Create a class map named salaryclass and enter the class-map configuration mode.

```
DES-7200(config)# class-map salaryclass
```

Define a match rule.

```
DES-7200(config-cmap)# match access-group salary acl
```

Exit to the global configuration mode.

```
DES-7200(config-std-nacl)# exit
```

Create a policy named salarypolicy and enter the policy-map configuration mode.

```
DES-7200(config)# policy-map salarypolicy
```

Set the policy to classify traffic based on salaryclass.

```
DES-7200(config-pmap)# class salaryclass
```

Limit the maximum outgoing traffic from the salary query server to 512Kbps and the burst traffic to 32Kbps, and drop the traffic exceeding this limit.

```
DES-7200(config-pmap-c)# police 512 32 exceed-action drop
```

Exit to the class-map configuration mode.

```
DES-7200(config-pmap-c)# exit
```

Exit to the global configuration mode.

```
DES-7200(config-pmap)# exit
```

Enter the G0/2 interface configuration mode.

```
DES-7200(config)# interface gigabitEthernet 0/2
```

Apply salarypolicy to the inbounding direction of the G0/2 interface.

```
DES-7200(config-if)# service-policy input salarypolicy
```

Exit to the privileged EXEC mode.

```
DES-7200(config-if)# end
```

Show the configuration.

```
DES-7200# show mls qos interface policers

Interface: GigabitEthernet 0/2

Attached input  policy-map: salarypolicy

DES-7200#show policy-map salarypolicy

 Policy Map salarypolicy

    Class salaryclass

      police 512 32 exceed-action drop

DES-7200#show class-map salaryclass

 Class Map salaryclass

   Match access-group salary_acl
```

```
DES-7200#show access-lists salary_acl

ip access-list standard salary_acl

 10 permit host 192.168.217.223
```

3 MPLS QOS Configuration

3.1 Introduction to MPLS QOS

In MPLS network, we can use the EXP bits in MPLS label to configure the priority level of MPLS packets, so as to realize service differentiation (similar to IP differentiation). We can use "class-map" command to divide MPLS packets into one class or multiple classes, and use "policy-map" command to configure the QoS policy for the class. Eventually, we can use service-policy command to apply the QoS policy to the interface.

Note

Since MPLS label switching routers (LSR) won't check the IP header during the forwarding process of label switching, MPLS LSRs use the EXP bits in MPLS label to configure the QoS policy.

3.1.1 MPLS QOS overview

MPLS QoS means to apply QoS over MPLS network. No specific QoS architecture is defined for MPLS QoS. In an actual MPLS network, MPLS QoS generally uses the differentiated services architecture, which is specifically designed for IP QoS. MPLS QoS architecture is the additional support of MPLS to differentiated services on the basis of differentiated services architecture.

Basic principle of differentiated services: At the network edge, the service is mapped to a certain class of service as per the QoS requirement for such service. As for IP packets, we can use 6-bit Differentiated Services Code Point (DSCP) to configure the priority of packets, so as to mark such service exclusively. After that, each node in the backbone network will implement the pre-configured service policy against various services according to this field, so as to ensure the quality of service. Different from the traditional IP QoS, MPLS QoS uses the EXP bits in MPLS labels to configure the priority of MPLS packets, thus achieving differentiated services.

As for IP QoS, we know that QoS comprises of traffic marking, congestion management, congestion avoidance and traffic shaping, and such scheduling

modes as WRR (Weighted Round Robin), DRR and SP can be applied to IP packets in order to achieve weighted random early detection (WRED), traffic monitoring and traffic shaping. We can use the same features according to EXP bits while implementing MPLS QoS.

3.1.2 <MPLS QoS Concept and Terminology>

This section defines MPLS QoS related terms.

3.1.2.1 <EXP>

EXP bits refer to the 20th to 22nd bits in MPLS label. These three labels are called experimental (EXP) bits, and are currently exclusively used for Quality of Service (QoS). The position of EXP field in MPLS label is shown in Fig 2. Like IP packets which can be classified and marked as per IP precedence and DSCP bits, in MPLS network, MPLS packets can also be classified and marked as per the EXP bits.

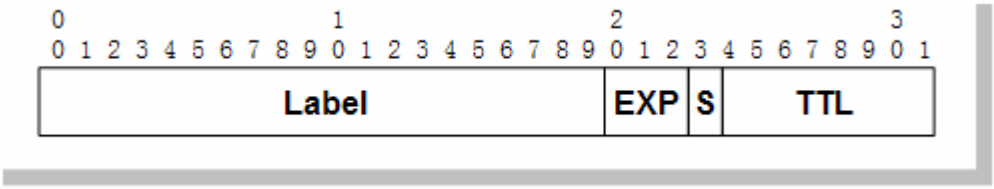


Fig 2 MPLS label architecture

3.1.2.2 <PHB>

Per-hop Behavior (PHB) defines how the router will handle packets while forwarding packets. "Per-hop" means that the behavior as mentioned here involves only the behavior of router-forwarding hop, and the behavior of next-hop router has nothing to do with this router. Generally, forwarding of IP packets based on IP Precedence/DSCP is called IP PHB, and forwarding of MPLS packets based on EXP is called MPLS PHB.

3.1.2.3 <E-LSP>

A LSP with PHB determined by EXP bits. During the forwarding process, LSP determines the forwarding path, but EXP bits determine the scheduling and discarding priority on each hop of LSR. Therefore, a single LSP can support up to eight classes of traffic with different PHBs (the range of 3-bit EXP field is 0-7), which are differentiated as per the EXP bits in MPLS header.

3.1.2.4 <LER>

LER (Label Switching Edge Router) is located at the network edge, and is responsible for imposing MPLS label upon the traffic entering into MPLS network and disposing of MPLS label from traffic which is about to leave the MPLS network. LER is also called Provider Edge (PE) Router.

3.1.2.5 <LSR>

LSR (Label Switching Router) is the core device of MPLS network, allowing label switching and label distribution. LSR is generally called Provider (P) Router.

3.1.3 Working principle

This section will describe how MPLS QoS works. We will take the network topology shown in Fig 3 as the example to describe how to implement MPLS QoS on the network.

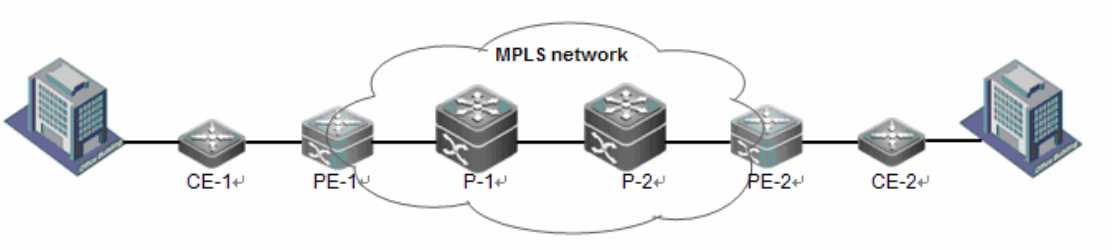


Fig 3 MPLS network topology

Topology description: In this network, CE refers to Customer Equipment. In Fig 3, the leftward part of PE-1 and the rightward part of PE-2 are both IP network. In this section, we assume that packets are transmitted from left to right. We will introduce MPLS QoS behaviors on PE-1, P-1, P-2 and PE-2.

3.1.3.1 PE-1

PE-1 is an ingress LER responsible for imposing the MPLS label upon the IP packets entering into MPLS network. Furthermore, PE-1 also needs to map the QoS information carried in IP packets into MPLS packets (IP packets carry QoS information through IP Precedence or DSCP field in IP header, while MPLS packets carry QoS information through EXP field in MPLS label). On PE-1, we can configure the EXP value in the MPLS label pushed by forming a mapping relation between DSCP and EXP, or use IP packets to classify traffic first and then configure the corresponding EXP value for each class of traffic.

3.1.3.2 P-1

P-1 is a LSR responsible for MPLS label switching. On P-1, we can classify MPLS packets according to MPLS EXP value and configure the corresponding QoS policy. For example, while implementing traffic monitoring of MPLS packets, the MPLS EXP can be remarked in MPLS packets exceeding the configured rate limit. During label switching, to maintain the original QoS information, the EXP value of old label must be copied to the EXP field of new label.

3.1.3.3 P-2

P-2 is also a LSR implementing the same MPLS QoS behaviors as P-1.

3.1.3.4 PE-2

PE-2 is an egress LER responsible for disposing of MPLS label from traffic which is about to leave the MPLS network. Meanwhile, PE-2 also needs to handle the QoS information carried in MPLS packets. It can choose to map the EXP value in MPLS packets to the IP Precedence/DSCP field of IP packets or choose not to handle the original IP packets, namely: no matter how many times the EXP bits are modified, the IP Precedence/DSCP bits in IP packets will be maintained, and the value viewed on PE-2 is the same as the value when IP packets enter into the MPLS network.

3.1.4 DiffServ Tunneling Modes

In the section "Working principle", we learn that the QoS information of IP packets entering into MPLS network can remain unchanged after leaving the MPLS network. In this way, MPLS QoS can be independent of user's IP QoS scheme. While IP packets are crossing various IP tunnels, the interaction between QoS information of original packets and QoS information of tunnel packets is called DiffServ Tunneling mode. MPLS LSP is actually a tunneling mode. The interaction between QoS information of original packets and QoS information of MPLS packets is called MPLS DiffServ Tunneling mode.

Currently, MPLS DiffServ Tunneling Modes can be divided into: Pipe Model, Short Pipe Model and Uniform Model. The difference between them is reflected in LER only. Before understanding details about specific models, we need to understand two concepts: LSP DiffServ information and Tunneling DiffServ information. LSP DiffServ information refers to the QoS information of MPLS packets transmitted from ingress LSR to the egress LSR along LSP (namely EXP bits), while Tunneling DiffServ information refers to the QoS information crossing MPLS network transparently (in case of IP packets entering into MPLS

network, the Tunneling DiffServ information is the IP Precedence or DSCP of IP packets).

3.1.4.1 Pipe Model

In the Pipe Model, the rules to be applied from ingress LSR to egress LSR are shown below:

- LSP DiffServ information can be obtained from the Tunneling DiffServ information on ingress LSR, or be acquired by configuring on the ingress LSR (please refer to behavior of PE-1 as described in working principle).
- On router P, the LSP DiffServ information of egress label is obtained from the LSP DiffServ information of ingress label.
- On the egress LSR, packets are forwarded and handled based on LSP DiffServ information, which won't be propagated to the Tunneling DiffServ information (if IP packets are received on the ingress LSR of MPLS network, then the EXP value won't be propagated to IP Precedence or DSCP).

Note

Currently, Pipe Model is not supported by switches.

3.1.4.2 Short Pipe Model

The only difference between Short Pipe Model and Pipe Model is reflected in the third rule. The third rule of Short Pipe Model is shown below:

- On the egress LSR, packets are forwarded and handled based on Tunneling DiffServ information, and the LSP DiffServ information won't be propagated to the Tunneling DiffServ information.

Note

The device must meet the following conditions in order to support Short Pipe Model.

DES-7200 series products operating in distributed MPLS mode.

3.1.4.3 Uniform Model

Uniform Model means that packets belong to the same QoS class at any time. The rules of Uniform Model are shown below:

- LSP DiffServ information is obtained on the ingress LSR from Tunneling DiffServ information.

- On router P, the LSP DiffServ information of egress label is obtained from the LSP DiffServ information of ingress label.
- On egress LSR, LSP DiffServ information must be propagated to the Tunneling DiffServ information.

Currently, Uniform Model is not supported by switches.

Note

3.1.5 Protocol specification

RFC 2475: The Architecture for Differentiated Services

RFC 3270: Multi-Protocol Label Switching (MPLS) Support of Differentiated Services

3.1.6 Product support

Currently, only DES-7200 series products support MPLS QoS. For DES-7200 series products, there are two MPLS modes: centralized (based on MPLS service card) and distributed. The support to MPLS QoS is different under these two modes.

- Centralized MPLS mode (based on MPLS service card)

Only supports CoS-to-EXP Map, which would be applied to the interface.

- Distributed MPLS mode

All configurations in "Configuration Guide" are supported.

3.1.6.1 <Inner CoS>

Inner CoS represents the inner precedence of packets on DES-7200 series switches. Inner CoS determines the precedence of packets during queuing and scheduling on the router or switch. Inner CoS functions as 802.1P bits and uses the same value range of 0-7.

The DES-7200 series switches, the Inner CoS is mainly related tot he QoS trust mode of interface:

- Interface trust mode is set to untrusted (default configuration)

When the incoming packets are IPv4 packets (no matter whether Tag is carried by packets), the DSCP value of packets will be modified as per the default CoS value (configurable, 0 by default) and CoS-to-DSCP Map of the interface, and the inner CoS is further configured as per DSCP-to-CoS Map. The final queuing of packets will be determined as per the inner CoS.

When the incoming packets are non IPv4 packets, the inner CoS will be configured as per the default CoS value of interface, and the final queuing of packets will be determined as per the inner CoS.

- Interface trust mode is set to trust CoS (configured by executing "mls qos trust cos")

When the incoming packets are IPv4 packets carrying the Tag, the DSCP value of packets will be modified as per the CoS value and CoS-to-DSCP Map of packets, and the inner CoS is further configured and CoS of packets is modified as per DSCP-to-CoS Map. The final queuing of packets will be determined as per the inner CoS.

When the incoming packets are untagged IPv4 packets, the DSCP value of packets will be modified as per the default CoS value and CoS-to-DSCP Map of interface, and the inner CoS is further configured and CoS of packets is modified as per DSCP-to-CoS Map. The final queuing of packets will be determined as per the inner CoS.

When the incoming packets are non IPv4 packets carrying the Tag, the inner CoS will be configured as per the CoS value of packets, and the final queuing of packets will be determined as per the inner CoS.

When the incoming packets are untagged non-IPv4 packets, the inner CoS will be configured as per the default CoS value of interface, and the final queuing of packets will be determined as per the inner CoS.

- Interface trust mode is set to IP Precedence (configured by executing "mls qos trust ip-precedence")

When the incoming packets are IPv4 packets, the DSCP value of packets will be obtained and modified as per the IP Precedence and IP PRE-to-DSCP Map of packets, and the inner CoS is further configured as per DSCP-to-CoS Map. The final queuing of packets will be determined as per the inner CoS.

When the incoming packets are non-IPv4 packets, trust CoS will be handled as per the interface trust mode.

- Interface trust mode is set to trust DSCP (configured by executing "mls qos trust dscp")

When the incoming packets are IPv4 packets, the inner CoS will be configured as per the DSCP value of packets and DSCP-to-CoS Map, and the final queuing of packets will be determined as per the inner CoS.

When the incoming packets are non-IPv4 packets, trust CoS will be handled as per the interface trust mode.

- Interface trust mode is set to trust EXP (configured by executing "mls qos trust experimental")

When the incoming packets are MPLS packets, the inner CoS will be configured as per the EXP value of the topmost label of incoming packets and EXP-to-CoS Map, and the final queuing of packets will be determined as per the inner CoS.

When the incoming packets are non-MPLS packets, trust CoS will be handled as per the interface trust mode.

Note EXP value newly imposed upon the label is mapped from the inner CoS of incoming packets through the Cos-to-EXP Map attached to the egress interface.

3.2 Default Configurations

Before proceeding with MPLS QoS configuration, the following information related to MPLS QoS shall be clarified:

- All configurations of IP QoS apply to MPLS QoS;
- MPLS QoS allows the differentiation of MPLS packets;
- When one or multiple labels are inserted into an IP packet, the default behavior is to map inner CoS to all EXP bits added into the label through the CoS-to-EXP Map attached to the egress port. By default, the first group of CoS-to-EXP Map is attached to all ports receiving and sending MPLS packets.
- Supporting one group of EXP-to-Cos Map and 8 groups of CoS-to-EXP Maps.

By default, MPLS QoS feature is disabled, namely the device will treat all packets equally. The following tables show the default configurations of MPLS QoS:

Function	Default setting
Interface trust mode	Untrusted
MPLS EXP copying	Disabled

Default EXP-to-CoS Map

	EXP value	CoS value
EXP to CoS	0	0
	1	1
	2	2

	3	3
	4	4
	5	5
	6	6
	7	7

Default CoS-to-EXP map

	CoS	EXP
CoS to EXP	0	0
	1	1
	2	2
	3	3
	4	4
	5	5
	6	6
	7	7

Usage guidelines

Caution The contents in 8 groups of default CoS-to-EXP maps are the same.

Note

Currently, MPLS QoS is supported by DES-7200 series products.

MPLS QoS doesn't apply to passthrough packets (such as BPDU passthrough in VPLS).

3.3 Configure MPLS QoS

Configuration commands supported by MPLS QoS include:

- match mpls experimental topmost
- mls qos map exp-cos
- mls qos map cos-exp
- mls qos service cos-exp
- set cos
- police

- mls qos trust
- mpls copy experimental
- mpls propagate-experimental none

Note MPLS QoS supports all IP QoS commands. Some of IP QoS commands are shown above, indicating that it has made some extensions to MPLS QoS.

3.3.1 Configuring Class Maps

The user can execute "match mpls experimental topmost" command to match the EXP field in the topmost label of MPLS packets and classify MPLS packets into multiple service classes by identifying the EXP value. We can configure different QoS service policies for different service classes (such as traffic monitoring).

Class Map configuration steps are shown below:

Command	Function
DES-7200# **configure terminal**	Enter configuration mode.
DES-7200(config)# **class-map** *class-map-name*	Create and enter class map configuration mode. Class-map-name is the name of class map to be created.
DES-7200(config-cmap)# **match mpls experimental topmost** *exp-value1* [*exp-value2* [*exp-valueN*]]	Configure the MPLS EXP value to be matched; exp-valueN is the EXP value to be matched; 8 different values can be matched at one time. This command only applies to MPLS packets.
DES-7200(config-cmap)# **exit**	Exit class-map configuration mode.

To delete an existing class map, execute "**no class-map** *class-map-name*" command.

To remove the specified EXP value from a class map, execute "**no match mpls experimental topmost** *exp-value1* [*exp-value2* [*exp-valueN*]]" command. This command can remove all EXP values or partial EXP values at a time.

The following example matches all MPLS packets with EXP value being 2, and classifies these packets into the class of mpls-exp-2.

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

```
DES-7200(config)# class-map mpls-exp-2

DES-7200(config-cmap)# match mpls experimental topmost 2

DES-7200(config-cmap)# exit
```

Note

Matching the EXP field in the topmost label of MPLS packets is only supported by DES-7200 series products.

3.3.2 Configuring Policy Maps

The user can configure different QoS service policies for different service classes (such as traffic monitoring, EXP remarking, etc).

Policy Map configuration steps are shown below:

Command	Function
DES-7200# **configure terminal**	Enter configuration mode.
DES-7200(config)# **policy-map** *policy-map-name*	Create and enter policy map configuration mode; policy-map-name is the name of policy map to be created.
DES-7200(config-pmap)# **class** *class-map-name*	Create and enter data classification configuration mode; class-map-name is the name of class map created already.
DES-7200(config-pmap-c)# **set** { **ip dscp** *new-dscp* | **cos** *new-cos* [**none-tos**]}	Set new ip dscp value or new cos value for IP packets in the traffic; the new ip dscp configured won't apply to non-IP packets. New-dscp is the new DSCP value configured; the value range differs from product to product. New-cos is the new CoS value to be configured, with range being 0-7. None-tos means to configure new CoS value without modifying the DSCP value of packets.

DES-7200(config-pmap-c)# **police** *rate-bps burst-byte* [**exceed-action** {**drop** | **dscp** *dscp-value* | **cos** *cos-value* [**none-tos**]}]	Limit the bandwidth for the specified traffic and specify the action for handling excess traffic. "Rate-bps" refers to the limited data rate per second (kbps); "burst-byte" refers to the limited burst data rate (kbyte); "**drop**" refers to discard excessive packets; "**dscp** dscp-value" refers to change the DSCP value of excessive packets; "**cos** cos-value" refers to change the CoS value of excessive packets; the range of "cos-value" is 0-7; "**none-tos**" options means to change the CoS value of packets without changing the DSCP value of packets.
DES-7200(config-pmap-c)# **exit**	Exit policy map configuration mode.
DES-7200(config-pmap)# **exit**	Exit data classification configuration mode.

To delete an existing policy map, execute "**no policy-map** *policy-map-name*" command.

To remove data class from a policy map, execute "**no class** *class-map-name*" command in policy map configuration mode.

To remove the CoS configured for traffic, execute "**no set cos**" command in data classification configuration mode.

To remove the bandwidth limit for the specified traffic and the action specified for handling excess traffic, execute "no police" command in data classification configuration mode.

With regard to MPLS QoS, do not configure or modify the DSCP value in the policy. While configuring or modifying the CoS value of packets, "**none-tos**" option shall be used to guarantee the integrity of DSCP value.

Example 1: Match all IP packets received on gigabitethernet 1/1 with DSCP value being 0-7, and classify these packets into the class of class-2; impose EXP value of 2 onto the MPLS label of outgoing packets (by configuring CoS value).

```
DES-7200# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

# Create class map

DES-7200(config)# class-map class-2

DES-7200(config-cmap)# match ip dscp 0 1 2 3 4 5 6 7
```

```
DES-7200(config-cmap)# exit

# Create policy map

DES-7200 (config)# policy-map policy-2

# Configure the inner CoS of packets in class-2 as 2

DES-7200(config-pmap)# class class-2

DES-7200(config-pmap-c)# set cos 2 none-tos

DES-7200(config-pmap-c)# exit

DES-7200(config-pmap)# exit

# Attach policy-2 to interface gigabitethernet 1/1

DES-7200(config)# interface gigabitethernet 1/1

DES-7200(config-if)# service-policy input policy-2

DES-7200(config-if)# exit

DES-7200 (config)#
```

Caution

Configuring or changing the CoS value of packets will change the value of inner CoS of packets.

MPLS EXP field cannot be configured directly. However, you can configure CoS first and then obtain and configure the EXP value through CoS-to-EXP Map in output direction for imposing upon the MPLS label.

Example 2: Match MPLS packets with MPLS EXP being 2 and classify these packets into the class of exp-2. Configure policy to rate limit the incoming packets and mark the CoS value of excessive packets as 0 (assuming that the ingress interface of MPLS packets is gigabitethernet 2/2).

```
DES-7200# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

# Create class map for matching all packets with MPLS EXP being 2

DES-7200(config)# class-map exp-2

DES-7200(config-cmap)# match mpls experimental topmost 2

DES-7200(config-cmap)# exit

# Create policy map

DES-7200(config)# policy-map policy-for-exp2

# Limit the data rate of traffic falling into the class of exp-2 to 1Mbits/s
and limit the burst traffic to 4096kbyte.
```

```
# Change the CoS value of excess packets to 0.
DES-7200(config-pmap)# class exp-2
DES-7200(config-pmap-c)# police 1000000 4096 exceed-action cos 0 none-tos
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
# Attach policy-for-exp2 to interface gigabitehternet 2/2
DES-7200(config)# interface gigabitethernet 2/2
DES-7200(config-if)# service-policy input policy-for-exp2
DES-7200(config-if)# exit
DES-7200(config)#
```

Note

The user can also classify traffic through ACL check of MPLS packets.

3.3.3 Configuring QoS trust mode of interface

By default, the QoS trust mode of interface is untrusted.

Command	Function
DES-7200# **configure terminal**	Enter configuration mode
DES-7200(config)# **interface** *interface*	Enter interface configuration mode
DES-7200(config-if)# **mls qos trust experimental**	Configure the QoS trust mode of interface to trust MPLS EXP.

To restore the interface to default QoS trust mode, execute the "**no mls qos trust**" command.

Example: Configure the trust mode of GigabitEthernet 0/4 to experimental:

```
DES-7200(config)# interface gigabitEthernet 0/4
DES-7200(config-if)# mls qos trust experimental
DES-7200(config-if)# end
DES-7200# show mls qos interface gigabitethernet 0/4
Interface: GigabitEthernet 0/4
Attached input  policy-map:
Attached output policy-map:
```

```
Default trust: experimental
Default COS: 0
Attached mpls cos-exp group: 1
DES-7200#
```

3.3.4 Configuring CoS-to-EXP Map

CoS-to-EXP Map is used to map the inner CoS value to the EXP field imposed upon label. Execute the following steps to configure CoS-to-EXP Map. Please refer to the default MPLS QOS configurations for the default configurations of CoS-to-EXP Map.

Command	Function
DES-7200# **configure terminal**	Enter configuration mode.
DES-7200(config)# **mls qos map cos-exp** *group-number exp1...exp8*	Change the configuration of CoS-to-EXP Map Group-number is the number of CoS-to-EXP Map Group (range: 1-8) Exp1-exp8 are the EXP values (range: 0-7) corresponding to CoS values of 0-7.

To restore to the default value, execute the "**no mls qos map cos-exp** *group-number*" command.

Example: Configure the first group of CoS-to-EXP Map.

```
DES-7200# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# mls qos map cos-exp 1 0 1 1 2 2 5 6 7
DES-7200(config)# end
```

3.3.5 Configuring EXP-to-CoS Map

EXP-to-CoS Map is used to map the EXP value of MPLS packets to the inner CoS. Execute the following steps to configure EXP-to-CoS Map. Please refer to the default MPLS QOS configurations for the default configurations of EXP-to-CoS Map.

Command	Function

DES-7200# **configure terminal**	Enter configuration mode.
DES-7200(config)# **mls qos map exp-cos** *cos1...cos8*	Change the configuration of EXP-to-CoS Map Cos1-cos8 are the CoS values (range: 0-7) corresponding to EXP values of 0-7.

To restore to the default value, execute the "**no mls qos map exp-cos**" command.

Example: Configure EXP-to-CoS Map.

```
DES-7200# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# mls qos map exp-cos 0 0 1 1 4 5 6 7
DES-7200(config)# end
DES-7200# show mls qos maps exp-cos
exp cos
--- ----
0   0
1   0
2   1
3   1
4   4
5   5
6   6
7   7
```

3.3.6 Configuring interface to apply CoS-to-EXP Map

The user can execute the following steps to apply CoS-to-EXP Map Group to the interface. By default, CoS-to-EXP Map Group 1 is applied to each interface.

Command	Function
DES-7200# **configure terminal**	Enter configuration mode.
DES-7200(config)# **interface** *interface*	Enter interface configuration mode
DES-7200(config-if)# **mls qos service cos-exp** *group-number*	Apply CoS-to-EXP Map Group to the interface Group-number is the number of CoS-to-EXP mapping group (range: 1-8)

To restore to the default value, execute the "**no mls qos service cos-exp**" command.

Example: Apply CoS-to-EXP Map Group 2 to interface Gigabitethernet 1/1.

```
DES-7200# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# interface gigabitethernet 1/1
DES-7200(config-if)# mls qos service cos-exp 2
DES-7200(config-if)# end
DES-7200# show mls qos interface gigabitethernet 1/1
Interface: GigabitEthernet 1/1
Attached input  policy-map:
Attached output policy-map:
Default trust: none
Default COS: 0
Attached mpls cos-exp group: 2
DES-7200#
```

Note

When MPLS EXP copying is not enabled, the CoS-to-EXP Map Group attached to the interface applies to SWAP and PUSH labels.

When MPLS EXP copying is enabled, the CoS-to-EXP Map Group attached to the interface only applies to PUSH label.

3.3.7 Configuring MPLS EXP copying

The user can execute the following steps to enable MPLS EXP copying. After enabling MPLS copying, the EXP value in the incoming topmost label will be copied to the outgoing label to be exchanged. When the ingress label is removed, the EXP value in the original incoming topmost label will be copied to the second topmost label.

Command	Function
DES-7200# **configure terminal**	Enter configuration mode.
DES-7200(config)# **mpls copy experimental**	Enable MPLS EXP copying.

To disable MPLS EXP copying, execute the "**no mpls copy experimental**" command.

Example: Enable MPLS EXP copying.

```
DES-7200# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# mpls copy experimental
DES-7200(config)# end
DES-7200# show mls qos mpls
Default mpls copy exp: enable
Default mpls propagate-exp none: disable
DES-7200#
```

Note

The user can enable MPLS EXP copying on P device to ensure that MPLS QoS information is propagated over MPLS network.

MPLS EXP copying only applies to PHP and SWAP behaviors; it doesn't apply to POP or PUSH behavior.

3.3.8 Configuring MPLS EXP not to propagate to inner label

By executing the following steps, when configuring to remove the label, the EXP value in the original incoming topmost label won't be copied to the second topmost label.

Command	Function
DES-7200# **configure terminal**	Enter configuration mode.
DES-7200(config)# **mpls propagate-experimental none**	While disposing of the label, the MPLS EXP in the topmost label won't be propagated to the second topmost label.

To restore the copying of EXP bits in the incoming topmost label to the second topmost label, execute the "**no mpls propagate-experimental none**" command.

Example: While disposing of the label, the MPLS EXP won't be copied to the inner label.

```
DES-7200# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# mpls propagate-experimental none
DES-7200(config)# end
DES-7200# show mls qos mpls
```

```
Default mpls copy exp: enable

Default mpls propagate-exp none: enable

DES-7200#
```

Caution

Before executing "mpls propagate-experimental none" command, MPLS EXP copying must be enabled first.

Note

When moving from one LSP tunnel to another LSP tunnel, to maintain the original LSP DiffServ information, the EXP value of topmost label shall never be copied to the inner label while disposing of the label.

3.4 MPLS QoS showing related commands

Note

MPLS QoS supports all IP QoS showing commands. Some of IP QoS commands are shown above, indicating that it has made some extensions to MPLS QoS.

3.4.1 Showing class-map

Execute the following steps to display the contents of class-map

Command	Function
show class-map [*class-name*]	Display the contents of class map.

Example: Display all class maps

```
DES-7200# show class-map

 Class Map mpls-exp-2
   Match mpls experimental topmost 2
DES-7200#
```

3.4.2 Showing policy-map

Execute the following steps to display the contents of policy-map

Command	Function
show policy-map [*policy-name* [**class** *class-name*]]	Display QoS policy map, *Policy-name* is the name of selected policy map; when "***class*** *class-name*" is specified, the class map bound to the corresponding policy map will be displayed.

Example: Display all policy maps

```
DES-7200# show policy-map

 Policy Map policy-2
    Class class-2
      set cos 2 none-tos
DES-7200#
```

3.4.3 Showing mls qos interface

The user can execute the following steps to display the qos information of all ports

Command	Function
show mls qos interface [*interface*	*policers*]	Display QoS information of interface, and the "policers" option specifies the policy map applied to the interface.

Example:

```
DES-7200# show mls qos interface gigabitethernet 1/1
Interface: GigabitEthernet 1/1
Attached input  policy-map: policy-2
Attached output policy-map:
Default trust: none
Default COS: 0
Attached mpls cos-exp group：2
DES-7200#
DES-7200# show mls qos interface policers
Interface: GigabitEthernet 1/1
Attached input  policy-map: policy-2
Attached output policy-map:
DES-7200#
```

3.4.4 Showing mls qos maps

The user can execute the following steps to display the corresponding mls qos maps

Command	Function
show mls qos maps [**cos-dscp** | **dscp-cos** | **ip-prec-dscp | cos-exp | exp-cos**]	Display the dscp-cos maps, dscp-cos maps, ip-prec-dscp maps, cos-exp maps and exp-cos maps.

Example:

```
DES-7200# show mls qos maps cos-exp
CoS-to-EXP Map group number: 1
cos exp
--- ----
0   0
1   1
2   1
3   2
4   2
5   5
6   6
7   7
CoS-to-EXP Map group number: 2
cos exp
--- ----
0   0
1   1
2   2
3   3
4   4
5   5
6   6
7   7
CoS-to-EXP Map group number: 3
cos exp
--- ----
0   0
1   1
2   2
3   3
4   4
5   5
6   6
```

```
7   7
CoS-to-EXP Map group number：4
cos exp
--- ----
0   0
1   1
2   2
3   3
4   4
5   5
6   6
7   7
CoS-to-EXP Map group number：5
cos exp
--- ----
0   0
1   1
2   2
3   3
4   4
5   5
6   6
7   7
CoS-to-EXP Map group number：6
cos exp
--- ----
0   0
1   1
2   2
3   3
4   4
5   5
6   6
7   7
CoS-to-EXP Map group number：7
cos exp
--- ----
0   0
1   1
2   2
3   3
4   4
5   5
6   6
```

```
7   7
CoS-to-EXP Map group number: 8
cos exp
--- ----
0   0
1   1
2   2
3   3
4   4
5   5
6   6
7   7
DES-7200# show mls qos maps exp-cos
exp cos
--- ----
0   0
1   1
2   1
3   2
4   2
5   5
6   6
7   7
```

3.4.5 showing policy-map interface

Execute the following steps to display policy map configurations of interface.

Command	Function
show policy-map interface *interface*	Display policy map configuration [of the interface].

Example:

```
DES-7200# show policy-map interface gigabitethernet 1/1
GigabitEthernet 0/1  input (tc policy): policy-2
   Class class-2
     set cos 2
     mark count 0

     current token tbf: NULL
     params:  1000000 bps, 4096 limit, 0 extended limit , 0 pir
     conformed 0 packets, 0 bytes; action: drop 0
```

```
exceeded 0 packets, 0 bytes; action: none 0
violated 0 packets, 0 bytes; action: none 0
cbucket 0, cbs 0; ebucket 0 ebs 0
```

Note

Mark count is currently not supported by switches.

3.4.6 Showing MPLS EXP copying state

Execute the following steps to display MPLS EXP copying state

Command	Function
show mls qos mpls	Display information about MPLS EXP copying

Example:

```
DES-7200# show mls qos mpls
 Default mpls copy exp: enable
Default mpls propagate-exp none: disable
DES-7200#
```

3.5 Typical example of configuring MPLS QoS DiffServ tunneling mode

3.5.1 Networking requirements

- PE devices shall allow the mutual mapping between IP QoS information and MPLS QoS information.
- P device shall allow MPLS EXP copying during label switching.
- DES-7200 series devices are used for PE-1, P and PE-2.

3.5.2 Network topology

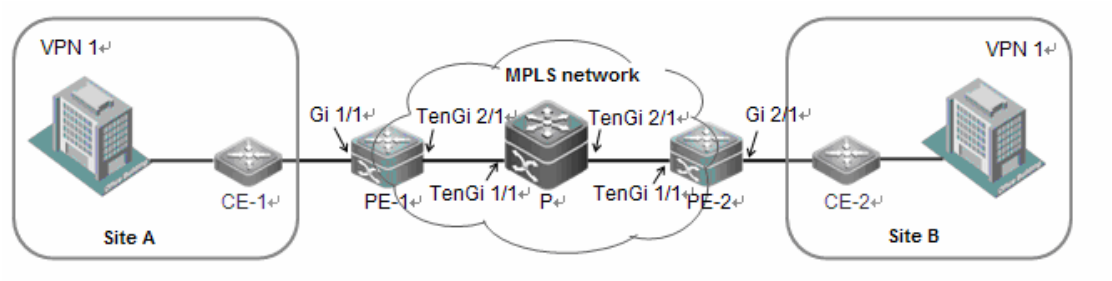


Fig 4 MPLS VPN

- Topology description: In Fig 4, the leftward part of PE-1 and the rightward part of PE-2 are both IP network. Packets are transmitted from site A to site B.
- Description of target: Assuming that the user has divided packets into 4 classes on CE-1: 1) voice packets, with DSCP marked as 48; 2) SAP packets, with DSCP marked as 16; 3) FTP packets, with DSCP marked as 8; 4) other packets, with DSCP marked as 0.

The user intends to reserve 10%, 30%, 20% and 40% bandwidth respectively for the 1st, 2nd, 3rd and 4th class of packets on PE-1. For the 1st class of packets, the user intends to impose EXP value of 6 upon MPLS label, and 3, 1 and 0 respectively for the 2nd, 3rd and 4th class of packets.

On P device, all traffic will be classified according to MPLS EXP value, and the bandwidth as per the ratio of 1:4:3:1:3:1:1:6 will be allocated according to the priority of traffic (from high to low). The service with the lowest priority will be subject to rate limit (not exceeding 1000Mbits/s).

On PE-2, the user expects to rate limit the outgoing traffic. The output data rate of all packets with DSCP value being 0 must not exceed 400Mbits/s.

We will introduce how to configure MPSL QoS on PE-1, P and PE-2 according to user's intents.

3.5.3 Short pipe model

Short pipe model requires configuring QoS policy on PE-2 according to the Tunneling DiffServ information. Here we will introduce how to configure short pipe model.

3.5.3.1 Configuration tips

- PE-2 communicates with CE-2 through Router Port. They cannot communicate through SVI (because on the current switch products, QoS policy cannot be associated to SVI interface).

- On egress interface Gi 2/1 of PE-2, configure QoS policy according to the DSCP value of packets.

3.5.3.2 Configuration Steps

PE-1:

1) Classify packets into 4 classes according to the DSCP value of packets.

Enter global configuration mode

```
DES-7200# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
# Create the class of class-voice to match DSCP value of 48 (all voice packets)
DES-7200(config)# class-map class-voice
DES-7200(config-cmap)# match ip dscp 48
DES-7200(config-cmap)# exit
# Create the class of class-sap to match DSCP value of 16 (all SAP packets)
DES-7200(config)# class-map class-sap
DES-7200(config-cmap)# match ip dscp 16
DES-7200(config-cmap)# exit
# Create the class of class-ftp to match DSCP value of 8 (all FTP packets)
DES-7200(config)# class-map class-ftp
DES-7200(config-cmap)# match ip dscp 8
DES-7200(config-cmap)# exit
# Create the class of class-other to match DSCP value of 0 (all other packets)
DES-7200(config)# class-map class-other
DES-7200(config-cmap)# match ip dscp 0
DES-7200(config-cmap)# exit
```

2) Configure the EXP value in MPLS labels of outgoing packets (by configuring inner CoS)

```
DES-7200(config)# policy-map policy-vpn-1
# Configure the inner CoS of packets belonging to class-voice as 6
# Rate limit class-voice, with CAR being 100Mbits/s and burst being 4096Kbyte;
discard excess packets.
DES-7200(config-pmap)# class class-voice
DES-7200(config-pmap-c)# set cos 6
DES-7200(config-pmap-c)# police 1000000 4096 exceed-action drop
DES-7200(config-pmap-c)# exit
# Configure the inner CoS of packets belonging to class-sap as 3
DES-7200(config-pmap)# class class-sap
DES-7200(config-pmap-c)# set cos 3
```

```
DES-7200(config-pmap-c)# exit
# Configure the inner CoS of packets belonging to class-voice as 1
DES-7200(config-pmap)# class class-ftp
DES-7200(config-pmap-c)# set cos 1
DES-7200(config-pmap-c)# exit
# Configure the inner CoS of packets belonging to class-voice as 0
DES-7200(config-pmap)# class class-other
DES-7200(config-pmap-c)# set cos 0
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
# Attach policy-vpn-1 to interface GigabitEhternet 1/1
DES-7200(config)# interface GigabitEthernet 1/1
DES-7200(config-if)# service-policy input policy-vpn-1
DES-7200(config-if)# exit
```

3) Allocate bandwidth for four service classes

class-voice corresponds to queue 7, with weight being 0 (SP queue)

class-sap corresponds to queue 4, with weight being 3; class-ftp corresponds to queue 2, with weight being 2.

class-other corresponds to queue 1, with weight being 4.

```
DES-7200(config)# wrr-queue bandwidth 4 2 0 3 0 0 0 0
DES-7200(config)# end
```

P device:

1) Implement traffic classification of incoming packets, and classify packets according to MPLS EXP.

Enter global configuration mode

```
DES-7200# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
# Create class
DES-7200(config)# class-map cls-mpls-exp-7
DES-7200(config-cmap)# match mpls experimental topmost 7
DES-7200(config-cmap)# exit
DES-7200(config)# class-map cls-mpls-exp-6
DES-7200(config-cmap)# match mpls experimental topmost 6
DES-7200(config-cmap)# exit
DES-7200(config)# class-map cls-mpls-exp-5
```

```
DES-7200(config-cmap)# match mpls experimental topmost 5
DES-7200(config-cmap)# exit
DES-7200(config)# class-map cls-mpls-exp-4
DES-7200(config-cmap)# match mpls experimental topmost 4
DES-7200(config-cmap)# exit
DES-7200(config)# class-map cls-mpls-exp-3
DES-7200(config-cmap)# match mpls experimental topmost 3
DES-7200(config-cmap)# exit
DES-7200(config)# class-map cls-mpls-exp-2
DES-7200(config-cmap)# match mpls experimental topmost 2
DES-7200(config-cmap)# exit
DES-7200(config)# class-map cls-mpls-exp-1
DES-7200(config-cmap)# match mpls experimental topmost 1
DES-7200(config-cmap)# exit
DES-7200(config)# class-map cls-mpls-exp-0
DES-7200(config-cmap)# match mpls experimental topmost 0
DES-7200(config-cmap)# exit
```

2) Configure the input service policy, and rate limit the service class of cls-mpls-exp 0

```
DES-7200(config)# policy-map policy-exp-0-rate-limit
# Rate limit cls-mpls-exp 0, with CAR being 1000Mbits/s and burst being 4096Kbyte
# Discard excess packets
DES-7200(config-pmap)# class cls-mpls-exp-0
DES-7200(config-pmap-c)# police 10000000 4096 exceed-action drop
DES-7200(config-pmap-c)# exit
DES-7200(config-pmap)# exit
# Attach policy-exp-0-rate-limit to interface TenGigabitEthernet 1/1
DES-7200(config)# interface TenGigabitEthernet 1/1
DES-7200(config-if)# service-policy input policy-exp-0-rate-limit
```

3) Configure QoS trust mode of ingress interface TenGigabitEthernet as trust MPLS EXP

```
DES-7200(config-if)# mls qos trust experimental
DES-7200(config-if)# exit
```

4) Allocate bandwidth for MPLS EXP service classes

Allocate the bandwidth according to the ratio of 6:1:1:3:1:3:4:1 for MPLS EXP0-MPLS EXP7

```
DES-7200(config)# wrr-queue bandwidth 6 1 1 3 1 3 4 1
```

5) Enable MPLS EXP copying

```
DES-7200(config)# mpls copy experimental
DES-7200(config)# end
```

PE-2:

1) On the ingress port, enable QoS trust mode and configure to trust MPLS EXP.

Enter global configuration mode

```
DES-7200# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
DES-7200(config)# interface TenGigabitEthernet 1/1
# Configure the interface trust mode as trust MPLS QoS
DES-7200(config-if)# mls qos trust experimental
DES-7200(config-if)# exit
```

2) Configure the output service policy, and rate limit the service class of class-dscp-0

```
# Create the class of class-dscp-0 to match DSCP value of 0
DES-7200(config)# class-map class-dscp-0
DES-7200(config-cmap)# match ip dscp 0
DES-7200(config-cmap)# exit
```

3) Configure the output service policy and rate limit the service class of cls-dscp-0 (not exceeding 400Mbits/s

```
DES-7200(config)# policy-map policy-vpn-1
DES-7200(config-pmap)# class class-dscp-0
DES-7200(config-pmap-c)# police 400000 4096 exceed-action drop
DES-7200(config-pmap-c)# exit
```

3) Attach policy-vpn-1 to egress interface GigabitEhternet 2/1

```
DES-7200(config)# interface GigabitEthernet 2/1
DES-7200(config-if)# service-policy output policy-vpn-1
DES-7200(config-if)# end
```

3.5.3.3 Verification

PE-1:

```
DES-7200# show class-map

 Class Map class-voice
   Match ip dscp 48
 Class Map class-sap
```

```
  Match ip dscp 16
 Class Map class-ftp
  Match ip dscp 8
 Class Map class-other
  Match ip dscp 0
 DES-7200# show policy-map

Policy Map policy-vpn-1
    Class class-voice
      set cos 6
      police 1000000 4096 exceed-action drop
    Class class-sap
      set cos 3
    Class class-ftp
      set cos 1
    Class class-other
      set cos 0
DES-7200# show mls qos interface GigabitEthernet 1/1
Interface: GigabitEthernet 1/1
Attached input  policy-map: policy-vpn-1
Attached output policy-map:
Default trust: none
Default cos: 0
Attached mpls cos-exp group: 1
DES-7200# show mls qos queueing
Cos-queue map:
cos qid
--- ---
0   1
1   2
2   3
3   4
4   5
5   6
6   7
```

```
7   8


wrr bandwidth weights:

qid weights

--- -------

1   4

2   2

3   0

4   3

5   0

6   0

7   0

8   0

DES-7200#
```

P device:

```
DES-7200# show class-map


 Class Map cls-mpls-exp-7
   Match mpls experimental topmost 7
Class Map cls-mpls-exp-6
   Match mpls experimental topmost 6
Class Map cls-mpls-exp-5
   Match mpls experimental topmost 5
Class Map cls-mpls-exp-4
   Match mpls experimental topmost 4
Class Map cls-mpls-exp-3
   Match mpls experimental topmost 3
Class Map cls-mpls-exp-2
   Match mpls experimental topmost 2
Class Map cls-mpls-exp-1
   Match mpls experimental topmost 1
Class Map cls-mpls-exp-0
   Match mpls experimental topmost 0
DES-7200# show policy-map


Policy Map policy-exp-0-rate-limit

     Class cls-mpls-exp-0

       police 10000000 4096 exceed-action drop
```

```
DES-7200# show mls qos interface TenGigabitEthernet 1/1

Interface: TenGigabitEthernet 1/1

Attached input  policy-map: policy-exp-0-rate-limit

Attached output policy-map:

Default trust: experimental

Default cos: 0

Attached mpls cos-exp group: 1

DES-7200# show mls qos queueing

Cos-queue map:

cos qid

--- ---

0   1

1   2

2   3

3   4

4   5

5   6

6   7

7   8


wrr bandwidth weights:

qid weights

--- -------

1   6

2   1

3   1

4   3

5   1

6   3

7   4

8   1

DES-7200# show mls qos mpls

Default mpls copy exp: enable

Default mpls propagate-exp none: disable
```

```
DES-7200#
```

PE-2:

```
DES-7200# show class-map

Class Map class-dscp-0
Match ip dscp 0
DES-7200# show policy-map

  Policy Map policy-vpn-1
      Class class-dscp-0
        police 400000 4096 exceed-action drop
  DES-7200# show mls qos interface TenGigabitEthernet 1/1
  Interface: TenGigabitEthernet 1/1
  Attached input  policy-map:
  Attached output policy-map:
  Default trust: experimental
  Default cos: 0
  Attached mpls cos-exp group：1
  DES-7200# show mls qos interface GigabitEthernet 2/1
  Interface: GigabitEthernet 2/1
  Attached input  policy-map:
  Attached output policy-map: policy-vpn-1
  Default trust: none
  Default cos: 0
  Attached mpls cos-exp group：1
  DES-7200# show mls qos mpls
  Default mpls copy exp：enable
  Default mpls propagate-exp none：disable
  DES-7200#
```

4 WRED Configuration

4.1 Understanding WRED

The working process of the window mechanism for TCP(Transmission Control Protocol) is described as follows: the sender sends a message segment in the size of one window; if it is successful for the sender to receive the response from the receiver, the sender will send the message segments in the size of 2 windows; if it succeeds, the sender will send the message segments in the size of 4 windows; the window size increases exponentially. Howerver, if the message segment loses, TCP flow will start slowly, and the window size is reduced to 1. The TCP flow window size grows in an exponential manner till it reaches half of the congestion size. Then the TCP flow window size grows linearly. TCP slow start is relevant to QoS, for the reason that when the export queue on an interface is full, all packets newly-arrived are dropped, which is “tail dropped”. All TCP flows are in the TCP slow start simultaneously.

Global synchronization refers to multiple TCP flows are in the state of TCP slow start at the same time. When the TCP synchronization occurs, the connection bandwidth can not be fully utilized, resulting in a waste of bandwidth.

To avoid that, Weighted Random Early Detection (WRED), the packet dropping policy, could be adopted. WRED provides a mechanism for randomly dropping packets, greatly reducing the synchronization of the speed of sending multiple TCP connections and preventing the TCP global synchronization. When the packets of one TCP connection are dropped, other TCP connections still send the packets at a high speed. In this way, the TCP connections always send the packets rapidly, improving the utilization of the line bandwidth.

The user can set the minimum and maximum threshold for the queue with WRED configured. When the queue length is less than the minimum threshold, the packets are not dropped; when the queue length is between the minimum and maximum thresholds, WRED starts to drop ttge packets randomly(the longer the queue length is, the higher the probability of the packet drop is); when the queue length is more than the maximum threshold, all packets are dropped.

The difference of RED and WRED lies in that WRED introduces the IP precedence to differentiate the drop policy. RED is a special condition of WRED. When all CoS-to-Min_threshold and CoS-to-Max_threshold are the same on the interface, the enabled WRED becomes the RED.

4.2 WRED Configuration

This section includes:

- Default WRED configuration
- Restriction of WRED configuration
- WRED configuration guide
- WRED configuration display

4.2.1 Default WRED Configuration

The default WRED configurations are as follows:

Feature		Default Value	
Queue1	Threshold1	CoS	0，1，2，3，4，5，6，7
		WRED-drop	100% low，100%high
		random-detect probability	60%
	Threshold2	CoS	NONE
		WRED-drop	80% low，100%high
		random-detect probability	80%
	Threshold3	CoS	Not supported by DES-7200 series.
		WRED-drop	Not supported by DES-7200 series.
		random-detect probability	Not supported by DES-7200 series.
Queue2	Threshold1	CoS	Not supported by DES-7200 series.
		WRED-drop	Not supported by DES-7200 series.
		random-detect probability	Not supported by DES-7200 series.
	Threshold2	CoS	Not supported by DES-7200 series.

		WRED-drop	Not supported by DES-7200 series.
		random-detect probability	Not supported by DES-7200 series.
	Threshold3	CoS	Not supported by DES-7200 series.
		WRED-drop	Not supported by DES-7200 series.
		random-detect probability	Not supported by DES-7200 series.

Note

By default, all queues map to the the first group of threshold of queue1; and the minimum threshold equals to the maximum threshold, both are 100%, representing to disable the WRED function.

4.2.2 Restriction of WRED Configuration

The restrictions of WRED configuration are as follows:

- WRED can only be configured on the physical port, including the AP member port, and can not be configured on the AP and SVI interface.
- DES-7200 series do not support the max_threshold configuration.
- The threshold number may be different for different products.
- The max_threshold must be more than the min_threshold in the same group.
- To disable the WRED function, the user can configure the min_threshold as 100%.
- For DES-7200 series, WRED configurations are supported on the following line cards (7200-48E, 7200-24GE, 7200-24G2XGE.)

4.2.3 WRED Configuration Guide

The following 3 parameters shall be configured:

1. min_threshold, which must be less than the max_threshold in the same group;

2. random-detect probability;

3. Threshold-Cos.

4.2.3.2 Configuring Min-threshold

To configure the min_threshold value, run the following commands in the interface configuration mode:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** <*interface*>	Enter the interface configuration mode.
DES-7200(config-if)# **wrr-queue random-detect min-threshold** *queue_id thr1 [thr2 thr3]*	Configure the minimum threshold value.
DES-7200(config-if)# **show queueing wred interface** <*interface*>	Show the WRED minimum threshold configuration.

The following example shows how to set the minimum threshold of queue 1 on an interface:

```
DES-7200(config-if)#wrr-queue random-detect min-threshold 1 68 69
```

Caution When both the min_threshold and the max_threshold are 100%, the WRED is disabled.

4.2.3.3 Configuring Random-detect Probability

To configure the random-detect probability, run the following commands in the interface configuration mode:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** <*interface*>	Enter the interface configuration mode.
DES-7200(config-if)# **wrr-queue random-detect probability** *queue_id prob1 [prob2 prob3]*	Configure the random-detect probability.

Command	Function
DES-7200(config-if)# **show queueing wred interface** <*interface*>	Show the WRED random-detect probability configuration.

The following example shows how to set the random-detect probability of queue 1 on an interface:

```
DES-7200(config-if)#wrr-queue random-detect probability 1 61 62 63
```

4.2.3.4 Configuring Threshold-CoS

To configure the threshold-cos, run the following commands in the interface configuration mode:

Command	Function
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** <*interface*>	Enter the interface configuration mode.
DES-7200(config-if)# **wrr-queue cos-map** *threshold_id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]	Configure the threshold-cos.
DES-7200(config-if)# **show queueing wred interface** <*interface*>	Show the WRED random-detect probability configuration.

The following example shows how to map the threshold2 to CoS1 and CoS6:

```
DES-7200(config-if)#wrr-queue cos-map 2 1 6
```

Note

The administrator can set the DSCP-threshold by mapping DSCP-CoS to CoS-Threshold.

The administrator can set the Queue-threshold by mapping CoS-Threshold to CoS-Queue.

4.2.4 Showing WRED Configuration

To show the WRED configuration, run the following commands in the Privileged mode:

Command	Function
DES-7200(config-if)# **show queueing wred interface** <*interface*>	Show the WRED configuration.

The following example shows the WRED configuration:

```
DES-7200#configure
DES-7200#show queueing wred interface gigabitethernet 0/1
---   -----  -----   ------    -----   -----    ------    -----   -----
------
qid  max_1 min_1 prob_1   max_2  min_2   prob_2   max_3 min_3 prob_3
---   -----  -----   ------     -----   -----   ------   -----  -----
------
1   0    0    90       0     0     91      0    0    92
2   88   66   90       87    55    91      86   66   92
3   0    0    0        0     0     0       0    0    0
4   0    0    0        0     0     0       0    0    0
5   88   66   0        89    67    0       90   68   0
6   0    0    0        0     0     0       0    0    0
7   0    0    0        0     0     0       0    0    0
8   0    0    0        0     0     0       0    0    0
cos  qid  threshold_id
---   ---   ------------
0   1   1
1   2   1
2   3   1
3   4   2
4   5   1
5   6   3
6   7   2
7   8   1
```

DES-7200

Reliability Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 VRRP Configuration

1.1 Overview

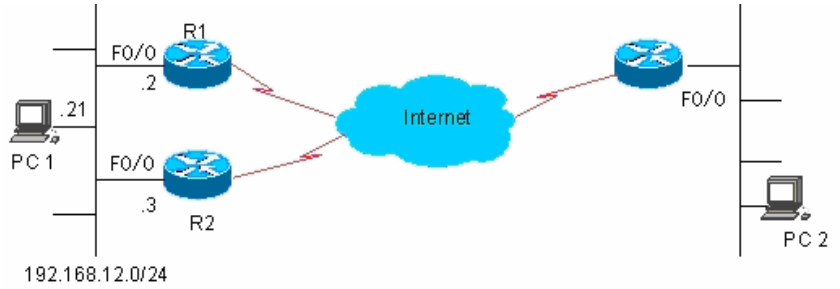
The Virtual Router Redundancy Protocol (VRRP) is designed to work in the active/standby mode to ensure that the standby router can take over the work without affecting internal and external data communication and modifying the parameters of internal networks when the master router fails. Multiple devices within a VRRP group are mapped to a virtual device. The VRRP ensures one and only one device to send packets on behalf of the virtual device at one time, while the host sends messages to that virtual device. The device that forwards packets is elected as the master device. If that device cannot work due to some reason, the one in standby status will be selected to replace it and become the active device. With VRRP, the hosts in the LAN seem to use only one router. The route connectivity is also guaranteed even when the currently-used first-hop router fails.

RFC 2338 defines the IP packet format in VRRP type and its working mechanism. The VRRP message means a kind of multicast message with specified destination address, which is sent by the master router by schedule to indicate its operation and are also used to elect the master router. The VRRP allows another router to automatically take over the operations when the router that undertaking route forwarding function in the IP LAN fails, thus implementing the hot-backup and error-tolerance of IP routing and ensuring the continuity and reliability of host communication in the LAN. Redundancy is implemented for a VRRP application group through multiple devices, but only one device acts as the master device at any time to undertake the route forwarding function. The others are in the backup roles. Inter-router switching in the VRRP application group is fully transparent for the host in the LAN. The RFC 2338 defines the router switching rules:

- The VRRP protocol adopts the preemption method to select the master router. First, it compares the VRRP priorities that are set for the interfaces of the routers a VRRP group. The one with the highest priority becomes the master router and its status will become Master. If the priority of the routers is identical, compare the master IP addresses of the network interfaces, the one with larger IP address will become the master router to forward packets.
- After the master device is elected, the others are in the standby status and monitor the status of the master device through the VRRP message sent by the master device. In normal operation, the master router sends a VRRP message at an interval, called advertised message, to notify the standby devices. The master

device is in the normal working status. If the standby device within the group doesn't receive the message from the master device for a long time, it becomes the master. If more than one device within the group become master, repeat the preempt process in step 1.In this process, the device with the maximum priority will be selected as the master router to execute the VRRP backup function.

Figure-1: VRRP working principles



Once a master device is elected in a VRRP backup group, the hosts in the LAN will execute route forwarding through that master device. The communication process is illustrated in Figure-1.

As you can see, R1 and R2 are connected with LAN 192.168.12.0/24 through the VRRP-enabled Ethernet interface Fa0/0. All hosts in the LAN use the IP address of the virtual router of the VRRP group as the default gateway. The hosts in the LAN only know the virtual router of the VRRP group, while the master router in the VRRP which is implementing the forwarding function is transparent to them. For example, if host PC 1 in the LAN is communicating with host PC 2 in another network, PC 1 will use the virtual router as the default gateway to send packets to PC 2. After receiving the packets, the master router in the VRRP group forwards them to PC 2. In this communication process, PC 1 only feels the virtual device but does not know whether R1 or R2 works. The master router is elected between R1 and R2 in the VRRP group. Once the master router fails, the other router automatically becomes the master.

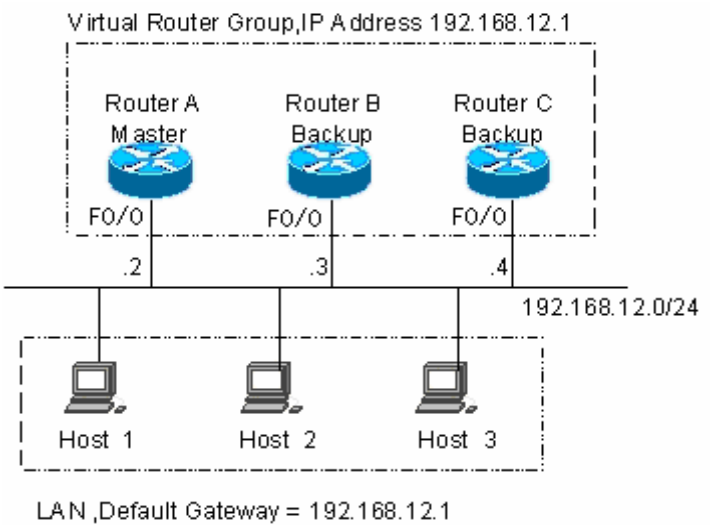
1.2 VRRP Applications

There are two VRRP application modes: basic and advanced. In basic applications, simple redundancy is implemented with a single backup group, while in advanced applications multiple backup groups are used to implement both route redundancy and load balancing.

1.2.1 Route Redundancy

The basic VRRP applications are illustrated in Figure-2.

Figure-2: Basic VRRP applications

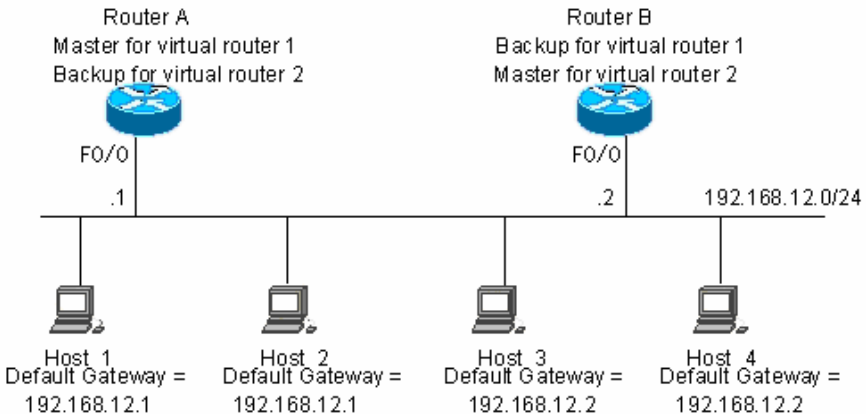


As shown in Figure-2, routers A, B and C are connected with the LAN through an VRRP-enabled Ethernet interface. They are in the same VRRP group with virtual IP address 192.168.12.1. Router A is elected as the master router of the VRRP, and routers B and C are standby routers. Hosts 1, 2 and 3 in the LAN use the IP address of the virtual router 192.168.12.1 as the gateway. The packets from the hosts in the LAN to other networks will be forwarded by the master router (router A in Figure-2). Once router A fails, the master router preempted between routers B and C undertakes the route forwarding function of the virtual device, resulting in a simply route redundancy.

1.2.2 Load Balancing

The advanced VRRP applications are illustrated in Figure-3.

Figure-3: Advanced VRRP applications



As shown in Figure-3, two virtual devices are set. For virtual router 1, router A uses the IP address of Ethernet interface Fa0/0 192.168.12.1 as the IP address of the virtual router, and thus router A becomes the master router and router B becomes the backup. For virtual router 2, router B uses the IP address of Ethernet interface Fa0/0 192.168.12.2 as the IP address of the virtual router, and thus router B becomes the

master router and router A becomes the backup. In the LAN, hosts 1 and 2 use the IP address of virtual router 1 192.168.12.1 as the default gateway, while hosts 3 and 4 use the IP address of virtual router 2 192.168.12.2 as the default gateway. In this VRRP application, router A and router B provide the route redundancy to share the traffic from the LAN, that is, load balancing.

1.3 VRRP Configuration

1.3.1 VRRP Configuration Task List

The VRRP is applicable for the multicast or broadcast LANs, such as Ethernet. The configuration of the VRRP is concentrated on the Ethernet interfaces. The configuration tasks are as follows:

- Enable VRRP backup function (mandatory)
- Set the authentication string of the VRRP backup group (optional)
- Set the advertisement interval of the VRRP backup group (optional)
- Set the preemption mode of the router in the VRRP backup group (optional)
- Set the priority of the router in the VRRP backup group (optional)
- Set the interface to be monitored by the VRRP backup group (optional)
- Set the IP address to be monitored by the VRRP backup group (optional)
- Set the learning function of the VRRP advertisement timer device(optional)
- Set the description string of the router in the VRRP backup group (optional)
- Set the delay reload of the VRRP backup group(optional)

Not all of the tasks are required here. Tasks that are required for a VRRP backup group depend on user requirements.

1.3.2 Enabling VRRP Backup Function

By specifying the backup group number and virtual IP address, you may add a backup in the specified LAN network segment to enable the VRRP backup function of the related Ethernet interfaces.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **ip** *ipaddress* [**secondary**]	Enable VRRP.
DES-7200(config-if)# **no vrrp** *group* **ip** *ipaddress* [**secondary**]	Disable VRRP.

The backup group number is in the range of 1 to 255. If the virtual IP address *ipaddress* is not specified, the router will not participate in the VRRP backup group. If

the **secondary** parameter is not used, the IP address set here will become the master IP address of the virtual router.

Note

If the virtual IP address (Primary or Secondary) of the VRRP group is the same as the IP address (Primary or Secondary) of the Ethernet interface, it is considered that the VRRP group occupies the actual IP address of the Ethernet interface, and the priority of the VRRP group is 255. If the corresponding Ethernet interface is available, the VRRP group will become the Master status automatically.

For NMX-2GEH line card, each interface supports up to 14 VRRP backup groups. It will prompt the error if the number of VRRP group exceeds 14.

1.3.3 Setting the Authentication String for the VRRP Backup Group

The VRRP supports plaintext password authentication mode and no authentication mode. When the authentication string is set for the VRRP backup group, it is also required to set the VRRP group to be in the plaintext password authentication mode. The members in the VRRP group must be in the same authentication mode for normal communication. In the plaintext authentication mode, the routers in the same VRRP group must have the same authentication password configured. The plaintext authentication password cannot provide security. It aims only to prevent/prompt the incorrect VRRP configuration.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **authentication** *string*	Set the authentication string of the VRRP.
DES-7200(config-if)# **no vrrp** *group* **authentication**	Set no authentication for VRRP.

By default, the VRRP is in the no authentication mode. For the plaintext password authentication mode, the length of the plaintext authentication mode cannot be greater than 8 bytes.

1.3.4 Setting the Advertisement Interval of the VRRP Backup Group

Command	Purpose

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **timers advertise** *interval*	Set the master device VRRP advertisement interval.
DES-7200(config-if)# **no vrrp** *group* **timers advertise** [*interval*]	Restore the VRRP advertisement interval of the master device to the default value.

If the current device becomes the master in the VRRP group, it will notify its VRRP status, priority and more information by sending VRRP advertisements at the specified interval. By default, this interval is 1 second.

Note

When the VRRP timer learning function is not configured, the routers in a VRRP group should be configured with the same VRRP advertisement interval; otherwise, the routers in the standby status will drop the received VRRP advertisement

1.3.5 Setting the Preemption Mode of the Router in the VRRP Backup Group

If the VRRP group is working in the preemption mode, once it finds its priority is higher than the Master priority, it will preempt to become the master of the VRRP group. If the VRRP group is not working in the preemption mode, even if a device finds its priority is higher than the Master priority, it will not preempt to become the master of the VRRP group. In case the VRRP group is using the Ethernet interface IP address, the setting of the preemption mode does not make sense, because this VRRP group has the highest priority and thus it automatically become the master in the VRRP group.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **preempt** [**delay** *seconds*]	Set VRRP backup group to work in the preemption mode
DES-7200(config-if)# **no vrrp** *group* **preempt** [**delay**]	Set VRRP backup group to work in the preemption mode

The optional parameter **delay seconds** defines the delay for the VRRP router prepares to declare its Master identify, 0 seconds by default. Once the VRRP function is enabled, the VRRP group will work in the preemption mode by default.

1.3.6 Setting the Accept_ Mode of IPv6 VRRP Virtual Router

IPv6 VRRP virtual router in Master state can use Accept_Mode to determine whether or not to receive and handle packets destined to the virtual router. If Accept_Mode is configured, it means that the IPv6 VRRP virtual router in Master state needs to receive

and handle any packets destined to the virtual router; if Accept_Mode is not configured, it means that the IPv6 VRRP virtual router in Master state will discard any packets destined to the virtual router, but it will not discard NA and NS packets. The Accept_Mode is not configured by default. In addition, IPv6 VRRP Master in Owner state will accept and handle all packets destined to the virtual router, no matter the Accept_Mode has been configured or not.

Command	Purpose
DES-7200(config-if)# **vrrp ipv6** *group* **accept_mode**	Configure the Accept_Mode of IPv6 VRRP backup group.
DES-7200(config-if)# **no vrrp ipv6** *group* **accept_mode**	Disable the Accept_Mode of IPv6 VRRP backup group.

1.3.7 Setting the Priority of the Router in the VRRP Backup Group

The VRRP protocol provides that the priority parameter of the device determines its position in the backup group. The device that has the highest priority in the preempt mode and has the virtual IP address becomes the active (or master) device in the backup group. Other devices of lower priority in the same group become the backup (or monitoring) devices. Once the VRRP function is enabled, the VRRP group has 100 as its default priority.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **priority** *level*	Set the priority of the VRRP backup group.
DES-7200(config-if)# **no vrrp** *group* **priority**	Restore the default of the VRRP priority

The priority level range is 1~254. If the VRRP virtual IP address is the same as the actual IP of the Ethernet interface, the priority of the corresponding VRRP group is 255. Now no matter whether the VRRP group in the preemption mode, the corresponding VRRP group will be in the Master status automatically (as long as the corresponding Ethernet interface is available).

1.3.8 Setting the Interface to be Monitored by the VRRP Backup Group

After the interface to be monitored by the VRRP backup group is configured, the system will dynamically adjust the priority of the router according to the monitored

interface. Once the status of the monitored interface becomes unavailable, the priority of the router in the VRRP backup group will be decreased according to the preset value. At the same time, another router in the backup group which has a more stable interface status or higher priority will become the active (master) router of the VRRP backup group.

Command	Purpose
DES-7200(config-if)# **vrrp** group **track** *interface-type number* *[interface –priority]*	Set the interface to be monitored by the VRRP backup group
DES-7200(config-if)# **no vrrp** *group* **track** *interface-type number*	Cancel setting of the interface to be monitored by the VRRP backup group

By default, there is no interface configured to be monitored by the VRRP backup group. The parameter *interface –priority* ranges 1~255. If the parameter *interface –priority* is default, the system will use the default value 10.

Note

The monitored interface only is layer-3 routable logical interfaces (such as Routed Port, SVI, Loopback and Tunnel).

1.3.9 Setting the IP/IPv6 address to be Monitored by the VRRP Backup Group

After the IP address to be monitored by the VRRP backup group is configured, the system will dynamically adjust the priority of local device according to the monitored address. Once the status of the monitored IP address becomes unreachable or it is unable to ping the monitored IP address, the priority of native device in the VRRP backup group will be decreased according to the preset value. At the time, another routing device in the same backup group which has a higher priority will become the active (master) router of the VRRP backup group. The optional parameter *interval–value* shows the interval time of probing whether the destination address is reachable or not. The Optional parameter *timeout-value* shows the timeout time of pinging the destination address.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **track** *ip-address* [[[**interval** *interval-value*] **timeout** *timeout-value*] *priority*]	Configure the IP address monitored by IPv4 VRRP backup group.
DES-7200(config-if)# **no vrrp** *group* **track** *ip-address*	Remove the IP address monitored by IPv4 VRRP backup group.

Command	Purpose
Or：	
DES-7200(config-if)# **vrrp ipv6** *group* **track** {*ipv6-global-address* | {*ipv6-linklocal-address interface-type number*}} [[[**interval** *interval-value*] **timeout** *timeout-value*] *priority*]	Configure the IP address monitored by IPv6 VRRP backup group.
DES-7200(config-if)# **no vrrp ipv6** *group* **track** {*ipv6-global-address* | {*ipv6-linklocal-address interface-type number*}}	Remove the IP address monitored by IPv6 VRRP backup group.

By default, there is no IP address configured to be monitored by the VRRP backup group. The parameter *interval–value* ranges 1~3600s. If the parameter *interval–value* is default, the system will use the default value 3s. The parameter *timeout–value* ranges 1~60s. If the parameter *timeout–value* is default, the system will use the default value 1s. Note that the *timeout-value* must be less than or equal to interval-value. The parameter *priority* ranges 1~255. If the parameter *priority* is default, the system will use the default value 10. To configure VRRP IPv6 address, you must first configure VRRP IPv6 link-local address. If the monitored address is a link-local address, the interface shall be specified as well.

1.3.10 Setting the Learning Function of VRRP Advertisement Timer Device

Once the timer learning function is enabled, if the current router is VRRP backup router, after setting the timer learning function, the router will learn VRRP advertisement sending interval from VRRP advertisement of the master router and calculate the failure judgment interval of master router. It does not calculate by VRRP advertisement sending interval set locally. Use this command to synchronize the VRRP advertisement timer between the backup router and master router.

Command	Function
DES-7200(config-if)# **vrrp group timers learn**	Set the timer learning function.
DES-7200(config-if)# **no vrrp group timers learn**	Delete the timer learning function.

By default, the VRRP group timer learning function is not set.

Note

In case the advertisement sending interval in VRRP advertisement received by VRRP backup router is inconsistent with the advertisement interval set locally, if the timer learning function is not configured on the VRRP backup router, the VRRP backup router will drop the VRRP advertisement; otherwise, it will receive the VRRP advertisement and calculate failure judgment interval of VRRP Master router by the advertisement interval.

1.3.11 Setting the Description String of the Router in the VRRP Backup Group

This command will set the descriptor for the VRRP group to facilitate identifying the VRRP group.

Command	Purpose
DES-7200(config-if)# **vrrp** *group* **description** *text*	Set the description string of the VRRP group.
DES-7200(config-if)# **no vrrp** *group* **description**	Cancel the description string of the VRRP group.

By default, the VRRP backup group has no description string configured. The length of the VRRP backup group description string is 80 by maximum.

Note

If blanks are contained in the description string of the VRRP backup group, quotation marks (") must be used to identify the description string.

1.3.12 Setting the Delay Reload of the VRRP Backup Group

This command will set the delay reload time of the VRRP backup group on an interface. The delay reload time has two types: the one when the system reloads and the one when the interface becomes active. You can set those two types of delay reload time separately or simultaneously.

In the non-preemption mode, when the VRRP backup group with higher priority reloads, it can not preempt the master router in the same backup group. However, even though the non-preemption mode is configured, the reloading VRRP backup group can also preempt the VRRP master router. That is because when the router reloads or the interface becomes active, the VRRP backup group on the interface fails to receive the VRRP packets sent from the master router in the same backup group in time.

At this time, you can enable the VRRP backup group to delay reload using the following command. After configuring this command, when the system reloads or the interface becomes active, the VRRP backup group on the interface can not reload immediately, but reload after the preset delay time, and the non-preemption configuration is still effective.

If the VRRP packets are received on the interface when the delay reload of VRRP backup group is configured, the delay reload configuration will be cancelled and the VRRP will be enabled immediately.

Command	Purpose
DES-7200(config-if)# **vrrp delay** { [**minimum** *min-seconds*] [**reload** *reload-seconds*] }	Set the delay reload of the VRRP group on the interface.
DES-7200(config-if)# **no vrrp delay**	Cancel the delay reload of the VRRP group.

By default, the VRRP backup group has no delay reload of VRRP backup group configured. The two types of the delay reload of the VRRP backup group ranges 0-60s.

1.3.13 Setting the VRRP Packet Version of IPv4 VRRP

Use this command to configure VRRP packet version of IPv4 VRRP: VRRPv2 or VRRPv3. VRRPv2 is the default version.

Command	Purpose
DES-7200(config-if)# **vrrp *group* version {***2* **|** *3***}**	Configure VRRP packet version of IPv4 VRRP
DES-7200(config-if)# **no vrrp *group* version**	Use the default version of VRRPv2

By default, the VRRP backup group has no description string configured. The length of the VRRP backup group description string is 80 by maximum.

1.4 Monitoring and Maintaining VRRP

Our products provide the **show vrrp** and **debug vrrp** commands to monitor and maintain VRRP. The **show vrrp** command is used to check the VRRP status of a local router; the **debug vrrp** command is used to check the information on the VRRP group status, received/sent VRRP advertisement and VRRP events.

1.4.1 show vrrp

Our product provides the following **show vrrp** commands to check the VRRP status of the local router.

Command	Purpose
DES-7200# **show vrrp** [**brief** | *group*]	Check the current VRRP status
DES-7200# **show vrrp interface** *type number* [**brief**]	Show the VRRP status of the specified network interface

Here are some examples of the command:

1. **show vrrp** command

```
DES-7200# show vrrp
GigabitEthernetFastEthernet 0/10 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
GigabitEthernetFastEthernet 0/20 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
```

The displayed messages above include the Ethernet name, VRRP backup group number configured on the interface, status, priority, preemption mode, VRRP advertisement interval, virtual IP address, virtual MAC address, Master router IP address, Master router priority, Master router advertisement interval, Master router failure judgment interval, current interface monitored by the VRRP backup group and corresponding priority change scale.

The current interface monitored by the VRRP backup group and the corresponding priority change metrics can be shown only after the monitoring interface function is enabled.

2. **show vrrp brief** command

```
DES-7200# show vrrp brief
Interface      Grp Pri Time Own Pre State   Master addr     Group addr
GigabitEthernet0FastEthernet0/0 1  100  3-    -    P  Backup 192.168.201.213
192.168.201.1
GigabitEthernet0FastEthernet0/0 2  120  -    -   P  Master  192.168.201.217
192.168.201.2
```

The information displayed above includes the Ethernet interface name, VRRP group number, priority, timeout period for backup turning into master, same as the interface IP address or not, preemption mode, master device IP address, and VRRP group IP address.

3. **show vrrp interface** command

```
DES-7200# show vrrp interface FastEthernet 0/1
GigabitEthernetFastEthernet 0/1 - Group 1
State is Backup
Virtual IP address is 192.168.201.1 configured
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 100
Master Router is 192.168.201.213 , pritority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
FastEthernet 0/1 - Group 2
State is Master
Virtual IP address is 192.168.201.2 configured
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 3 sec
Preemption is enabled
min delay is 0 sec
Priority is 120
Master Router is 192.168.201.217 (local), priority is 120
Master Advertisement interval is 3 sec
Master Down interval is 9 sec
DES-7200#
```

The displayed messages above include the specified Ethernet name, VRRP backup group number configured on the interface, status, priority, preemption mode, VRRP advertisement interval, virtual IP address, virtual MAC address, Master router IP address, Master router priority, Master router advertisement interval, Master router failure judgment interval, current interface monitored by the VRRP backup group and corresponding priority change scale.

1.4.2 debug vrrp

Our produce has the following **debug vrrp** commands to provide the VRRP status debugging information of the local router.

Command	Purpose
DES-7200# **debug vrrp errors**	Turn on the VRRP error prompt debug switch
DES-7200# **no debug vrrp errors**	Turn off the VRRP error prompt debug switch
DES-7200# **debug vrrp events**	Turn on the VRRP event debug switch
DES-7200# **no debug vrrp events**	Turn off the VRRP event debug switch
DES-7200# **debug vrrp packets**	Turn on the VRRP packet Debug switch
DES-7200# **no debug vrrp packets**	Turn off the VRRP packet debug switch
DES-7200# **debug vrrp state**	Turn on the VRRP state debug switch
DES-7200# **no debug vrrp state**	Turn off the VRRP status debug switch
DES-7200# **debug vrrp**	Turn on the VRRP debug switch
DES-7200# **no debug vrrp**	Turn off the VRRP debug switch

Here are some examples of the command:

1. **debug vrrp** command

```
DES-7200# debug vrrp
DES-7200#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Event - Advert higher or equal priority
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 1 state Master ->
Backup
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 1 state Backup ->
Master
DES-7200#
```

The **debug vrrp** command is equivalent to the joint execution of debug vrrp errors, debug vrrp events, `debug vrrp packets` and `debug vrrp state`.

2. **debug vrrp errors** command

```
DES-7200# debug vrrp errors
DES-7200#
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
VRRP: Grp 1 Advertisement from 192.168.201.213 has invalid virtual address
192.168.1.1
```

The above displayed information indicates the VRRP advertisement comes from 192.168.201.213 for VRRP group 1. The virtual IP address 192.168.1.1 in the advertisement is not in local VRRP group 1.

3. **debug vrrp events** command

```
DES-7200# debug vrrp events
```

```
DES-7200#
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
VRRP: Grp 1 Event - Advert higher or equal priority
DES-7200#
```

The above displayed information indicates the priority in the VRRP advertisement received by the local VRRP group is not lower than the local priority.

4. **debug vrrp packets** command

```
DES-7200#debug vrrp packets
DES-7200#
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
VRRP: Grp 2 sending Advertisement checksum DD4D
```

The above displayed information indicates the local VRRP group 2 is sending VRRP advertisement, whose VRRP checksum is 0XDD4D.

```
DES-7200# debug vrrp packets
DES-7200#
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
VRRP: Grp 1 Advertisement priority 120, ipaddr 192.168.201.213
```

The above displayed information indicates the VRRP advertisement is received from 192.168.201.213 for VRRP group 1, whose priority is 120.

5. **debug vrrp state** command

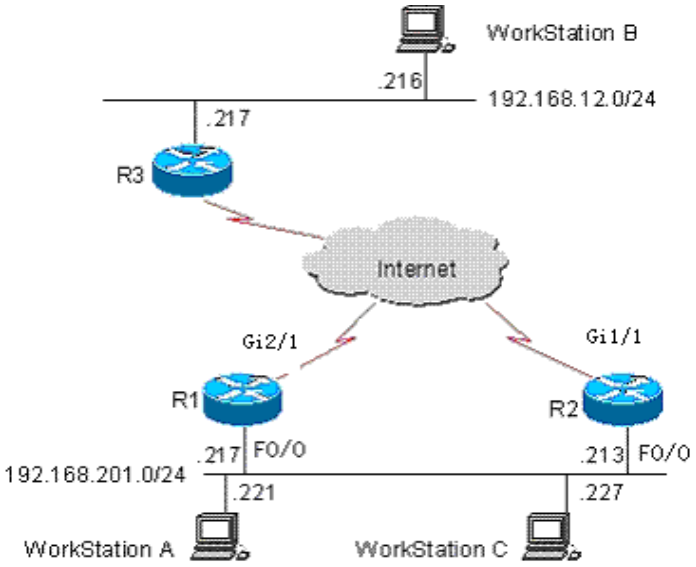
```
DES-7200# debug vrrp state
VRRP State debugging is on
DES-7200#
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 2 state Master ->
Backup
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 2 state Backup ->
Master
DES-7200# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernetfastethernet 0/0
DES-7200(config-if)# no shutdown
DES-7200(config-if)# end
DES-7200#
%VRRP-6-STATECHANGE: GigabitEthernetFastEthernet 0/0 Grp 2 state Master ->
Init
DES-7200#
```

The above displayed information indicates the VRRP group status on GigabitEthernet 0/0 is shifting among Master, Backup and Init.

1.5 Example of Typical VRRP Configuration

As shown in Figure-4, the VRRP backup group is configured on R1 and R2 to provide VRRP services for 192.168.201.0 /24. R3 is not configured with VRRP but just common routing functions. The following shows the VRRP configuration of R1 and R2.

Figure-4: Network connection with VRRP



In the configuration example below, the configurations of device R3 remain unchanged, The configuration on device R3 is shown below:

```
DES-7200# configure terminal
DES-7200(config)# !
!
hostname "R3"
!
!
!
interface gigabitEthernetFastEthernet 0/0
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.12.217 255.255.255.0
DES-7200(config-if)# exit
DES-7200(config)# !
interface GigabitEthernet 1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 60.154.101.5 255.255.255.0
DES-7200(config-if)# exit!
DES-7200(config)# interface GigabitEthernet 2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 202.101.90.61 255.255.255.0
DES-7200(config-if)# exit!
DES-7200(config)# router ospf 1
DES-7200(config-router)# network 202.101.90.0 0.0.0.255 area 10
```

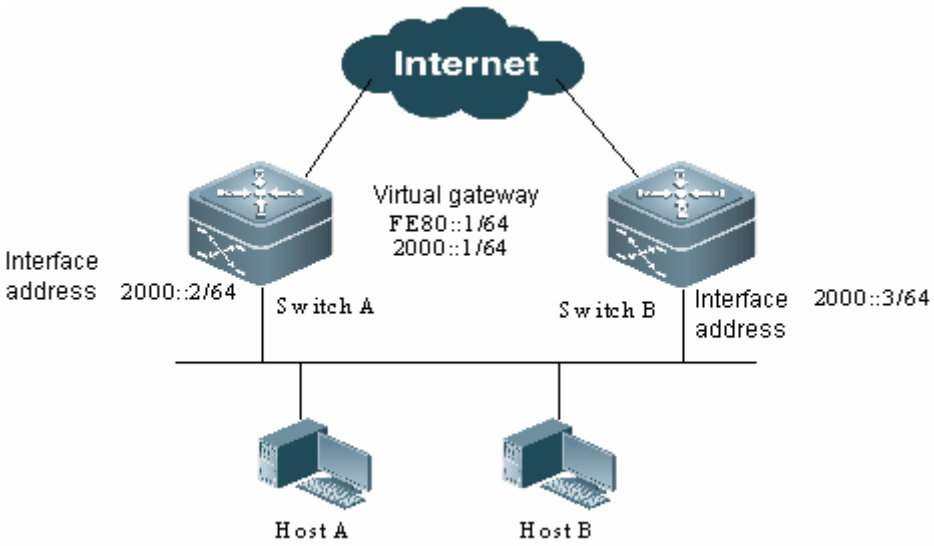
```
DES-7200(config-router)# network 192.168.12.0 0.0.0.255 area 10
DES-7200(config-router)# network 60.154.101.0 0.0.0.255 area 10
DES-7200(config-router)# !
!
!
end
```

1.5.1 Example of Single VRRP Backup Group Configuration

1.5.1.1 Networking Requirements

- Host A and Host B need to access Internet resources through the gateway, using 2000::1/64 as the default gateway;
- Switch A and Switch B belong to backup group 1 of IPv6 virtual router, with the virtual addresses of 2000::1/64 and FE80::1;
- When Switch A operates normally, packets sent from Host A to Internet are forwarded by Switch A; when Switch A fails, packets sent from Host A to Internet are forwarded by Switch B.

1.5.1.2 Network Topology



1.5.1.3 Configuration Steps

1) Configure Switch A:

```
!
!
```

```
!
# Configure the IPv6 address of interface in order to enable IPv6 service on
the interface
interface FastEthernet 0/1
no switchport
ipv6 address 2000::2/64
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
# Configure the priority of Switch A in VRRP group as 120
vrrp ipv6 1 priority 120
# Adjust the advertisement interval of VRRP group to 3s
vrrp ipv6 1 timers advertise 3
# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 1 accept_mode
!


!
!
```

Configure Switch B:

```
!
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/1
no switchport
ipv6 address 2000::3/64
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
# Configure the priority of Switch B in VRRP group as 100
vrrp ipv6 1 priority 100
# Adjust the advertisement interval of VRRP group to 3s
vrrp ipv6 1 timers advertise 3
# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 1 accept_mode
!
!
!
```

We can see that Switch A and Switch B are in IPv6 VRRP backup group 1 pointing to the same IPv6 address (2000::1) of virtual router and operating in VRRP preemptive mode. Since the priority of Switch A in IPv6 VRRP backup group is 120 and the priority of Switch B in VRRP backup group is 100 (default value), Switch A will act as the Master router of IPv6 VRRP under normal conditions.

1.5.1.4 Verification

After configuration, execute "show ipv6 vrrp 1" command to view VRRP configurations.

Display the configurations of Switch A

```
DES-7200#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
```

Display the configurations of Switch B

```
DES-7200#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

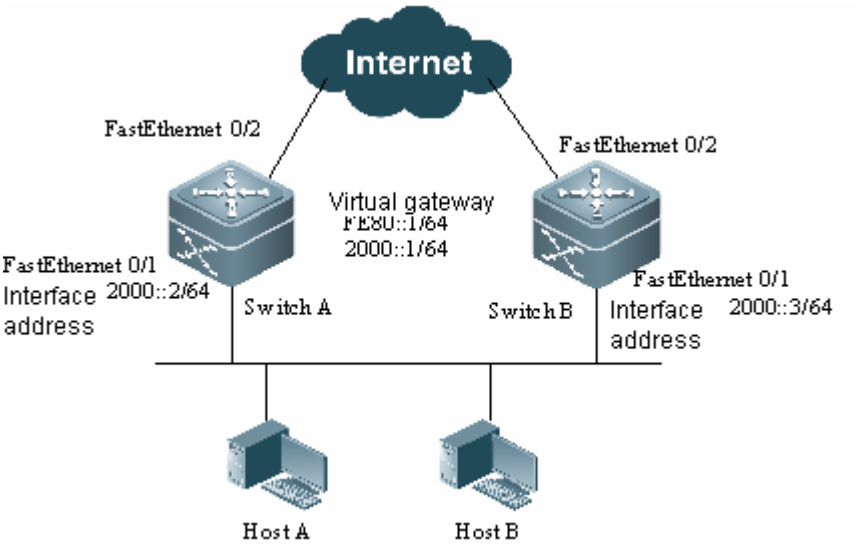
1.5.2 Example of configuration to monitor interface with VRRP

1.5.2.1 Networking Requirements

- Host A and Host B need to access Internet resources through the gateway, using 2000::1/64 as the default gateway;

- Switch A and Switch B belong to backup group 1 of IPv6 virtual router, with the virtual addresses of 2000::1/64 and FE80::1;
- Switch A monitors its Internet-connecting interface of Fastethernet 0/2. When Fastethernet 0/2 is not available, VRRP 1 on Switch A will reduce its priority, and Switch B will take over the role of gateway.

1.5.2.2 Network Topology



1.5.2.3 Configuration Steps

1) Configure Switch A:

```
!
!
!
# Configure the IPv6 address of interface in order to enable IPv6 service on
the interface
interface FastEthernet 0/0
no switchport
ipv6 address 2000::2/64
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
!
# Configure the priority of Switch A in VRRP group as 120
vrrp ipv6 1 priority 120
!
# Adjust the advertisement interval of VRRP group to 3s
```

```
vrrp ipv6 1 timers advertise 3
!
# Configure VRRP 1 to track interface FastEthernet 0/2
vrrp ipv6 1 track FastEthernet 0/2 50
# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 1 accept_mode


!
!
```

Configure Switch B:

```
!
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/0
no switchport
ipv6 address 2000::3/64
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
# Configure the priority of Switch B in VRRP group as 100
vrrp ipv6 1 priority 100
!
# Adjust the advertisement interval of VRRP group to 3s
vrrp ipv6 1 timers advertise 3
# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 1 accept_mode
!
!
!
```

We can see that Switch A and Switch B are in IPv6 VRRP backup group 1 pointing to the same IPv6 address (2000::1) of virtual router and operating in VRRP preemptive mode. Since the priority of Switch A in IPv6 VRRP backup group is 120 and the priority of Switch B in VRRP backup group is 100 (default value), Switch A will act as the Master router of IPv6 VRRP under normal conditions. If Switch A as the Master device detects that interface FastEthernet 0/2 is not available, it will reduce its priority in VRRP backup group by 50 (the priority becomes 70). In this way, Switch B becomes the Master device. After this, if Switch A detects that its interface of FastEthernet 0/2 becomes available again, it will increase its priority by 50 (the priority becomes 120 again), so that Switch A will become the Master device again.

1.5.2.4 Verification

After configuration, execute "show ipv6 vrrp 1" command to view VRRP configurations.

Display the configurations of Switch A

```
DES-7200#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
Tracking state of 1 interface, 1 up:
    up FastEthernet 0/2 priority decrement=50
```

Display the configurations of Switch B

```
DES-7200#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

1.5.3 Example of Multiple VRRP Backup Groups

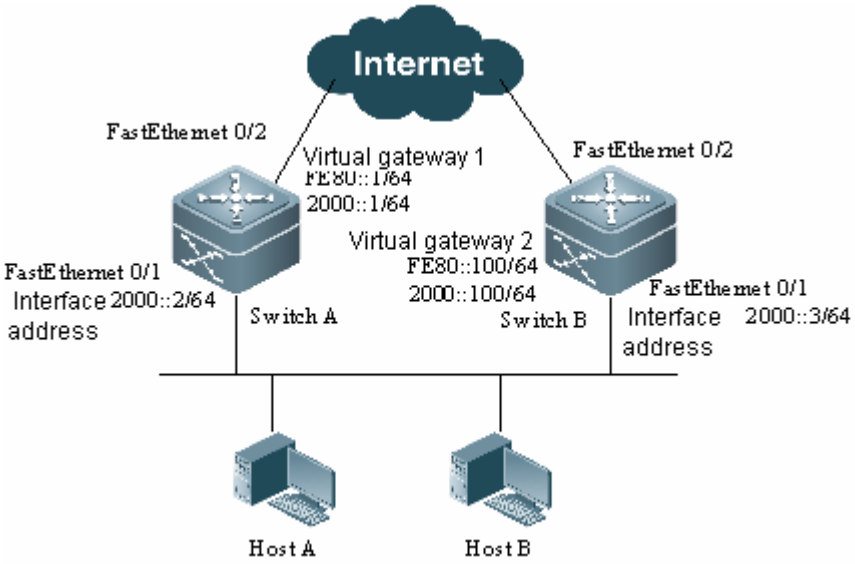
Besides single backup group, our products also support multiple VRRP backup groups configured on the same Ethernet interface. The advantage of using multiple backup groups is: allow load balancing while providing more stable and reliable network service through mutual backup.

1.5.3.1 Networking Requirements

- Host A and Host B need to access Internet resources through the gateway, using 2000::1/64 and 2000::100/64 as the default gateways;

- Switch A and Switch B belong to backup group 1 of IPv6 virtual router, with the virtual addresses of 2000::1/64 and FE80::1;
- Meanwhile, Switch A and Switch B also belong to backup group 2 of IPv6 virtual router, with the virtual addresses of 2000::100/64 and FE80::100;
- Both Switch A and Switch B act as the gateway forwarding traffic and serve as the backup of each other.

1.5.3.2 Network Topology



1.5.3.3 Configuration Steps

1) Configure Switch A:

```
!
!
# Configure the IPv6 address of interface in order to enable IPv6 service on
the interface
interface FastEthernet 0/0
no switchport
ipv6 address 2000::2/64
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
!
# Configure the priority of Switch A in VRRP group as 120
vrrp ipv6 1 priority 120
!
# Adjust the advertisement interval of VRRP group to 3s
```

```
vrrp ipv6 1 timers advertise 3
# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 1 accept_mode
!
# Create a VRRP group 2 and set its virtual IPv6 address to FE80::100 and
2000::100
vrrp 2 ipv6 FE80::100
vrrp 2 ipv6 2000::100
!
# Configure the priority of Switch A in VRRP group as 100
vrrp ipv6 2 priority 100

! # Adjust the advertisement interval of VRRP group to 3s
vrrp ipv6 2 timers advertise 3

# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 2 accept_mode
```

Configure Switch B:

```
!
!
interface FastEthernet 0/0
no switchport
ipv6 address 2000::3/64
!
# Create a VRRP group 1 and set its virtual IPv6 address to FE80::1 and 2000::1
interface FastEthernet 0/0
vrrp 1 ipv6 FE80::1
vrrp 1 ipv6 2000::1
# Configure the priority of Switch B in VRRP group as 100
vrrp ipv6 1 priority 100
!
# Adjust the advertisement interval of VRRP group to 3s
vrrp ipv6 1 timers advertise 3
# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 1 accept_mode
!
!
# Create a VRRP group 2 and set its virtual IPv6 address to FE80::100 and
2000::100
vrrp 2 ipv6 FE80::100
vrrp 2 ipv6 2000::100
!
# Configure the priority of Switch B in VRRP group as 120
vrrp ipv6 2 priority 120

! # Adjust the advertisement interval of VRRP group to 3s
vrrp ipv6 2 timers advertise 3
!
```

```
# Configure the Accept_Mode of IPv6 VRRP
vrrp ipv6 2 accept_mode
!
```

We can see that Switch A and Switch B are in IPv6 VRRP backup group 1 pointing to the same IPv6 address (2000::1) of virtual router and operating in IPv6 VRRP preemptive mode. As for backup group 1, since the priority of Switch A in VRRP backup group is 120 and the priority of Switch B in VRRP backup group is 100 (default value), Switch A will act as the Master router of IPv6 VRRP backup group 1 under normal conditions. As for backup group 2, since the priority of Switch A in IPv6 VRRP backup group is 100 and the priority of Switch B in IPv6 VRRP backup group is 120, and backup group 2 operates in preemptive mode, Switch B will act as the Master router of IPv6 VRRP backup group 2 under normal conditions. For hosts in the same LAN, Host A takes backup group 1 as the default gateway, and Host B takes backup group 2 as the default gateway. Router redundancy is realized between Router A and Router B, which share the traffic from LAN in the mean time to achieve load balancing. In this example, you must manually configure the default gateway for IPv6 hosts in order to achieve load balancing feature of IPv6 VRRP backup group.

1.5.3.4 Verification

After configuration, execute "show ipv6 vrrp" command to view VRRP configurations.

Display the configurations of Switch A

```
DES-7200#show ipv6 vrrp
FastEthernet 0/1 - Group 1
  State is Master
  Virtual IPv6 address is as follows:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::1234 (local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec

FastEthernet 0/1 - Group 2
  State is Backup
  Virtual IPv6 address is as follows:
FE80::100
2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
```

```
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::5678, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec
```

Display the configurations of Switch B

```
DES-7200#show ipv6 vrrp 1
FastEthernet 0/1 - Group 1
  State is Backup
  Virtual IPv6 address is as follow:
FE80::1
2000::1
  Virtual MAC address is 0000.5e00.0201
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 100
  Master Router is FE80::1234, priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.82 sec

FastEthernet 0/1 - Group 2
  State is Master
  Virtual IPv6 address is as follows:
FE80::100
2000::100
  Virtual MAC address is 0000.5e00.0202
  Advertisement interval is 3 sec
  Accept_Mode is enabled
  Preemption is enabled
    min delay is 0 sec
  Priority is 120
  Master Router is FE80::5678(local), priority is 120
  Master Advertisement interval is 3 sec
  Master Down interval is 10.59 sec
```

1.6 Diagnosing and Troubleshooting VRRP

You can troubleshoot VRRP failures by viewing configuration and debugging information. Here is analysis of some common faults.

Symptom: Unable to ping the virtual IP address

Analysis:

- Ensure at least one router in the backup group is active.
- If it is possible to ping the virtual IP address from other network devices, the causes may be the VRRP status changing needs some time (although brief). Execute the **show vrrp** command to check the VRRP information and confirm this.
- If the local network device is in the same network segment of the virtual router, check whether ARP table of the local network device contains the APP entry for the IP virtual address. If no, check the network lines.
- If the local network device is not in the same network segment of the virtual router, make sure the local network device has a router to the virtual IP address.

Symptom: multiple master devices in the same VRRP backup group

Analysis:

- In the same VRRP backup group, the Ethernet interfaces of those routers are in different VRRP group authentication modes.
- In the same VRRP backup group, the Ethernet interfaces of those routers are in the plaintext password VRRP group authentication mode, but the authentication strings are not the same.
- In the same VRRP backup group, the cables the Ethernet interfaces of some routers may be disconnected, since the routers fail to detect that.
- In the same VRRP backup group, the VRRP advertisement interval is inconsistent and the timer learning function is not configured.
- In the same VRRP backup group, the virtual IP address for the routers are not the same.

2 VRRP Plus Configuration

2.1 Overview

VRRP Plus (Virtual Router Redundancy Protocol Plus) is the extension to VRRP protocol. It utilizes VRRP protocol to perform gateway backup and load balancing in an IEEE 802.3 LAN.

One drawback of VRRP is that the backup router doesn't participate in packet forwarding. To achieve load balancing by utilizing VRRP, we need to manually configure multiple VRRP groups, and point the gateway of LAN hosts to the virtual IP of different VRRP groups. This will increase the workload of network administrator. VRRP Plus is introduced to address the aforementioned drawback.

The benefit of VRRP Plus is automatic load balancing. It will automatically distribute the traffic from different hosts to VRRP Plus members, thus substantially easing the load of network administrator.

2.2 Working Principle

Basic principle of VRRP Plus: Hosts in the LAN use the same gateway IP. When different hosts send ARP requests to the gateway, VRRP Plus will reply with different virtual MAC addresses, thus distributing the traffic from different hosts to different VRRP Plus members and allowing load balancing.

VRRP Plus has introduced two roles:

BVG: Balancing Virtual Gateway, which is responsible for distributing virtual MAC addresses among VRRP Plus members, replying to gateway ARP requests and forwarding packets sent by hosts in the LAN.

BVF: Balancing Virtual Forwarder, which is responsible for forwarding packets sent by hosts in the LAN.

VRRP Plus is independent from the VRRP protocol and features the following rules:

The Master role in VRRP corresponds to the BVG role in VRRP Plus; the Backup role in VRRP corresponds to the BVF role in VRRP Plus. The gateway of LAN hosts still points the same virtual IP as mentioned in VRRP.

BVG is responsible for distributing virtual MAC addresses to BVFs. In order to be compatible with VRRP, BVG directly uses the virtual MAC address of VRRP, namely 00-00-5E-00-01-{VRID} (VRID is the ID of VRRP group). BVF uses the virtual MAC address of 00-1A-A9-16-{MemberID}-{VRID}. MemberID is the ID of VRRP Plus member. Currently, VRRP Plus can support four members. BVG uses the member ID of 01, while other three BVF members use ID 02-04.

BVG responds to the ARP requests sent by hosts in the LAN. Depending on different balancing policies, BVG will reply with different virtual MAC addresses. There are three balancing policies: host-dependent, round-robin and weighted. The host-dependent policy indicates that BVG will reply with specific virtual MAC address to the specific host; the round-robin policy indicates that BVG will respond to the ARP requests with the virtual MAC addresses in the backup group by rotation; the weighted policy indicates that BVG will respond to ARP requests according to the forwarding capacity of the device.

VRRP Plus also provides the feature of redundant backup. BVG can utilize VRRP-BFD session information to establish session with BVF, so as to detect the active state of BVF within milliseconds. If BVF fails, BVG will arrange one of the remaining members to take over the forwarding function of the failed BVF. This feature is called proxy forwarding. If BVF recovers from the fault, then it will restore its forwarder role and continue to forward packets of this virtual MAC address. However, if such device doesn't recover, then the backup group shall stop redirecting traffic to this virtual MAC address, namely further ARP requests will no longer be replied with this virtual MAC address. Moreover, after a long-enough time, we can assume that users using this virtual MAC address as the gateway MAC address have already updated ARP entry of gateway address, with traffic being handled by other devices. By this time, we can delete this virtual MAC address, and packets sent to this virtual MAC address shall be dropped. For this reason, VRRP Plus supports the configuration of redirect and timeout timers of the backup group. When the device fails, the backup group will assign the virtual MAC address to other device for proxy forwarding. Within the redirect time, the backup group will continue to reply to ARP requests with this virtual MAC address; after the redirect timer runs out, it will no longer reply with this virtual MAC address. Upon expiration of the timeout timer, the backup group will delete this virtual MAC address.

VRRP Plus supports weighting configuration of the backup group. By configuring different weights for difference devices, those with larger weights will share more traffic and those with smaller weights will share less traffic, so that the forwarding capacity of difference devices can be fully utilized. When the weighting value of BVF device in the backup group is below the lower

threshold, it will automatically quit the forwarding role. When the weighting value recovers and is beyond the upper threshold, it will automatically resume the forwarding role.

VRRP Plus supports the linkage with link detection protocol and weighting value adjustment as per link status. Each device in the backup group can associate with the corresponding link status. When a certain link fails, the device will automatically decrease its weighting value; if the weighting value is too low, it will quit the forwarding role. If the backup group is using the weighted load balancing policy, it can then allocate the corresponding traffic according to the new weighting value. When the associated link status recovers, this device will automatically recover the weighting value and resume the forwarding role. As for the backup group adopting weighted load balancing policy, it will allocate the traffic from different hosts according to the weighting value after recovery.

VRRP Plus supports the feature of forwarder preemption. VRRP Plus can only support up to four devices participating in load balancing, namely one VRRP Plus backup group will have four virtual MAC addresses at the most. When additional devices join a VRRP Plus group, only four devices will participate in packet forwarding, while the remaining devices will only listen to the status of other devices. The remaining devices will replace forwarder devices and forward packets only if they fail. When there are already four devices forming a VRRP Plus backup group and forwarding packets, if the fifth device joins the VRRP Plus group and boasts better forwarding capacity, or if the forwarding capacity of one original forwarder is reduced due to link failure, the fifth device will preempt the device with lower weighting value (lower forwarding capacity) if preemption function is enabled. Configure higher weighting value for device with better forwarding capacity, so that when the device in listening mode has a weighting value higher than that of the existing forwarder, the listening device can preempt the role of such forwarder. In this way, device with better forwarding capacity will be responsible for packet forwarding and device with lower forwarding capacity will listen to the status of other devices, thus reducing the waste of resources. Since the BVG device in the backup group is responsible for virtual MAC address assignment, the BVG role cannot be preempted. Only the forwarder role of BVFs can be preempted.

If BVG device fails, VRRP will reelect the Master and BVG will be generated on the new Master device.

After VRRP Plus is configured, ARP requests received from hosts will be replied according to different load balancing policies to allow load balancing of these hosts. However, hosts having learned the virtual gateway address of VRRP before VRRP Plus is configured will not participate in load balancing. Therefore, if VRRP Plus is configured after VRRP status is switched to Master, the load balancing cannot be truly achieved before the aging of the ARP

learned. The load balancing policy will only take effect after the gateway ARP ages and the host sends out a new request for gateway address.

The interface will periodically send out gratuitous ARP. This feature will also affect the load balancing function of VRRP Plus. When VRRP Plus is enabled, the feature of gratuitous ARP sending will be blocked. When the virtual address overlaps with the real address, it will stop sending gratuitous ARP packets about this address.

When the address of a host conflicts with the address of this device, the ARP module will also broadcast the gratuitous ARP packets about this address. If the host address conflicts with the virtual address of VRRP Plus, then the gratuitous ARP packets sent will lead to the circumstance that the MAC address of host gateway is relearned, thus compromising the load balancing function of VRRP Plus. In such a case, the load balancing function of VRRP Plus is not supported for the moment.

2.3 VRRP Plus Application

The application topology of VRRP Plus can be illustrated in Figure 1:

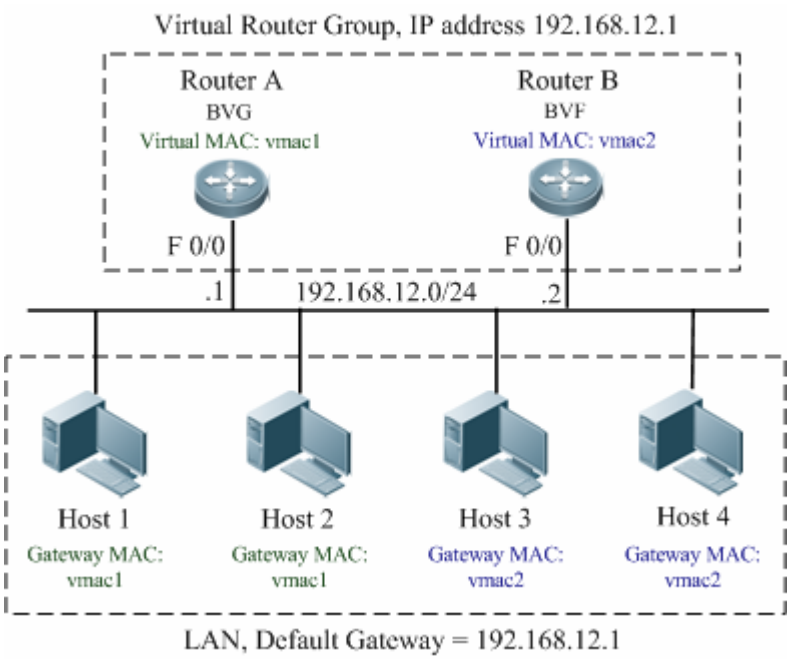


Fig 1 Topology of VRRP Plus application

The IP network segment of the LAN as shown in Figure 1 is 192.168.12.0/24. Two layer-3 devices (A and B) form a VRRP Plus group, with virtual IP being 192.168.12.1. Device A is the Master of VRRP acting as BVG, while device B is the Backup of VRRP acting as BVF. Four hosts in the LAN all point to the gateway of 192.168.12.1. When Host1 and Host2 send ARP requests to gateway, the MAC address replied will be 0000.5e00.0101; when Host3 and

Host4 send ARP requests to gateway, the MAC address replied will be 001A.A916.0201. In this way, packets sent by Host1 and Host2 for communicating with the exterior network will be forwarded to layer-3 device A, while packets sent by Host3 and Host4 will be forwarded to layer-3 device B, thus achieving load balancing.

2.4 Configurations of VRRP Plus

2.4.1 VRRP Plus Configuration Tasks

VRRP Plus protocol is applicable to IEEE 802.3 LAN and runs on Ethernet interface. To enable VRRP Plus, the user must configure VRRP first. The configuration tasks of VRRP Plus include:

Default configurations of VRRP Plus

(Required) Enable VRRP Plus

(Optional) Configure VRRP Plus load balancing policy

(Optional) Configure the redirect timer and timeout timer for the proxy virtual MAC address of VRRP Plus backup group

(Optional) Configure weighting and threshold for VRRP Plus backup group

(Optional) Configure forwarder preemption for VRRP Plus backup group

(Optional) Configure weighting tracking object for VRRP Plus backup group

2.4.2 Default Configurations

The following table describes the default configurations of VRRP Plus.

Function	Default setting
VRRP Plus	Not configured
Load balancing policy after VRRP Plus is enabled	Rotation-robin load balancing
Redirect time of proxy virtual MAC address after VRRP Plus is enabled	300 seconds (i.e., 5 minutes)
Timeout time of proxy virtual MAC address after VRRP Plus is enabled	14400 seconds (i.e., 4 hours)

Weighting of backup group after VRRP Plus is enabled	100
Upper threshold of the weighting of backup group after VRRP Plus is enabled	100
Lower threshold of the weighting of backup group after VRRP Plus is enabled	1
Forwarder preemption in backup group after VRRP Plus is enabled	Enabled
Weighting tracking object of backup group after VRRP Plus is enabled	Not configured
Penalty of weighting tracking object of backup group after VRRP Plus is enabled	10 by default after tracking object is configured

2.4.3 Enable VRRP Plus

You can only enable VRRP Plus after configuring VRRP function on the Ethernet interface. The configurations steps of VRRP Plus are:

Command	**Function**
DES-7200(config)# **interface** *type number*	Enter interface configuration mode
DES-7200(config-if)# **vrrp** *group* **ip** *address*	Configure a VRRP group
DES-7200(config-if)# **vrrp** *group* **balance**	Enable VRRP Plus on the IPv4 VRRP backup group with the specified group ID.

The VRRP Plus group ID of "group" shall range between 1-255 (same as VRRP).

2.4.4 Configure VRRP Plus Load Balancing Policy

VRRP Plus currently supports three kinds of load balancing policies: 1) uses different virtual MAC addresses to reply to ARP requests from different hosts; 2) use different virtual MAC addresses in turn to reply to ARP requests; 3) reply according to the weighting value of the device in the backup group.

Command	**Function**

DES-7200(config-if)# **vrrp** *group* **load-balancing** { **host-dependent	round-robin**	**weighted**}	Configure VRRP Plus load balancing policy: host-dependent refers host-based balancing; round-robin refers to round-robin based balancing; weighted refers to backup group weighting based balancing.
DES-7200(config-if)# **no vrrp** *group* **load-balancing** { **host-dependent	round-robin**	**weighted**}	Restore to default VRRP Plus load balancing policy.

The default load balancing policy is round-robin.

2.4.5 Configure the Redirect Timer and Timeout Timer for the Proxy Virtual MAC Address of VRRP Plus Backup Group

VRRP Plus supports the configuration of redirect and timeout timers of the backup group. When the device fails, the backup group will assign the virtual MAC address to other device for proxy forwarding. Within the redirect time, the backup group will continue to reply to ARP requests with this virtual MAC address; after the redirect timer runs out, it will no longer reply with this virtual MAC address. Upon expiration of the timeout timer, the backup group will delete this virtual MAC address.

Command	Function
DES-7200(config-if)# vrrp group timers redirect redirect timeout	Configure the redirect timer and timeout timer for the proxy virtual MAC address of VRRP Plus backup group.
DES-7200(config-if)# no vrrp group timers redirect	Restore to the default redirect time and timeout time of VRRP Plus backup group (you can input the specific time, but the value will not be matched).

redirect: Redirect time; default value is 300 seconds (5 minutes), selecting between 0 and 3600;

timeout: Timeout time; default value is 14400 seconds (4 hours), selecting between (redirect + 600) and 64800.

2.4.6 Configure Weighting and Threshold for VRRP Plus Backup Group

By configuring different weights for difference devices, those with larger weights will share more traffic and those with smaller weights will share less traffic, so that the forwarding capacity of difference devices can be fully utilized. When the weighting value of BVF device in the backup group is below the lower threshold, it will automatically quit the forwarding role. When the weighting value recovers and is beyond the upper threshold, it will automatically resume the forwarding role.

Command	Function
DES-7200(config-if)# vrrp group weighting maximum [lower lower] [upper upper]	Configure weighting and upper/lower threshold for VRRP Plus backup group
DES-7200(config-if)# no vrrp group weighting	Restore to the default weighting value of VRRP Plus backup group (you can input complete commands, but the value will not be matched).

Maximum: Weighting value; default value is 100, selecting between 1 and 255;

Lower: Lower threshold of weight; default value is 1, selecting between 1 and (maximum - 1);

Upper: Upper threshold of weight; default value is 100, selecting between lower and maximum.

2.4.7 Configure Forwarder Preemption for VRRP Plus Backup Group

VRRP Plus allows the configuration of forwarder preemption for the backup group. Configure higher weighting value for device with better forwarding capacity, so that when the device in listening mode has a weighting value higher than that of the existing forwarder, the listening device can preempt the role of such forwarder. In this way, device with better forwarding capacity will be responsible for packet forwarding and device with lower forwarding capacity will listen to the status of other devices.

Command	Function
DES-7200(config-if)# vrrp group forwarder preempt	Configure forwarder preemption for VRRP Plus backup group

DES-7200(config-if)# no vrrp group forwarder preempt	Disable forwarder preemption

Forwarder preemption is enabled by default.

2.4.8 Configure weighting tracking object for VRRP Plus backup group

Allowing dynamic adjustment of the weighting of backup group according to link detection status.

Command	Function
DES-7200(config-if)# vrrp group weighting track object-number [decrement value]	Configure weighting tracking object for VRRP Plus backup group
DES-7200(config-if)# no vrrp group weighting track object-number	Delete the corresponding tracking object

Tracking is not configured by default.

Object-number is the number of tracked object (selecting between 1 and 700). For details about track object configuration, you can refer to track function related documents, such as "TRACK-RNS-CREF.doc" and "TRACK-RNS-SCG.doc".

Value indicates the weighting value decreased when the tracked object is down (default: 10, selecting between 1 and 255).

2.5 VRRP Plus Monitoring and Maintenance

2.5.1 debug vrrp balance

Add the following debug switches for VRRP Plus module:

debug vrrp balance errors Monitor error messages

debug vrrp balance messages Monitor messages between VRRP and TRACK module

debug vrrp balance packets Monitor packets of VRRP Plus protocol

debug vrrp balance state Monitor the status of VRRP Plus group

debug vrrp balance timer Monitor the timer messages of VRRP Plus group

debug vrrp balance event Monitor the events of VRRP Plus group

debug vrrp balance Monitor all messages

2.5.2 show vrrp balance

Execute the following two commands to display the running status of VRRP Plus:

Command	Function
DES-7200# show vrrp balance [brief | group]	To display the status of VRRP Plus. Specify the group number and display the brief information.
DES-7200# show vrrp balance interface type number [brief]	Display VRRP Plus information on the specified interface. Parameter "brief" indicates brief information.

The followings are the examples of using these commands:

1. show vrrp balance [brief | *group*]

```
DES-7200# show vrrp balance brief
Interface     Grp   State     Group Addr      MAC addr
VLAN 1         1    BVG       192.168.1.1     0000.5e00.0101
DES-7200#show vrrp balance
VLAN 1 - Group 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
    Track object 1, state: down
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
    Owner ID is 00d0.f822.33ab
  Forwarder 2
    MAC address:
      001a.a916.0201
    Owner ID is 00d0.f822.8800
```

2. show vrrp balance interface *type number* [brief]

```
DES-7200# show vrrp balance interface vlan 1
VLAN 1 - Group 1
  State is BVG
  Virtual IP address is 192.168.1.54
  Hello time 1 sec, hold time 3 sec
  Load balancing: host-dependent
  Redirect time 300 sec, forwarder time-out 14400 sec
  Weighting 100 (configured 100), thresholds: lower 1, upper 100
    Track object 1, state: down
  There are 2 forwarders
  Forwarder 1 (local)
    MAC address:
      0000.5e00.0101
```

```
   Owner ID is 00d0.f822.33ab
 Forwarder 2
   MAC address:
     001a.a916.0201
   Owner ID is 00d0.f822.8800
```

2.6 Typical VRRP Plus Configuration Example

As shown in the typical topology illustrated Figure 1, two layer-3 devices are configured as follows:

Layer-3 device A:

```
 DES-7200(config)#track 1 interface FastEthernet 0/14 line-protocol
interface FastEthernet 0/0
no switchport
ip address 192.168.1.2 255.255.255.0
vrrp 1 ip 192.168.1.1
vrrp 1 balance
vrrp 1 load-balancing weighted
vrrp 1 weighting track 1 decrement 100
```

Layer-3 device B:

```
DES-7200(config)#track 1 interface FastEthernet 0/14 line-protocolinterface
FastEthernet 0/0
no switchport
ip address 192.168.1.3 255.255.255.0
vrrp 1 ip 192.168.1.1
vrrp 1 balance
vrrp 1 load-balancing weighted
vrrp 1 weighting track 1 decrement 100
```

3 BFD Configuration

3.1 Understanding BFD

3.1.1 BFD Overview

Bidirectional forwarding detection (BFD) provides low-overhead, short-duration detection of the connectivity in the forwarding path between adjacent routers. The fast detection of failures in the forwarding path speeds up enabling the backup forwarding path and improves the network performance.

3.1.2 BFD Packet Format

The two types of BFD packets are control packets and echo packets. The local end sends echo packets to the peer, which returns the received echo packets back without processing. Therefore, no BFD echo packet format is defined. Only BFD control packet format is defined. There are two versions for the BFD control packet: version 0 and version 1. By default, the BFD session establishment adopts the version 1. However, if one end receives the version 0 control packets from the peer, the default version 1 will automatically switch to version 0 to establish the BFD session. You can use the **show bfd neighbors** command to view the version member. The format of the version 1 packet is shown as follows:

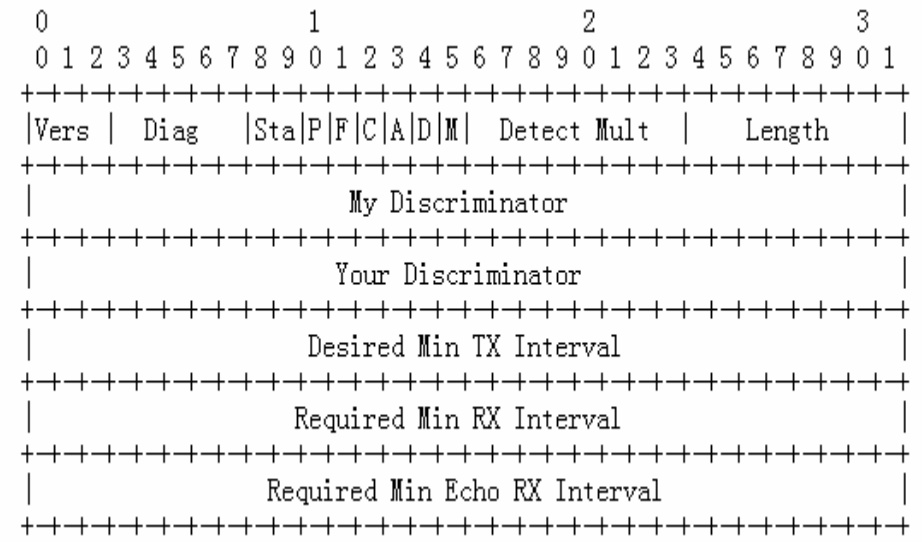


Figure-1 BFD Control Packet Format

- Vers: BFD version. The current version is 1.
- Diags: The reasons for the last transition of the local protocol from UP to some other state, including:

0—no diagnostic information

1—detection timeout of the control packets

2—echo failure

3—adjacency advertisement session is Down

4—reset the forwarding panel

5—channel failure

6—channel connection failure

7—AdminDown

- Sta: Current BFD session state. Its value can be 0 for AdminDown, 1 for Down, 2 for Init and 3 for Up.
- P: When the parameter changes, the sender offsets the Poll(P) bit in the BFD packet and the receiver must response to this packet immediately.
- F: It must be offset in the echo packet of responding the Poll(P) bit offset.
- C: The forwarding/control separation bit. Once it is offset, the change of control panel has no influence on the BFD detect. For example, BFD is able to go on detecting the link state if OSPF(the control panel) reloads/GR.
- A: Authentication identifier. Offset means the session needs to be verified. If it is set to 1, the control packet contains the authentication field and the session is authenticated.
- D: Inquiry demand. Offset means the sender expects to detect the links in the inquiry demand mode.
- M: Used in the one-to-multiple application and must be set to 0.
- Detect Mult: Detect the timeout multiplier, used to calculate the detection timeout time for the detector.
- Length: the packet length.
- My Discriminator: the local discriminator connecting the BFD session.
- Your Discriminator: the peer discriminator connecting the BFD session.

- Desired Min Tx Interval: the minimum BFD packets sending interval for the local protocol.
- Required Min Rx Interval: the minimum BFD packets receiving interval for the local protocol.
- Required Min Echo Rx Interval: the minimum Echo packets receiving interval for the local protocol (if the Echo function is not supported for the local protocol, set the value to 0)
- Auth Type: the authentication type(optional), including:
  - Simple Password
  - Keyed MD5
  - Meticulous Keyed MD5
  - Keyed SHA1
  - Meticulous Keyed SHA1
- Auth Length: the authentication data length
- Authentication Data: the authentication data field

Caution

Since v10.3(4b3), DES7200 supports the packet format in version 1 and version 0. By default, version 1 is used for the packet sending of BFD session. If the packets sent from the peer with version 1 are received, it will automatically switch to the version 0 to establish the session.

3.1.3 BFD Operation Mechanism

The BFD detection mechanism is independent from the applicated interface media type, the encapsulation format mad the associated upper-layer protocols such as OSPF、BGP、RIP. The BFD establishes a session between adjacent routers, enables the route protocols to re-calculate the route table by rapidly sending the detection fault to the running route protocols and decreases the network convergence time sharply. The BFD itself can not discover the neighbors, so it needs the upper-layer protocols to notify the neighbors of which the session is established.

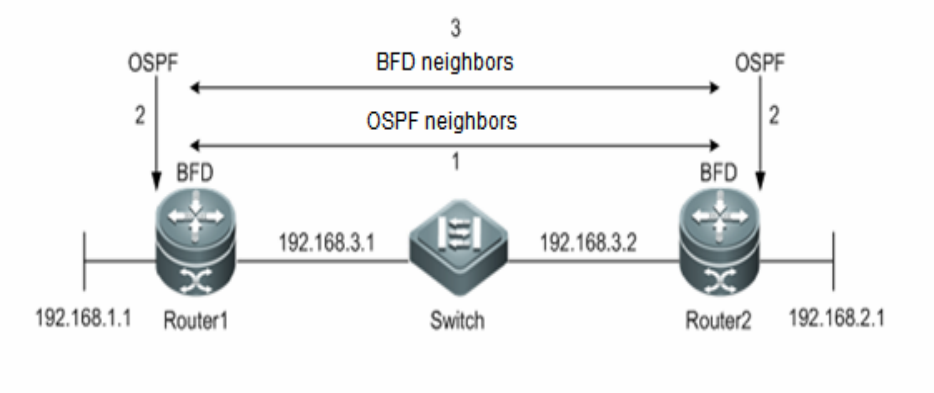


Figure-2 BFD Session Establishment

As the Figure-2 shows, two routers are connected via a L2 switch. OSPF and BFD are running in the two routers at the same time. The BFD session establishment process is:

Step 1: OSPF discovers neighbors and establish neighbor relationships.

Step 2: OSPF notifies BFD of establishing the session with the neighbors.

Step 3: BFD establishes the session with the neighbors.

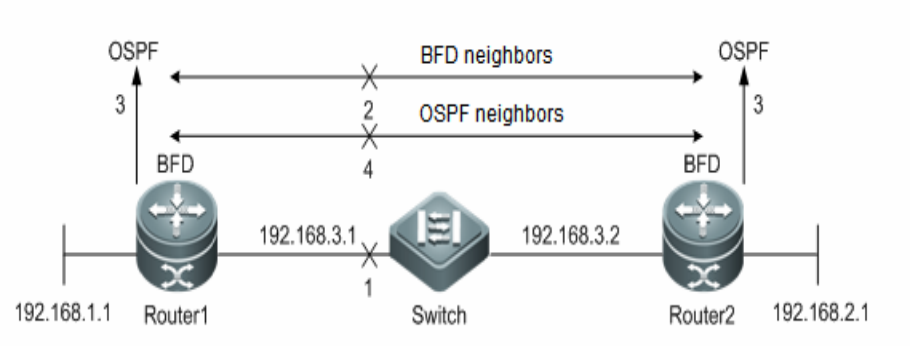


Figure-3 BFD Fault Detection Process

As the Figure-3 shows, the BFD fault detection process is:

Step 1: A link communication failure between Router1 and Router2 occurs.

Step 2: BFD session between the Router1 and Router2 detects the fault.

Step 3: BFD notifies the fault of the OSPF reachability to the forwarding path of the neighbor.

Step 4: OSPF deals with the process of the neighborDown. If the backup forwarding path exists and the convergence is about to happen, the backup forwarding path will be enabled.

3.1.4 Related Protocols and Regulations

The related BFD protocols and regulations are:

draft-ietf-bfd-base-09：Bidirectional Forwarding Detection

draft-ietf-bfd-generic-05：Generic Application of BFD

draft-ietf-bfd-mib-06 ： Bidirectional Forwarding Detection Management Information Base

draft-ietf-bfd-v4v6-1hop-09：BFD for IPv4 and IPv6 (Single Hop)

draft-ietf-bfd-multihop-07：BFD for IPv4 and IPv6 (Multihop)

draft-ietf-bfd-mpls-07：BFD For MPLS LSPs

The draft-ietf-bfd-mpls-07 is not supported in firmware v10.4(1), v10.3(4b3) and v10.3(5).

Caution The draft-ietf-bfd-mib-06 is not supported in all firmware versions.

3.2 BFD Features

This section describes the BFD features:

- Establish mode of the BFD Session
- BFD Detection Mode
- BFD Session Parameters
- BFD Authentication Method
- BFD for Dynamic Route Protocols
- BFD for Static Route
- BFD for PBR
- BFD for VRRP
- BFD for VRF
- Supported BFD Interfaces

3.2.1 BFD Session Establishment Mode

The BFD session is established in the following modes:

1. Active Mode: Before a session is established, BFD actively sends the BFD control packets regardless of whether any BFD control packet is received from the peer.
2. Passive Mode: Before a session is established, no BFD control packet is sent until a BFD control packet is received from the peer.

Caution

In firmware v10.4(1), v10.3(4b3) and v10.3(5), the passive mode is not supported and can not be configured.

3.2.2 BFD Detection Mode

The BFD detection modes are as follows:

- Asynchronous Mode

In the asynchronous mode, the BFD control packets are sent periodically among the systems. If one system receives no BFD control packet from the peer within the BFD interval, the BFD session will be down.

- Demand Mode

In the demand mode, suppose that every system has an independent method to confirm whether it has been connected to other systems, once a BFD session is established, the system stops sending the BFD control packets unless a system needs the connection verification. If the connection verification is necessary, the system will send a BFD control packet with the short sequence. If no returned packet is received within the detection interval, the BFD session will be down. If the echo packet is received from the peer, the forwarding path is normal.

- Echo Mode

The local system sends the BFD echo packet periodically. The peer system loops back the echo packet via the forwarding channel. The BFD session will be down if the continuous echo packets are not received within the detection interval. The echo mode can be co-used with the above-mentioned two detection modes. In the echo mode, the packets are forwarded back via the forwarding panel of the peer system rather than the control panel, reducing the delay and speeding up the fault detection in comparison to the control packet sending. In the asynchronous mode, the control packet sending will be decreased with the echo function enabled, for the echo function processes the detection. If the echo function is enabled in the demand mode, the control packet sending can be cancelled after the BFD session establishment. The echo function must be enabled in the BFD session, otherwise the echo function will be invalid.

1. The demand mode is not supported in firmware v10.4(1), v10.3(4b3) and v10.3(5).

Caution

2. The **no ip redirects** command must be executed to disable the redirect function of the IP packets and the **no ip deny land** command must be executed to disable the function of anti-attack of the Land-based DDOS before configuring the echo mode. The BFD echo function works on the condition that the version of the BFD control packet is version 1.

3.2.3 BFD Session Parameter

The BFD session parameters(for example, Desired Min Tx Interval, Required Min Rx Interval, Detect Mult, ect) can be modified after the BFD session is established. The modified BFD session will renegotiate and use the newest parameter value to detect the session. During the modification, the session keeps in the UP state.

3.2.4 BFD Authentication Method

The BFD authentication methods include:

1. Simple Password
2. Keyed MD5
3. Meticulous Keyed MD5
4. Keyed SHA1
5. Meticulous Keyed SHA1

Caution

The BFD authentication is not supported in firmware v10.4(1), v10.3(4b3) and v10.3(5).

3.2.5 BFD for Dynamic Route Protocols

Configuring BFD for the route protocols improves the convergence performance of the protocol by taking advantages of the faster fault detection of the BFD in comparison to the HELLO mechanism of the protocol. Generally, the fault detection time can be decreased to less than 1s. Firmware v10.4(1), v10.3(4b3) and v10.3(5) support the following route protocols:

1. RIPv1、RIPV2
2. OSPFv2
3. BGP

Firmware v10.4(3) and later also support the OSPFv3 route protocol. Make sure that the BFD for corresponding protocol is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for this protocol will be established automatically.

3.2.6 BFD for Static Route

Configuring BFD for static route prevents the static route from being the forwarding path when the router selects the routing under the circumstances that the configured static route is unreachable. It can rapidly switch to the backup forwarding path if the backup forwarding path exists.

Being different from the dynamic route protocol, the static route protocol has no mechanism of discovering the neighbor. Therefore, when configuring the BFD for static route, the reachability of the next-hop of the static route is dependent on the BFD session state. If the BFD session detects the fault, which means that next-hop of the static route is unreachable, the static route can not be installed into the RIB. Make sure that the BFD for static route is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for static route will be enabled automatically.

If the BFD session is removed from the peer in the process of the BFD session establishment, the BFD session will be down. And under this circumstance, the static route forwarding shall be ensured.

3.2.7 BFD for PBR

Configuring BFD for PBR prevents the PBR from being the forwarding path when the router selects the routing under the circumstances that the configured PBR is unreachable. It can rapidly switch to the backup forwarding path if the backup forwarding path exists.

The method of BFD for PBR is similar to the BFD for static route. If the BFD session detects the fault by following the forwarding path of the specified neighbor, the PBR will be notified of the unreachability to the corresponding next-hop. The PBR reaching the next-hop is ineffective.

Make sure that the BFD for PBR is enabled on all BFD session neighbors, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for PBR will be enabled automatically.

If the BFD session is removed from the peer in the process of the BFD session establishment, the BFD session will be down. And under this circumstance, the PBR forwarding shall be ensured.

Only firmware v10.4(1), v10.3(4b3) and v10.3(5) support the BFD for IPv4 PBR.

Caution Firmware v10.4(3) and later support the BFD for IPv6 PBR.

3.2.8 BFD for VRRP

BFD for VRRP configuration can replace the HELLO mechanism of VRRP itself to realize the fast detection of running state of the master and backup routers and improve the network performance. Generally, the time of failure detection can be shortened to less than 1s.

Make sure that the BFD for VRRP is enabled on the router at both ends, or the BFD session cannot be established. However, if the dynamic route protocol or other applications have already notify the BFD of establishing the session with the corresponding neighbor, the BFD for VRRP will also be configured.

VRRP can also use BFD to follow the specified neighbor. If the BFD session detects the fault of the forwarding path to the neighbor, it will reduce the VRRP priority automatically and trigger the switchover between the master and backup routers. The BFD can be established only when the dynamic route protocol or other applications notify BFD of establishing the session with corresponding neighbor.

3.2.9 BFD for VRRP+

BFD for VRRP+ can replace the BVF detection by BVG of VRRP+, allowing quick detection of BVF operating state and accelerating the switchover of forwarding entity during failure. Under general circumstances, the fault detection time can be shortened to less than 1 second.

Since VRRP+ is based on VRRP protocol, no extra configuration will be needed during its association with BFD. You only need to make sure VRRP has been enabled on the devices at both ends and BFD session has been correctly associated.

Caution

BFD for VRRP+ is supported in release firmware v10.4(3).

3.2.10 BFD supports to change the State of Layer3 Interfaces

BFD supports to change the state of layer-3 interface. In configuration mode, execute "bfd bind peer-ip" to detect the directly connected address of the specified layer-3 interface. The BFD session state established by this CLI command will generate the BFD state of the corresponding interface, such as BFD-DOWN/BFD-UP. In various types of FRR, BFD is used to detect interface state and perform fast FRR switchover.

Caution

Association between BFD and layer-3 interface is supported in release firmware v10.4(3).

3.2.11 BFD for MPLS-LSP

BFD for MPLS mainly refers to the case that LSP (Label Switched Path) uses BFD to carry out quick neighbor detection. The detection modes supported include:

1. Configure BFD for detecting static LSP;
2. Configure BFD for detecting the LSP generated by LDP;
3. Configure BFD for detecting backward LSP with IP

Caution

BFD for MPLS-LSP is supported in release firmware v10.4(3).

3.2.12 BFD for VRF

The BFD supports VPN Routing and Forwarding(VRF) and detects the connectivity of the forwarding path between the Provider Edge(PE) and the Customer Edge(CE).

3.2.13 Supported BFD Interfaces

For the switches, it is allowed to configure the BFD on the Routed Port and SVI only, excluding the L3 AP port. Besides, it fails to set the BFD session on the SVI L2AP member port.

For the routers, it is allowed to configure the BFD on the synchronous port, the asynchronous port, ATM, the serial port, the frame relay, POS, CPOS, the dialed port, Ethernet port and its sub-port, E1, channelized ATM, channelized CPOS, MPPP interface.

3.3 Configuring BFD

This section describes how to configure the BFD features:

- Configuring the BFD session parameters (Mandatory)
- Configuring the BFD Echo function (Optional)
- Configuring the BFD UP-Dampening Time (Optional)
- Configuring the BFD protection policy (Optional)
- Configuring the BFD for RIP (Mandatory)
- Configuring the BFD for OSPF (Mandatory)
- Configuring the BFD for BGP (Mandatory)
- Configuring the BFD for the static route (Mandatory)
- Configuring the BFD for the PBR (Mandatory)
- Configuring the BFD for the VRRP (Mandatory)

3.3.1 Default Configurations

Function	Defaults
BFD session creation mode	Active mode, can not be set.
BFD detection mode	Asynchronous mode, the echo function is enabled by default.
BFD session parameter	No default value, must be set.
BFD authentication method	Disabled, can not be set.
BFD for dynamic route protocol	Disabled
BFD for static route	Disabled
BFD for PBR	Disabled
BFD for VRRP	Disabled
BFD for VRF	Disabled

3.3.2 Configuring the BFD Session Parameter

The BFD session parameter has no default value and must be configured. The following are the configuration steps:

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *type number*	Enter the interface configuration mode.
DES-7200(config-if)#bfd interval milliseconds min_rx milliseconds multiplier interval-multiplier	Configure the BFD parameters on the specified interface. Interval milliseconds: configure the minimum sending interval, in millisecond; min_rx milliseconds: configure the minimum receiving interval, in millisecond; multiplier interval-multiplier: configure the detection timeout multiplier.
DES-7200(config-if)# **end**	Exit the interface configuration mode and return to the privileged mode.

Use the **no bfd interval** command in the interface configuration mode to remove the BFD session parameter configurations.

The following example shows how to configure the BFD session parameter on the Routed Port FastEthernet 0/2:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface fastEthernet 0/2
DES-7200(config-if)# bfd interval 100 min_rx 100 multiplier 3
```

Caution

The difference of the bandwidth transmitted on different interfaces should be considered when configuring the parameters. If the minimum sending and receiving intervals are too low, it may result in the oversized bandwidth of the BFD and the influence of the data transmission.

It is not allowed to configure the BFD session parameter on the L3 AP port.

3.3.3 Configuring the BFD Echo Function

By default, the BFD echo function is enabled. Enabling the echo function does not influence the established session state. With the echo function disabled, the echo packets will not be sent, and not be received on the forwarding panel.

Follow the following steps to configure the BFD echo function:

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *type number*	Enter the interface configuration mode.
DES-7200(config-if)#bfd echo	Enable the echo function.
DES-7200(config-if)# **end**	Exit the interface configuration mode and return to the privileged mode.

Use the **no bfd echo** command in the interface configuration mode to disable the BFD echo function.

The following example shows how to configure the BFD echo function on the Routed Port FastEthernet 0/2:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface fastEthernet 0/2
DES-7200(config-if)# bfd echo
```

After enabling the echo function in the BFD asynchronous mode, the slower frequency can be adopted to send the BFD control packets.

Follow the following steps to configure this parameter:

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **bfd slow-timer [***milliseconds***]**	Configure the time of the slow-timer, in milliseconds, ranging from 1000 to 30000. The default value is 1000.
DES-7200(config-if)# **end**	Exit the global configuration mode.

Use the **no bfd slow-timer** command in the global configuration mode to restore it to the default value.

The following example shows how to configure the time of the slow-timer to 1400 milliseconds:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# bfd slow-timer 1400
```

Caution

The local end sends the BFD echo packet to the peer, which returns the received packets with processing on the forwarding panel. In this process, the BFD session detection may fail for the peer has been congested resulting in the loss of the echo packets. Under these circumstances, the corresponding QoS policy is necessary to be configured to make sure that the echo packets take the precedence to be processed or the echo function is disabled.

3.3.4 Configuring the BFD UP-Dampening Time

The BFD up-dampening time configuration solves the problem that due to the line instability, BFD session state frequent switchover between DOWN and UP occurs, which results in the frequent forwarding path switchover of the associated application(for example, the static route) and the abnormal operation.

Follow the following steps to configure the BFD up-dampening time:

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *type number*	Enter the interface configuration mode.
DES-7200(config-if)#bfd up-dampening milliseconds	Configure the up-dampening time.
DES-7200(config-if)# **end**	Exit the interface configuration mode and return to the privileged mode.

Use the **no bfd up-dampening** command in the interface configuration mode to restore to the default value.

The following example shows how to configure the BFD up-dampening time as 60,000ms:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface fastEthernet 0/2
DES-7200(config-if)# bfd up-dampening 60000
```

3.3.5 Configuring the BFD Protection Policy

BFD protocol is so sensitive that if the device with BFD function enabled suffers from attack (for example, a large amount of Ping packets attack the device), which lead to the BFD session turbulence, the device can be protected by enabling the BFD protection policy. However, if the BFD function and the BFD protection policy are enabled at the same time, the loss of BFD packets on the attacked device occurs when the packets sent from the last-hop device go through this device, influencing the BFD session establishment between the last-hop device and other devices. This function is valid only for the switches.

Follow the following steps to configure the BFD protection policy:

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **bfd cpp**	Enable the BFD protection policy.
DES-7200(config)# **end**	Exit the global configuration mode.

By default, the BFD CPP is enabled. Use the **no bfd cpp** command in the global configuration mode to disable the BFD CPP.

The following example shows how to enable the BFD CPP:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# bfd cpp
```

3.3.6 Configuring the BFD for RIP

RIP sends the route updating information periodically. A route is invalid and RIP cannot rapidly respond to the link failure when no route updating information is received within the specified time.

After enabling the BFD for RIP, the BFD session will be established for the RIP route information source(the source address for RIP route updating packet). Once BFD detects that a neighbor is invalid, RIP route information will directly be in the invalid state and not join in the route forwarding no longer. The

convergence time can be decreased from 180s(the default RIP timer) to less than 1s.

Use the **bfd all-interfaces** command to configure the BFD for RIP on all interfaces. Or use the **ip rip bfd [disable]** command in the interface configuration mode to enable or disable the BFD for RIP on the specified interface.

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router rip**	Enter the Router configuration mode.
DES-7200(config-router)# **bfd all-interfaces**	Enable the BFD for RIP on all interfaces.
DES-7200(config-router)# **exit**	(Optional) Exit the Router configuration mode and return to the global configuration mode.
DES-7200(config)# **interface** *type number*	(Optional) Enter the interface configuration mode.
DES-7200(config-if)# **ip rip bfd [disable]**	(Optional) Enable or disable the BFD for RIP on a specified interface.
DES-7200(config-if)# **end**	(Optional) Exit to the privileged mode.
DES-7200# **show bfd neighbor [details]**	(Optional) Show the information of the BFD session establishment and whether RIP is associated to the specified session.

Use the **no bfd all-interfaces** command in the Router configuration mode to disable the BFD for RIP on all interfaces.

The following example shows how to enable the BFD for RIP on all interfaces excluding the FastEthernet 0/2:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# router rip
DES-7200(config-router)# bfd all-interfaces
DES-7200(config-router)# exit
DES-7200(config)# interface FastEthernet 0/2
DES-7200(config-if)# ip rip bfd disable
DES-7200(config-if)#end
```

When configuring BFD for IPv4 PBR, the route information source (source address for RIP route updating packet) of two devices with RIP enabled shall be in the same network segment to establish the BFD session between adjacent routers.

Before enabling BFD for IPv4 PBR, the BFD session parameter must be configured, or it is ineffective.

Caution

For the non-unnumbered interface, if the neighbor end and the local end are not connected directly, the BFD for IPv4 PBR fails to be enabled.

The BFD session cannot be established if the specified interface and the actual outbound interface for the BFD packets are inconsistent because of the IP routing.

The BFD session cannot be established if the specified interface and the actual incoming interface for the BFD packets are inconsistent.

3.3.7 Configuring the BFD for OSPF

OSPF protocol dynamically discovers the neighbors by the Hello packets. With BFD for OSPF configured, the BFD session for the neighbors in FULL relationship will be established and the neighbor state will be detected by the BFD mechanism. Once BFD neighbor is invalid, OSPF processes the network convergence. The convergence time could be from 120s(by default, the sending interval of the OSPF Hello packet in non-broadcast network is 30s, which is a quarter of the invalid time for the adjacency router, namely, 120s) to less than 1s.

Use the **bfd all-interfaces** command to configure the BFD for OSPF on all interfaces. Or use the **ip rip bfd [disable]** command in the interface configuration mode to enable or disable the BFD for OSPF on the specified interface.

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router ospf** *process-id*	Enter the Router configuration mode.
DES-7200(config-router)# **bfd all-interfaces**	Enable the BFD for OSPF on all interfaces.

Command	Function
DES-7200(config-router)# **exit**	(Optional) Exit the Router configuration mode and return to the global configuration mode.
DES-7200(config)# **interface** *type number*	(Optional) Enter the interface configuration mode.
DES-7200(config-if)# **ip rip bfd [disable]**	(Optional) Enable or disable the BFD for OSPF on a specified interface.
DES-7200(config-if)# **end**	(Optional) Exit to the privileged mode.
DES-7200# **show bfd neighbor [details]**	(Optional) Show the information of the BFD session establishment and whether OSPF is associated to the specified session.
DES-7200# **show ip ospf**	(Optional) Verify whether OSPF is associated to the specified session.

Use the **no bfd all-interfaces** command in the Router configuration mode to disable the BFD for OSPF on all interfaces.

The following example shows how to enable the BFD for OSPF on all interfaces excluding the FastEthernet 0/2:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# router ospf 123
DES-7200(config-router)# bfd all-interfaces
DES-7200(config-router)# exit
DES-7200(config)# interface FastEthernet 0/2
DES-7200(config-if)# ip rip bfd disable
DES-7200(config-if)#end
```

Caution

The BFD for OSPFv3 is not supported in firmware v10.4(1) and v10.3(4b3).

Before enabling BFD for OSPF, the BFD session parameter must be configured, or it is ineffective.

The BFD session cannot be established if the specified interface and the actual outbound interface for the BFD packets are inconsistent because of the IP routing.

The BFD session cannot be established if the specified interface and the actual incoming interface for the BFD packets are inconsistent.

BFD monitoring is not supported in the virtual link of OSPFv2/OSPFv3.

3.3.8 Configuring the BFD for BGP

Being similar to OSPF, by configuring the BFD for BGP, BGP protocol rapidly detects the faults, realizes the rapid detection of the neighbor relationship and fastens the protocol convergence. By default, the BGP keepalive interval is 60s and the holdtime is 180s. The minimum value of the keepalive interval and holdtime are 1s and 3s respectively. It is slow to detect the neighbor relationship. A large amount of the packets will be lost on the interface that receives and sends the packets at the fast speed.

Use the **neighbor** *ip-address* **fall-over bfd** command to enable the BFD for BGP.

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **router bgp** *as-tag*	Enter the Router configuration mode.
DES-7200(config-router)# **neighbor** *ip-address* **fall-over bfd**	Configure the BFD for BGP to detect the fault of the specific neighbor.
DES-7200(config-router)# **end**	(Optional) Exit to the privileged mode.
DES-7200# **show bfd neighbor [details]**	(Optional) Show the information of the BFD session establishment and whether BGP is associated to the specified session.
DES-7200# **show ip bgp neighbors**	(Optional) Verify whether BGP is associated to the specified session.

Use the **no neighbor** *ip-address* **fall-over bfd** command in the Router configuration mode to disable the BFD for BGP.

The following example shows how to enable the BFD for BGP, and detect the forwarding path with the neighbor 172.16.0.2:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface FastEthernet 0/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.16.0.1 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if)# exit
DES-7200(config)# router bgp 44000
DES-7200(config-router)# bgp log-neighbors-changes
DES-7200(config-router)# neighbor 172.16.0.2 remote-as 45000
```

```
DES-7200(config-router)# neighbor 172.16.0.2 fall-over bfd
DES-7200(config-router)# end
```

Caution

Only the BFD for IPv4 BGP is suppoted in firmware v10.4(1), v10.3(4b3) and v10.3(5).

If BGP establishes the session using the loopback address and enables BFD to detect the neighbors, the outbound interface for the BFD packets will be specified according to the result of IP routing. In this situation, before configuring the BFD for BGP, the **bfd interval** command is necessary to be used to configure the BFD session parameter on the possible outbound interface, or it may fail to establish the session.

The BFD session cannot be established if the specified interface and the actual incoming interface for the BFD packets are inconsistent.

3.3.9 Configuring the BFD for Static Route

Execute the following steps to configure the BFD for static route.

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **ip route static bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway* [**souce** *ip-addess*]	Configure the session neighbors of the BFD for static route. *interface-type interface-number:* the neighbor interface; *gateway:* the IP address for the neighbor ; In the circumstances of multi-hopping, use the source ip-address command to configure the source IP address for the session. Make sure that the BFD session parameter for the interface has been configured before configuration. For details, see *Configuring the BFD Session Parameter*.

Command	Function
DES-7200(config)# [**ip|ipv6**] **route** *prefix mask* {*ip-address* | *interface-type interface-number* *[ip-address*]}	Configure the static route. In order to ensure the BFD for static route configuration, the input parameters of *interface-type interface-number* and *ip-address* and the ones configured in step3 must be consistent.
DES-7200(config)# **end**	(Optional) Exit to the privileged mode.
DES-7200# **show bfd neighbor [details]**	(Optional) Show the information of the BFD session establishment and whether the static route is associated to the specified session.

Use the **no ip route static bfd [vrf** *vrf-name***]** *interface-type interface-number gateway* command in the interface configuration mode to disable the BFD for static route.

The following example shows how to enable the BFD for static route, and detect the forwarding path with the neighbor 172.16.0.2:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface FastEthernet 0/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.16.0.1 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if)# ip route static bfd FastEthernet 0/1 172.16.0.2
DES-7200(config-if)# ip route 10.0.0.0 255.0.0.0 FastEthernet 0/1 172.16.0.2
DES-7200(config-if)# end
```

3.3.10 Configuring the BFD for PBR

Execute the following steps to configure the BFD for PBR.

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# route-map route-map-name [permit | deny] sequence	Define the route map and enter the route-map configuration mode.
DES-7200(config-route-map)#match ip address access-list-number	Configure the matched access list.

Command	Function
DES-7200(config-route-map)#set ip next-hop verify-availability [next-hop-address [track number|bfd [vrf vrf-name] interface-type interface-number gateway]]	Configure the session neighbor of the BFD for PBR. interface-type interface-number: the neighbor interface; gateway: the IP address for the neighbor ; Make sure that the BFD session parameter for the interface has been configured before configuration. For details, see Configuring the BFD Session Parameter. If the BFD session faults are detected, the next-hop specified by the next-hop-address is unreachable. Use the no form of this command to remove the configuration.
DES-7200(config-route-map)#exit	Exit the route-map configuration mode.
DES-7200(config)# interface type number	Enter the interface configuration mode.
DES-7200(config-if)#ip policy route-map route-ma	Configure the BFD for the PBR.
DES-7200(config)-if# end	(Optional) Exit to the privileged mode.
DES-7200# show bfd neighbor [details]	(Optional) Show the information of the BFD session establishment and whether PBR is associated to the specified session.
DES-7200#show route-map	(Optional) Verify whether PBR is associated to the specified session.

Use the **no set ip next-hop verify-availability** [*next-hop-address* [**track** *number*|**bfd** [**vrf** *vrf-name*] *interface-type interface-number gateway*]] command in the route-map configuration mode to disable the BFD for PBR.

The following example shows how to enable the BFD for PBR, and detect the forwarding path with the neighbor 172.16.0.2:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# route-map Example1 permit 10
DES-7200(config-route-map)# match ip address 1
DES-7200(config-route-map)# set ip precedence priority
DES-7200(config-route-map)#set ip next-hop verify-availability 172.16.0.2
bfd FastEthernet 0/1 172.16.0.2
DES-7200(config-route-map)#exit
```

```
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 172.16.0.1 255.255.255.0
DES-7200(config-if)#bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if)#ip policy route-map Example1
DES-7200(config-if)#exit
```

Caution The BFD for PBRv6 is not supported in firmware v10.4(1), v10.3(4b3) and v10.3(5).

3.3.11 Configuring the BFD for VRRP

Execute the following steps to configure the BFD for VRRP to detect the master and slave routers.

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *type number*	Enter the interface configuration mode.
DES-7200(config-if)#**vrrp** *group-number* **ip** [*ip-address*[**secondary**]]	Create the VRRP group and virtual Ip address on the specified interface.
DES-7200(config-if)# **vrrp** *group-number* **bfd** *ip-address*	Configure the BFD for VRRP. *ip-address:* the IP address for the specified neighbor.
DES-7200(config)-if# **end**	(Optional) Exit to the privileged mode.
DES-7200# **show bfd neighbor [details]**	(Optional) Show the information of the BFD session establishment and whether VRRP is associated to the specified session.
DES-7200#**show vrrp**	(Optional) Verify whether VRRP is associated to the specified session.

Use the **no vrrp** *group-number* **bfd** command in the interface configuration mode to disable the BFD for VRRP and the application of the master and slave router detection.

The following example shows how to enable the BFD for VRRP, and detect the forwarding path between the master and slave routers:

```
DES-7200# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface FastEthernet 0/1
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.201.11 255.255.255.0
DES-7200(config-if)#bfd interval 50 min_rx 50 multiplier 3
DES-7200(config-if)#vrrp 1 priority 120
DES-7200(config-if)#vrrp 1 ip 192.168.201.1
DES-7200(config-if)#vrrp 1 bfd 192.168.201.12
DES-7200(config-if)#end
```

Execute the following steps to configure the BFD for VRRP to follow the specified neighbor IP.

Command	Function
DES-7200>**enable**	Enter the privileged mode.
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *type number*	Enter the interface configuration mode.
DES-7200(config-if)#**vrrp** *group-number* **ip** [*ip-address*[**secondary**]]	Create the VRRP group and virtual Ip address on the specified interface.
DES-7200(config-if)# **vrrp** *group-number* **track bfd** *interface-type interface-number ip-addess* [*priority*]	Specify the VRRP group to follow the neighbor IP address of the specified interface. Use the **no** form of this command to remove this configuration.
DES-7200(config)-if# **end**	(Optional) Exit to the privileged mode.
DES-7200# **show bfd neighbor [details]**	(Optional) Show the information of the BFD session establishment and whether VRRP is associated to the specified session.
DES-7200#**show vrrp**	(Optional) Verify whether VRRP is associated to the specified session and follows the specified neighbor IP.

Use the no **vrrp** *group-number* **track bfd** *interface-type interface-number ip-addess* command in the interface configuration mode to disable the BFD for VRRP and the application of following the specified neighbor IP.

The following example shows how to specify the VRRP to follow the specified neighbor 192.168.1.3:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)#interface FastEthernet 0/1
```

```
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)#bfd interval 50 min_rx 50 multiplier 3
DES-7200(config)#interface FastEthernet 0/2
DES-7200(config-if)#no switchport
DES-7200(config-if)#ip address 192.168.201.17 255.255.255.0
DES-7200(config-if)#vrrp 1 priority 120
DES-7200(config-if)#vrrp 1 ip 192.168.201.1
DES-7200(config-if)#vrrp 1 track bfd FastEthernet 0/1 192.168.1.3 30
DES-7200(config-if)#end
```

3.3.12 Configuring the BFD for VRRP+

Since VRRP+ relies on VRRP, after configuring BFD for VRRP, VRRP+ will automatically associate with BFD.

3.3.13 Configuring BFD to Support Changing the State of Layer 3 Interfaces

Generally, it will take a long time for link communication failure or link failure to change the interface state. For various FRRs relying on interface state, high-performance switchover cannot be achieved. Therefore, BFD is generally associated with the layer-3 interface state to realize fast detection of interface state. Execute the following configurations to associate BFD and layer 3 interface states.

Command	Function
DES-7200>**enable**	Enter privileged mode
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200(config)# **interface** *type number*	Enter a specific layer-3 interface
DES-7200(config-if)# **bfd bind peer-ip** *ip-address* **[source-ip** *ip-adress***] process-pst**	Configure the neighbor detected by BFD Source-IP is used to specify the source IP of BFD packets to prevent such packets from being discarded due to the failure of uRPF check while uRPF is enabled at the same time. Process-pst refers to the BFD state of the interface generating BFD session.
DES-7200(config-if)#**end**	(Optional) Exit privilege mode

Command	Function
DES-7200#**show bfd neighbors** [**details**]	(Optional) Display the information about BFD session establishment and whether the interface has been associated to the relevant session.

To disable BFD on the interface, execute "**no bfd bind peer-ip ip-address**" in the configuration mode.

Configuration example:

Configure to enable BFD on interface FastEthernet 0/2

```
DES-7200#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface FastEthernet 0/2
DES-7200(config-if)#no sw
DES-7200(config-if)#ip address 1.1.1.1 255.255.255.0
DES-7200(config-if)#bfd bind peer-ip 1.1.1.2 source-ip 1.1.1.1 process-pst
DES-7200(config-if)#end
```

3.3.14 Configuring BFD For MPLS

BFD for MPLS mainly uses BFD to quickly detect the LSPs on MPLS network in order to enhance the reliability of MPLS network.

3.3.14.1 Configuring BFD for Detecting Static LSP

Command	Function
DES-7200>**enable**	Enter privileged mode
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200#**mpls router ldp**	Enter LDP configuration mode
DES-7200(config)# **bfd bind static-lsp peer-ip** *ip-address* **nexthop** *ip-address* **interface** *type number* **local-discriminator** *number* r**emote-discriminator** *number* **process-state**	Configure BFD for detecting static LSP and handle BFD session state. You can configure the peer IP address, the next-hop address and the egress interface of LSP. If no local discriminator is configured, the system will automatically select the local discriminator. If no remote discriminator is configured, the system will use auto-configuration to learn the remote discriminator.

3.3.14.2 Configuring BFD for Detecting Dynamic LSP

Command	Function
DES-7200>**enable**	Enter privileged mode
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200#**mpls router ldp**	Enter LDP configuration mode
DES-7200(config-mpls-router)# **bfd bind ldp-lsp peer-ip** *ip-address* **nexthop** *ip-address* **interface** *type number* **local-discriminator** *number* **remote-discriminator** *number* process-state	Configure BFD for detecting dynamic LSP and handle BFD session state. You can configure the peer IP address, the next-hop address and the egress interface of LSP. If no local discriminator is configured, the system will automatically select the local discriminator. If no remote discriminator is configured, the system will use auto-configuration to learn the remote discriminator.

3.3.14.3 Configuring BFD for Detecting Backward LSP with IP

Command	Function
DES-7200>**enable**	Enter privileged mode
DES-7200# **configure terminal**	Enter global configuration mode
DES-7200#**mpls router ldp**	Enter LDP configuration mode
DES-7200(config-mpls-router)# **bfd bind backward-lsp-with-ip peer-ip** *ip-address* **interface** *type number* **source-ip** ***ip-address*** **local-discriminator** *number* **remote-discriminator** *number*	Configure BFD for detecting backward LSP with IP. You can configure the source IP address, peer IP address and the egress interface of LSP. The local discriminator and remote discriminator must be configured manually.

To learn more details about BFD for MPLS-LSP and the command reference, please refer to the documents named "MPLD-CERF" and "MPLS-SCG".

3.3.15 Displaying BFD Configuration and State

BFD offers the following displaying commands to view various configurations and running information. The functions of each command are explained as follows:

Command	Function
show bfd neighbors [vrf vrf-name] [ipv4 ip-addess [details]] ipv6 ipv6-addess [details] |client {bgp|ospf|rip|vrrp|static-route|pbr} [ipv4 ip-addess [details] | ipv6 ipv6-addess [details]] details]]	Show the BFD session information. For details, see the field description in Table-1.
show vrrp	Show the configuration of BFD for VRRP.
show route-map	Show the configuration of BFD for PBR.
show ip static route	Show the configuration of BFD for static route.
show ip bgp neighbors	Show the configuration of BFD for BGP.
show ip ospf	Show the configuration of BFD for OSPF.
show ip rip database	Show the configuration of BFD for RIP.

Caution The displaying commands above can be configured in any configuration mode except for the user mode.

3.4 Configuration Examples

3.4.1 Example of Configuring BFD for RIP

3.4.1.1 Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the RIP protocol and enable the BFD for RIP on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the RIP of the failure, triggering the rapid convergence.

3.4.1.2 Network Topology

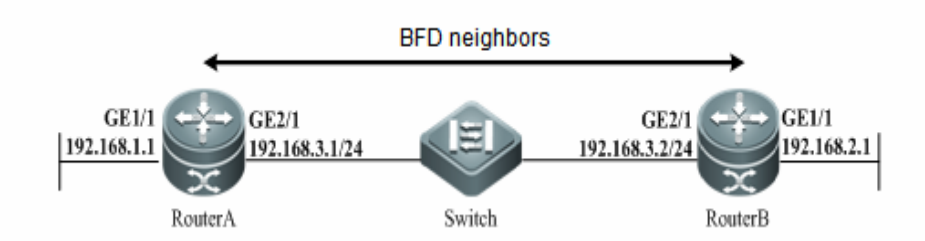


Figure-4 Topology of Configuring BFD for RIP

3.4.1.3 Configuration Steps

1) RouterA Configuration

Configure the Routed Port gi 2/1, the IP address, the BFD session parameter for Router A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Configure the Routed Port *gi1/1*:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
```

Enable RIP and configure the BFD for RIP to detect the neighbor 192.168.3.2:

```
DES-7200(config-if)# exit
DES-7200(config)# router rip
DES-7200(config-router)# version 2
DES-7200(config-router)# network 192.168.3.0
DES-7200(config-router)# network 192.168.1.0
DES-7200(config-router)# passive-interface GigabitEthernet 2/1
DES-7200(config-router)# bfd all-interfaces
```

2) RouterB Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router B:

```
DES-7200# configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 5
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
```

Enable RIP and configure the BFD for RIP to detect the neighbor 192.168.3.1:

```
DES-7200(config-if)# exit
DES-7200(config)# router rip
DES-7200(config-router)# version 2
DES-7200(config-router)# network 192.168.3.0
DES-7200(config-router)# network 192.168.2.0
DES-7200(config-router)# passive-interface GigabitEthernet 2/1
DES-7200(config-router)# bfd all-interfaces
DES-7200(config-router)# end
```

3.4.1.4 Configuration Verification

1) View the BFD session of RouterA

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
192.168.3.1  192.168.3.2  1/2      1        532 (3 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: RIP
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
```

```
Min tx interval: 50000     - Min rx interval: 50000
Min Echo interval: 0
```

Field	Description
OurAddr	IP address for the session on the local end.
NeighAddr	IP address for the adjacent session.
LD/RD	The session discriminator on the local and peer end.
RH	Whether the peer session responds to the local session or not.
Holdown(mult)	The time of not receiving the Hello packets on the local end and the detected timeout time of the session.
State	Current session state.
Int	The interface number for the session.
Session state is UP and using echo function with 50 ms interval	Whether the session is in echo mode and the interval of sending frames. This information is shown only in the echo mode.
Local Diag	The diagnostic information of the session.
Demand mode	Whether the demand mode is enabled or not.
Poll bit	Whether the session configuration is modified.
MinTxInt	The minimum sending interval of the session on the local end.
MinRxInt	The minimum receiving interval of the session on the local end.
Multiplier	The timeout times detected on the local end.
Received MinRxInt	The minimum sending interval of the session on the peer end.
Received Multiplier	The timeout times detected on the peer end.
Holdown (hits)	Session detection time and the detected timeout times.

Field	Description
Hello (hits)	The minimum interval of receiving the Hello packet after the session negotiation.
Rx Count	The count of BFD packets received on the local end.
Rx Interval (ms) min/max/avg	The minimum/maximum/average interval of receiving the session on the local end.
Tx Count	The count of BFD packets sent on the local end.
Tx Interval (ms) min/max/avg	The minimum/maximum/average interval of sending the session on the local end.
Registered protocols	Type of protocol registered to the session
Uptime	Time of keeping the session UP.
Last packet	Last BFD packet received on the local end.

Table-1 Filed Description of the Session Displaying

2) View the BFD session of RouterB

```
DES-7200# show bfd neighbors details
OurAddr       NeighAddr         LD/RD    RH   Holdown (mult)
    State Int
192.168.3.2   192.168.3.1  2/1      1        532 (5 )         Up
      Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197
Registered protocols: RIP
Uptime: 02:18:49
Last packet:  Version: 1               - Diagnostic: 0
I Hear You bit: 1      - Demand bit: 0
Poll bit: 0                - Final bit: 0
Multiplier: 5              - Length: 24
My Discr.: 1           - Your Discr.: 2
Min tx interval: 200000    - Min rx interval: 200000
```

```
Min Echo interval: 0
```

3.4.2 Example of Configuring BFD for OSPF

3.4.2.1 Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the OSPF protocol and enable the BFD for OSPF on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the OSPF of the failure, triggering the rapid convergence.

3.4.2.2 Network Topology

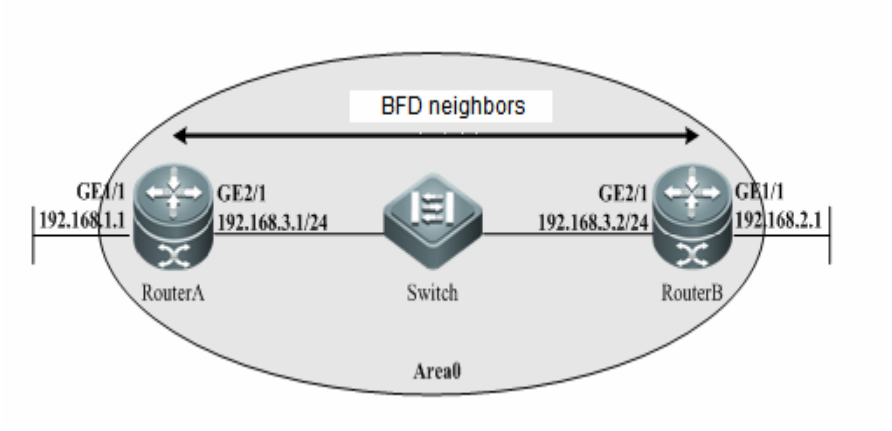


Figure-5 Topology of Configuring BFD for OSPF

3.4.2.3 Configuration Steps

1) RouterA Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
```

```
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
```

Enable RIP and configure the BFD for OSPF to detect the neighbor 192.168.3.2:

```
DES-7200(config-if)# exit
DES-7200(config)# router ospf 123
DES-7200(config-router)# log-adjacency-changes detail
DES-7200(config-router)# network 192.168.3.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.1.0 0.0.0.255 area 0
DES-7200(config-router)# bfd all-interfaces
DES-7200(config-router)# end
```

2) RouterB Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router B:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.2 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.2.1 255.255.255.0
```

Enable OSPF and configure the BFD for OSPF to detect the neighbor 192.168.3.1:

```
DES-7200(config-if)# exit
DES-7200(config)# router ospf 123
DES-7200(config-router)# log-adjacency-changes detail
DES-7200(config-router)# network 192.168.3.0 0.0.0.255 area 0
DES-7200(config-router)# network 192.168.1.0 0.0.0.255 area 0
DES-7200(config-router)# bfd all-interfaces
DES-7200(config-router)# end
```

3.4.2.4 Configuration Verification

1) View the BFD session of RouterA

```
DES-7200# show bfd neighbors details
```

```
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
192.168.3.1  192.168.3.2  1/2      1        532 (3 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0
```

2) View the BFD session of RouterB

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
192.168.3.2  192.168.3.1  2/1      1        532 (5 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: OSPF
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 5                  - Length: 24
My Discr.: 1          - Your Discr.: 2
Min tx interval: 200000   - Min rx interval: 200000
Min Echo interval: 0
```

3.4.3 Example of Configuring BFD for BGP

3.4.3.1 Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the BGP protocol and enable the BFD for BGP on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the BGP of the failure, triggering the rapid convergence.

3.4.3.2 Network Topology

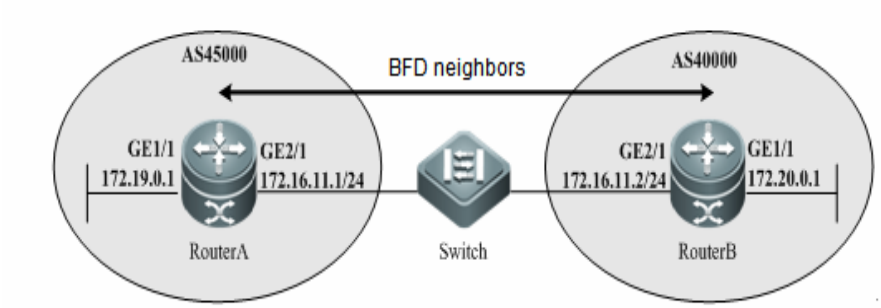


Figure-6 Topology of Configuring BFD for BGP

3.4.3.3 Configuration Steps

1) RouterA Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.16.11.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.19.0.1 255.255.255.0
```

Enable BGP and configure the BFD for BGP to detect the neighbor 172.16.11.2:

```
DES-7200(config-if)# exit
DES-7200(config-router)# router bgp 45000
DES-7200(config-router)# bgp log-neighbor-changes
DES-7200(config-router)# neighbor 172.16.11.2 remote-as 40000
DES-7200(config-router)# neighbor 172.16.11.2 fall-over bfd
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 172.16.10.2 activate
DES-7200(config-router-af)# no auto-summary
DES-7200(config-router-af)# no synchronization
DES-7200(config-router-af)# network 172.19.0.0 mask 255.255.255.0
DES-7200(config-router-af)# exit-address-family
DES-7200(config-router)# end
```

2) RouterB Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router B:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.16.11.2 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.20.0.1 255.255.255.0
```

Enable BGP and configure the BFD for BGP to detect the neighbor 172.16.11.1:

```
DES-7200(config-if)# exit
DES-7200(config-router)# router bgp 40000
DES-7200(config-router)# bgp log-neighbor-changes
DES-7200(config-router)# neighbor 172.16.11.1 remote-as 45000
DES-7200(config-router)# neighbor 172.16.11.1 fall-over bfd
DES-7200(config-router)# address-family ipv4
DES-7200(config-router-af)# neighbor 172.16.11.1 activate
DES-7200(config-router-af)# no auto-summary
DES-7200(config-router-af)# no synchronization
DES-7200(config-router-af)# network 172.20.0.0 mask 255.255.255.0
DES-7200(config-router-af)# exit-address-family
```

```
DES-7200(config-router)# end
```

3.4.3.4 Configuration Verification

- View the BFD session of RouterA

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
172.16.11.1  172.16.11.2  1/2      1        532 (3 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: BGP
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0
```

- View the BFD session of RouterB

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
172.16.11.2  172.16.11.1  2/1      1        532 (5 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: BGP
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 5                  - Length: 24
My Discr.: 1          - Your Discr.: 2
```

```
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0
```

3.4.4 Example of Configuring BFD for Static Route

3.4.4.1 Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the static route protocol and enable the BFD for static route on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the static route of the failure, triggering the static route removal from RIB and preventing the routing error.

3.4.4.2 Network Topology

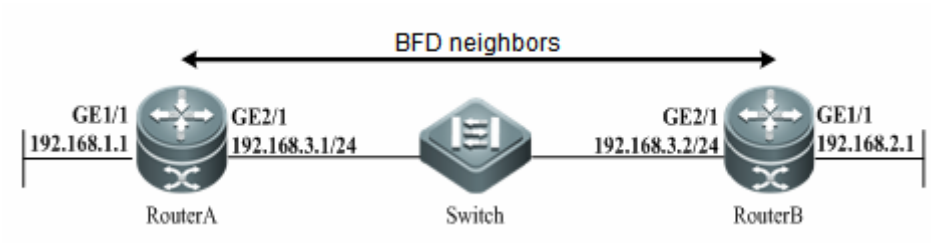


Figure-7 Topology of Configuring BFD for Static Route

3.4.4.3 Configuration Steps

1) RouterA Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Configure the Routed Port *gi1/1*:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
```

Configure the BFD for static route to detect the neighbor 192.168.3.2:

```
DES-7200(config-if)# exit
DES-7200(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.2
DES-7200(config)# ip route 192.168.2.0 255.255.255.0 GigabitEthernet 2/1
192.168.3.2
DES-7200(config)# end
```

2) RouterB Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router B:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.2 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.2.1 255.255.255.0
```

Configure the BFD for static route to detect the neighbor 192.168.3.1:

```
DES-7200(config-if)# exit
DES-7200(config)# ip route static bfd GigabitEthernet 2/1 192.168.3.1
DES-7200(config)# ip route 192.168.1.0 255.255.255.0 GigabitEthernet 2/1
192.168.3.1
DES-7200(config)# end
```

3.4.4.4 Configuration Verification

1) View the BFD session of RouterA

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
192.168.3.1  192.168.3.2  1/2      1        532 (3 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
```

```
Registered protocols: STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0
```

2) View the BFD session of RouterB

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
192.168.3.2  192.168.3.1  2/1      1        532 (5 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 5                  - Length: 24
My Discr.: 1          - Your Discr.: 2
Min tx interval: 200000   - Min rx interval: 200000
Min Echo interval: 0
```

3.4.5 Example of Configuring BFD for PBR

3.4.5.1 Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the PBR protocol and enable the BFD for PBR on the interface. After a link failure between RouterB and L2 switch occurs, BFD detects the failure and notifies the PBR of the failure, triggering the PBR removal preventing the routing error.

3.4.5.2 Network Topology

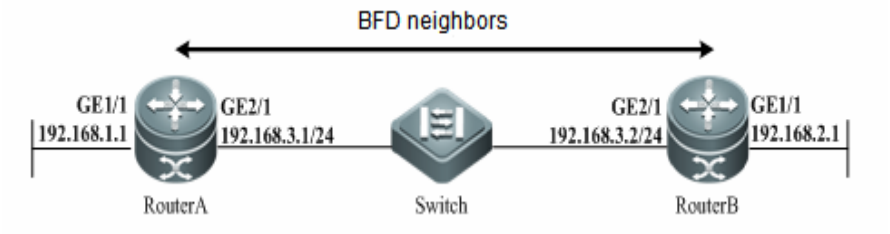


Figure-8 Topology of Configuring BFD for PBR

3.4.5.3 Configuration Steps

1) RouterA Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
```

Configure the BFD for PBR to detect the neighbor 192.168.3.2:

```
DES-7200(config)# ip access-list extended 100
DES-7200(config-ext-nacl)# permit ip any 10.10.10.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip any any
DES-7200(config-ext-nacl)# exit
DES-7200(config)# route-map Example1 permit 10
DES-7200(config-route-map)# match ip address 100
DES-7200(config-route-map)# set ip precedence priority
DES-7200(config-route-map)#set ip next-hop verify-availability 192.168.3.2
bfd GigabitEthernet 0/1 192.168.3.2
DES-7200(config)# end
```

2) RouterB Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router B:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.3.2 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 192.168.2.1 255.255.255.0
```

Configure the BFD for PBR to detect the neighbor 192.168.3.1:

```
DES-7200(config)# ip access-list extended 100
DES-7200(config-ext-nacl)# permit ip any 10.10.11.0 0.0.0.255
DES-7200(config-ext-nacl)# deny ip any any
DES-7200(config-ext-nacl)# exit
DES-7200(config)# route-map Example1 permit 10
DES-7200(config-route-map)# match ip address 100
DES-7200(config-route-map)# set ip precedence priority
DES-7200(config-route-map)#set ip next-hop verify-availability 192.168.3.1
bfd GigabitEthernet 2/1 192.168.3.1
DES-7200(config)# end
```

3.4.5.4 Configuration Verification

1) View the BFD session of RouterA

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
192.168.3.1  192.168.3.2  1/2      1        532 (3 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: PBR
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
```

```
I Hear You bit: 1          - Demand bit: 0
Poll bit: 0                - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
Min tx interval: 50000     - Min rx interval: 50000
Min Echo interval: 0
```

2) View the BFD session of RouterB

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
192.168.3.2  192.168.3.1  2/1      1        532 (5 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 209/440/332 last: 66 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 153/249/197 last: 190 ms ago
Registered protocols: PBR
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1          - Demand bit: 0
Poll bit: 0                - Final bit: 0
Multiplier: 5                  - Length: 24
My Discr.: 1          - Your Discr.: 2
Min tx interval: 200000    - Min rx interval: 200000
Min Echo interval: 0
```

3.4.6 Example of Configuring BFD for VRRP

3.4.6.1 Network Requirement

RouterA and RouterB are interconnected through a L2 switch. Both routers run the VRRP protocol and enable the BFD for PBR on the interface to detect the master and backup routers. After a link failure between RouterB and L2 switch occurs, BFD detects the failure, notifies VRRP of the failure, and triggers the priority level decline of the VRRP master router resulting in the switchover between the master and backup routers, which enables the backup router rapidly.

RouterA and RouterB access the Internet through RouterC and RouterD respectively. Configure the static routes to establish the forwarding path between RouterA and RouterC, RouterB and RouterD and enable the BFD to

detect the neighbor. At the same time, RouterA and RouterB are configured the BFD for VRRP to detect the forwarding path between the RouterA and RouterC, RouterB and RouterD. The detection failure triggers the decline of priority for VRRP master router and switchover between the master and backup routers, which enables the backup router rapidly.

3.4.6.2 Network Topology

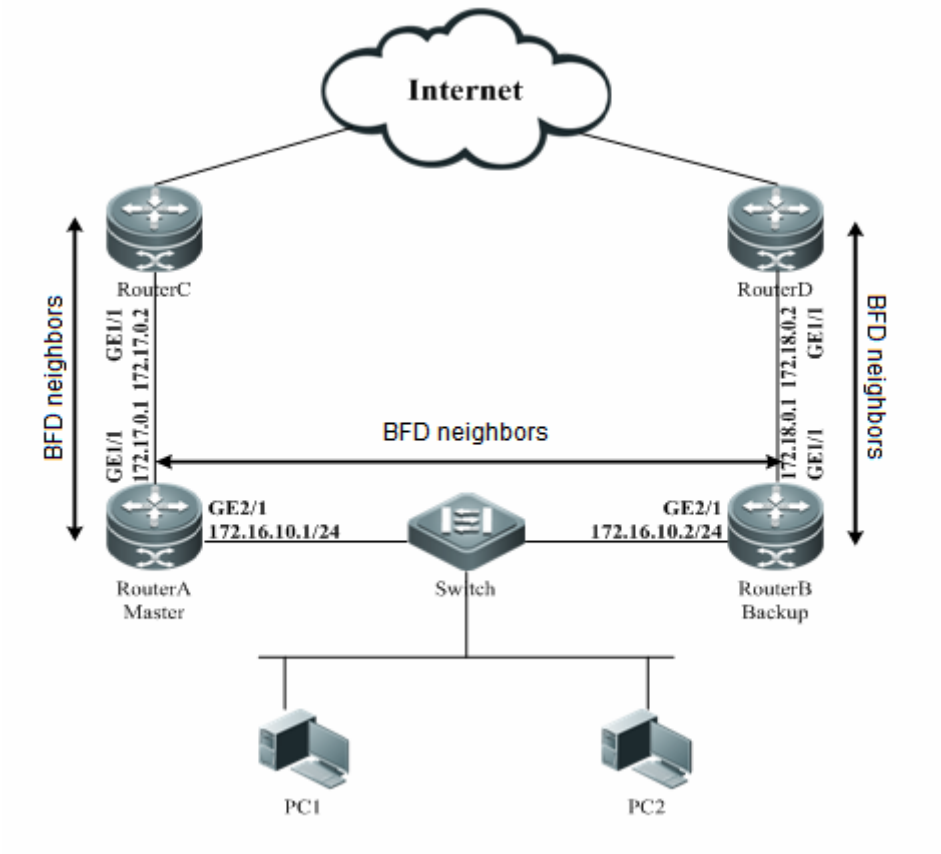


Figure-9 Topology of Configuring BFD for VRRP

3.4.6.3 Configuration Steps

1) RouterC Configuration (Omitted)

2) RouterD Configuration (Omitted)

3) RouterA Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router A:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
```

```
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.16.10.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.17.0.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Enable VRRP and configure the BFD for VRRP to detect the neighbor 172.16.10.2 and 172.17.0.2 at the same time:

```
DES-7200(config-if)# interface GigabitEthernet2/1
DES-7200(config-if)# vrrp 1 timers advertise 3
DES-7200(config-if)# vrrp 1 ip 172.16.10.3
DES-7200(config-if)# vrrp 1 priority 120
DES-7200(config-if)# vrrp 1 bfd 172.16.10.2
DES-7200(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.17.0.2 30
```

Configure the static route and associate the BFD to detect the neighbor 172.17.0.2:

```
DES-7200(config-if)# exit
DES-7200(config)# ip route static bfd GigabitEthernet 1/1 172.17.0.2
DES-7200(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.17.0.2
DES-7200(config)# end
```

2) RouterB Configuration

Configure the Routed Port, the IP address, the BFD session parameter for Router B:

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# interface GigabitEthernet2/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.16.10.2 255.255.255.0
DES-7200(config-if)# bfd interval 50 min_rx 50 multiplier 3
```

Configure the Routed Port gi1/1:

```
DES-7200(config-if)# exit
DES-7200(config)# interface GigabitEthernet1/1
DES-7200(config-if)# no switchport
DES-7200(config-if)# ip address 172.18.0.1 255.255.255.0
DES-7200(config-if)# bfd interval 200 min_rx 200 multiplier 5
```

Enable VRRP and configure the BFD for VRRP to detect the neighbor 172.16.10.1 and 172.18.0.2 at the same time:

```
DES-7200(config-if)# interface GigabitEthernet2/1
DES-7200(config-if)# vrrp 1 timers advertise 3
DES-7200(config-if)# vrrp 1 ip 172.16.10.3
DES-7200(config-if)# vrrp 1 priority 120
DES-7200(config-if)# vrrp 1 bfd 172.16.10.1
DES-7200(config-if)# vrrp 1 track bfd GigabitEthernet 1/1 172.18.0.2 30
```

Configure the static route and associate the BFD to detect the neighbor 172.18.0.2:

```
DES-7200(config-if)# exit
DES-7200(config)# ip route static bfd GigabitEthernet 1/1 172.18.0.2
DES-7200(config)# ip route 0.0.0.0 0.0.0.0 GigabitEthernet 1/1 172.18.0.2
DES-7200(config)# end
```

3.4.6.4 Configuration Verification

- View the BFD session of RouterA

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
172.16.10.1  172.16.10.2  1/2      1        532 (3 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196
Registered protocols: VRRP
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0

OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
172.17.0.1   172.17.0.2            2/3      1        532 (3 )          Up
    Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
```

```
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: VRRP,STATIC ROUTE
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0
```

- View the BFD session of RouterB

```
DES-7200# show bfd neighbors details
OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
172.16.10.2  172.16.10.1  2/1      1        532 (3 )          Up
Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 50000, MinRxInt: 50000, Multiplier: 3
Received MinRxInt: 200000, Received Multiplier: 5
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: VRRP
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 1          - Your Discr.: 2
Min tx interval: 200000   - Min rx interval: 200000
Min Echo interval: 0

OurAddr      NeighAddr         LD/RD    RH   Holdown(mult)     State    Int
172.18.0.1       172.18.0.2        1/3      1        532 (3 )          Up
    Ge2/1
Local Diag: 0, Demand mode: 0, Poll bit: 0
MinTxInt: 200000, MinRxInt: 200000, Multiplier: 5
Received MinRxInt: 50000, Received Multiplier: 3
Holdown (hits): 600(22), Hello (hits): 200(84453)
Rx Count: 49824, Rx Interval (ms) min/max/avg: 208/440/332 last: 68 ms ago
Tx Count: 84488, Tx Interval (ms) min/max/avg: 152/248/196 last: 192 ms ago
Registered protocols: VRRP,STATIC ROUTE
```

```
Uptime: 02:18:49
Last packet: Version: 1                - Diagnostic: 0
I Hear You bit: 1         - Demand bit: 0
Poll bit: 0               - Final bit: 0
Multiplier: 3                  - Length: 24
My Discr.: 2          - Your Discr.: 1
Min tx interval: 50000    - Min rx interval: 50000
Min Echo interval: 0
```

3.4.7 Example of Associating Layer 3 Interface with BFD

Layer 3 interface and BFD association is commonly applied in FRR, and separate use is not recommended.

3.4.8 Example of Configuring BFD for MPLS

Please refer to the descriptions given in MPLS-SCG.doc.

3.4.9 Example of Configuring BFD for VRRP+

Please refer to the descriptions given in *VRRP-PLUS-SCG.doc*.

4 DLDP Configuration

4.1 Overview

Based on the SDH platform, the MSTP supports access, processing, and transmission of multiple services, such as TDM, ATM, and Ethernet, providing a multi-service node for the unified network management system. Because Ethernet lacks in the link keep-alive protocol, Ethernet access is always used at user access points. As a result, link protocol status is still normal even if lines for Ethernet to access the MSTP network are disconnected. In this case, route convergence slows down and the difficulty in locating a fault is increased.

The major procedure for device link detection can be divided into the following stages:

1. Initialization stage

When DLDP is enabled on the interface, DLDP is changed into initialization status, and then an ARP request is sent to obtain the MAC address of the peer device. If DLDP cannot obtain the peer MAC address, DLDP is in the initialization stage unless users prohibit this function and DLDP status is changed into deleted. After the peer MAC address is obtained, DLDP status is changed into link succeeded.

2. Link succeeded status

In this state, DLDP can send a link detection request to detect line connectivity. After DLDP responses are received, the interface is marked UP. If responses are not received, requests are sent until the number of requests exceed the maximum number. In this case, the link is marked failed and DLDP status is changed into initialization. If users delete this function during this process, DLDP status is changed into deleted.

3. Deleted status

In deleted state, the interface status is not analyzed by the link detection function. In this case, the interface status is consistent with the physical channel status.

The devices on both sides detected by DLDP can be set to work in active/passive mode. In the passive mode, DLDP detection packets are not sent actively and only the DLDP detection packets from the peer end are detected and replied to for link detection. When multi-channel DLDP detection is configured on a convergence router,

the passive mode can greatly reduce processing load of the convergence device and traffic load of lines.

In the passive mode, the peer end must be set to active mode so that the devices on both sides can normally work with each other.

4.2 Configuring Device Link Detection

4.2.1 Task List

Follow the task list below to configure Ethernet link detection:

- Configuring Ethernet link detection function
- Configuring the next-hop IP address
- Configuring interval
- Configuring retry times
- Configuring resume times
- Clearing the records of the times when DLDP status is changed from UP to DOWN
- Checking the times when DLDP status is changed from UP to DOWN within a period of time

4.2.2 Configuring Ethernet Link Detection Function

This command can be configured on the Ethernet port only. By default, this function is not enabled. To activate it, run the following command:

Command	Function
DES-7200(config-if)#**dldp** *ip [nexthopip]*	It is used to activate the link detection protocol.

Note

1) This function is implemented with the help of ICMP ECHO packets. The peer device should enable the ICMP response function.

2) The precondition of enabling this function is that the interface is in UP state.

3) After this function is enabled, if the interface is in down state, the IP address of the interface cannot be modified.

4) In the case of detection across network segments, the next-hop IP address should be configured. For example, the local interface IP address is 10.1.1.1 needs to detect 30.1.1.1 through the 20.1.1.1 gateway, the next-hop IP address 20.1.1.1 should be configured.

4.2.3 Configuring Interval

Setting heartbeat intervals can change the frequency of sending handshaking packets for link detection.

Command	Function
DES-7200(config-if)# **dldp ip interval** *val*	It is used to set the interval for device link detection.

4.2.4 Configuring Retry Times

Command	Function
DES-7200(config-if)# **dldp ip retry** *val*	It is used to set the threshold of error times during device link detection.

4.2.5 Configuring Active/Passive Mode

Command	Function
DES-7200(config-if)# **dldp passive**	It is used to set device link detection to work in passive mode.

4.2.6 Configuring Resume Times

Command	Function
DES-7200(config-if)# **dldp ip resume** *val*	It is used to set the threshold of resuming the device link. The threshold indicates that the times for receiving continuous DLDP detection packet responses before the link status is changed from DOWN to UP. The resumption time is related to the interval for sending link detection packets set by running the dldp ip interval command. That is, line resumption time = resume times * dldp ip interval.

Note

This function is used to avoid device link oscillation. For example, when users run the **ping** command to detect link status and the results show that some links are not connected all the time, links are oscillated all the time. That is, link status is always changed between UP and DOWN or ARP is always switched over. Setting a greater resume value can avoid this problem. Only when the number of detection packet responses received by the link reached the threshold set by using the **resume** command, link status is changed from DOWN to UP.

4.2.7 Clearing the Records of the Times when DLDP Status is Changed from UP to DOWN

Command	Function
DES-7200(config-if)# **clear-dldp***[all] [ip [nexthopip]]*	DES-7200 routers can record the times of UP and DOWN status of device links. Running the clear-dldp command can clear the recorded times and begin to record the times.

Note

1) Running the **clear-dldp all** command to clear the times when all links on an interface are changed from UP to DOWN within a period of time and to record the times from 0.

2) Running the **clear-dldp ip [nexthopip]** command to clear the times when the specified link is changed from UP to DOWN within a period of time and to record the times from 0.

4.2.8 Checking the Times when Ethernet Link Status is UP and DOWN Within a Period of Time

Command	Function
DES-7200(config-if)# **show dldp interface** *[ ] [FastEthernet/GigabitEthernet number]*	It is used to check the times when Ethernet links are changed from UP to DOWN within a period of time on the configured DLDP-enabled interface.

Note

1) Run the **show dldp interface** command to check the times of all Ethernet links when their status is UP and DOWN and the time for beginning to record the times.

2) Run the **show dldp interface FastEthernet/GigabitEthernet number** command to check the times when links are UP and DOWN on the Ethernet interface and the time for beginning to record the times.

5 RERP Configuration

5.1 RERP Overview

5.1.1 Understanding RERP

For the loop blocking and link recovery in core ring network, currently the OSPF and BGP4 are mostly used for the implementation. For complex network, the link recovery may take tens of seconds. If MSTP is used for loop blocking in the link layer, the STP needs to advertise level by level by the spanning tree, the network convergence may take rather long time in case of complicated network.

The Rapid Ethernet Ring Protection Protocol (RERP) is a special layer-2 link redundancy backup protocol designed for core Ethernet. The loop blocking and link recovery for the RERP are centrally implemented on the master device and the non-master devices directly report their link conditions to the master device without additional processing on the non-master devices; however the STP works with the spanning tree to advertise level by level by the spanning tree and determine the final link status through level-by-level calculations. So, the loop block and recovery with the RERP are faster than those with the STP. Based on the above difference, the link recovery of RERP in ideal environment may be completed in 50 microseconds.

The RERP involves the following key concepts: Region, Ring, Master, Backup, Transit, Primary Edge Node, Secondary Edge Node, Primary Port, Secondary Port, Shared Port and Control Vlan. They are explained through the following typical applications.

Note As an alternative of STP in the core ring network, the RERP cannot be turned on at the same time with the STP in the actual configurations. RERP and REUP cannot share one port.

5.1.2 Typical Applications

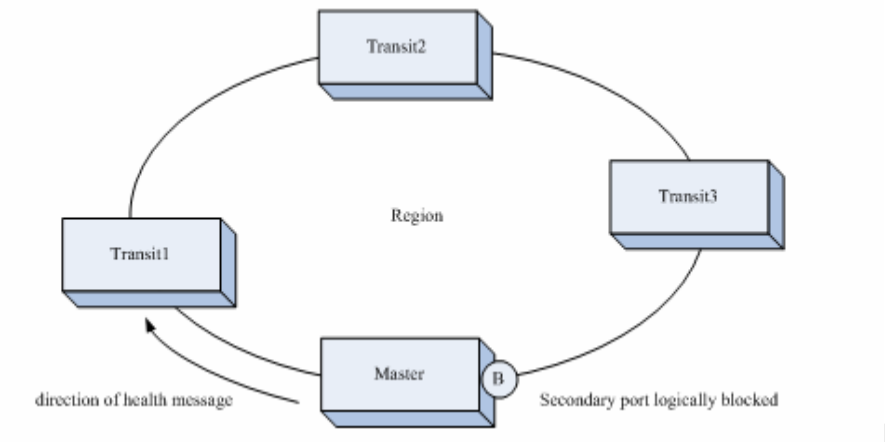


Figure-1

As shown above, the four devices are all core Ethernet devices and form a ring core network. In such a topology, each device has two and only two interface to be connected with the ring. This type of ring is called a RERP region, identified uniquely with an integer. Each RERP region can have several rings. Each RERP region can have only one Master and one Backup specified. The others are all Transit. Each device must be specified with the region and configured with the master/backup port.

Master:

The link is a TRUNK connection. The ring has an independent VLAN as the control VLAN, which is specially used to transmit various control messages defined by the RERP. The other VLANs are the data VLANs and used for the transmission of dataflow.

The two ports of the master connected to the ring are called the primary port and secondary port respectively, whether the primary port sends the Hello message outside on regular basis.

Loop blocking:

In normal cases, the master device prevents the generation of layer-2 loop in the whole ring by blocking the secondary port.

Link interruption:

When a link fails in the Ethernet ring (the link between Transit1 and Transit2 is broken, for example), both Transit1 and Transit2 may recognize this condition in the link, and advertise a LINK DOWN message via the control VLAN to the master. When the master receives it, it clears the layer-2 forwarding table information related with its data VLAN, and sends the FLUSH NOW message to notify all control devices to clear all data VLAN related layer-2 forwarding information. At the same time, the BLOCK status turns into the FORWARDING status.

Link recovery:

When the interrupted link recovers in the Ethernet (the one between Transit1 and Transit2 recovers normal, for example), Transit1 and Transit2 recognize the link recovery information, and make the ports of the recovery link ends in the BLOCK status, to forbid forwarding any messages. Then, they send the LINK UP advertisement to the master. The master receives it and turns the secondary interface in the BLOCK status, and then sends FLUSH NOW message to notify all controlled device to clear all data VLAN related layer-2 address table information. When Transit1 and Transit2 find the link recovery devices receive the FLUSH NOW message, they clear the layer-2 address table information in all data VLAN and then change the ports in BLOCK status into the FORWARDING status.

Device abnormity detection:

When the primary port of the master sends the HELLO message on regular basis (at an adjustable time interval, in seconds), if the secondary interface of the master does not receive the HELLO message from the primary port of the master, it considers the devices on the ring abnormal. Now, the master clears the data VLAN related layer-2 forwarding table information and sends the FLUSH NOW message to notify all controlled device to clear the DATA VLAN layer-2 forwarding table information, and then changes the BLOCK status of the secondary port into the FORWARDING status.

When the secondary port of the master receives the HELLO message from the primary interface, it immediately turns the secondary port to the BLOCK status, and then sends the FLUSH NOW message to notify the controlled devices to clear the layer-2 address table information in all data VLANs.

Master failure detection:

The user can specify a secondary device as the backup master. When the backup master does not detect the HELLO message sent from the master, it considers failure of the master and escalates itself to the master.

After the backup master switches to the master device, if it receives the message from the original master, it transfers the control to the original master and degrades again to the backup master.

The RERP supports tangent multiple rings. In other words, it allows multiple rings to share one devices. In this topology, two rings can run independently, which can be in the same domain or belong to different domains.

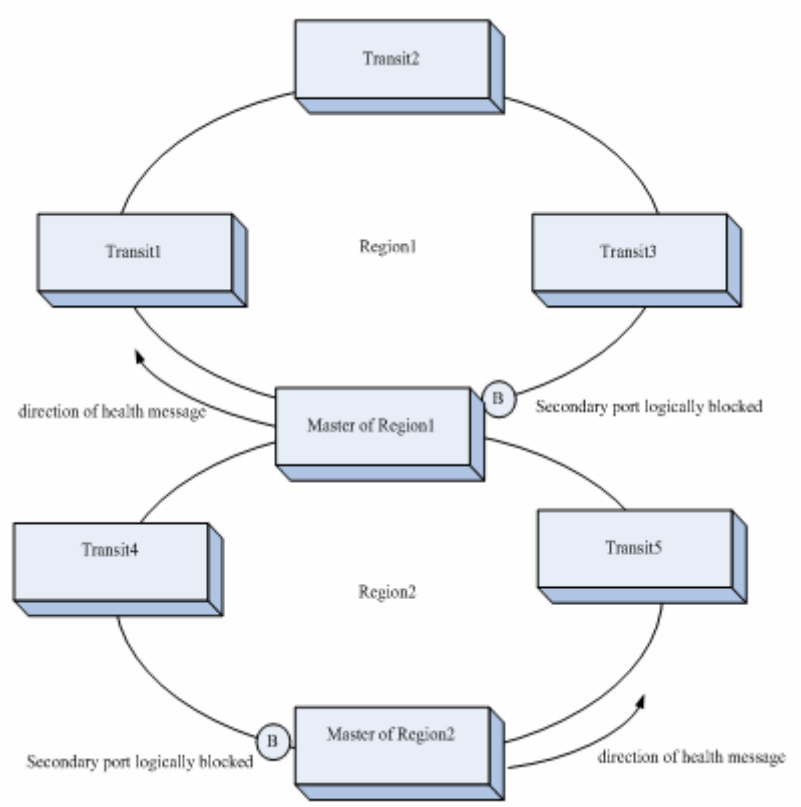


Figure-2

RERP also support the intersection of multiple rings in the single domain:

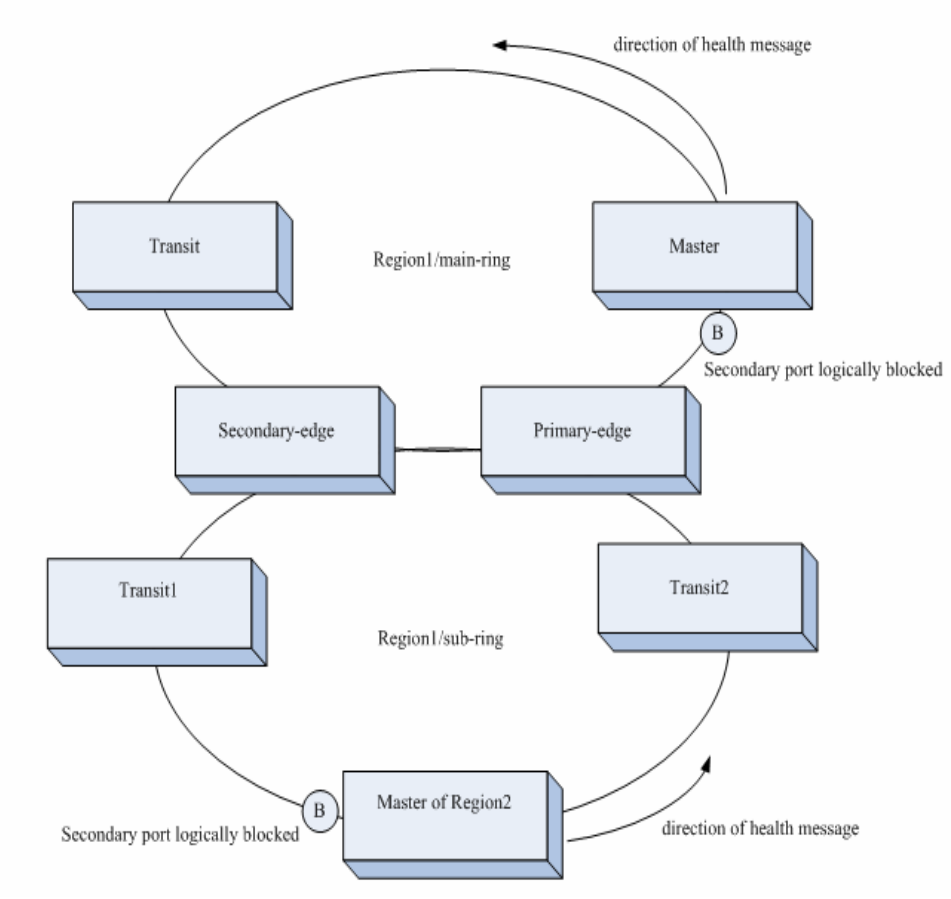


Figure-3

As shown in Figure-3, two rings are intersected in Region 1. In other words, the two rings (main-ring and sub-ring) share one link. The two intersected nodes are called Primary-edge and Secondary-edge respectively. RERP only support one sub-ring in one shared link. The connection line between Secondary-edge and Primary-edge in Figure-3 is the shared link. The characteristic of the intersected rings is that the RERP messages for the sub-ring can be controlled as the datagram in the main-ring that provides two backup links for the sub-ring. As shown in the Figure, the Secondary-edge and Primary-edge communicate through two paths. If one path is Down, no change happens for the sub-ring. While if the two paths are both Down, Secondary-edge is able to detect the failure rapidly and notify the Master in the sub-ring in time, enabling the rapid switchover of the sub-ring, rather than switchover untill the hello failure for the sub-ring. Besides, when the link between the Secondary-edge and the Primary-edge is recovered, Secondary-edge will discover and notify the Master in the sub-ring of blocking the secondary port and loop prevention. That fast processing depends on the new edge health detection mechanism between the Secondary-edge and the Primary-edge. The Secondary-edge and Primary-edge inter-detect each other in both directions of the main-ring, and the Secondary-edge is responsible for notifying the Master in the sub-ring. This ring

intersection technology improves the flexibility of the RERP network topology enormously.

5.2 Configuring RERP

The following sections describe how to configure RERP.

- RERP defaults
- Configure global RERP
- Configure RERP detection interval
- Configure RERP detection failure period
- Configure RERP region
- Configure RERP ring
- Configure RERP edge node
- Configure RERP region control VLAN

5.2.1 Default RERP Configuration

Global RERP status	DISABLE
RERP detection interval	1S
RERP failure time	3S

Precautions before Configuration:

- The RERP and STP are exclusive. In other words, if the RERP is configured, the STP shall be turned off. RERP and REUP cannot share a port.
- The refresh failure waiting time and the detection failure time are always the same and equal to the failure time.
- If the Transit and Backup do not receive the HELLO message from the Master, they will use the detection interval and detection failure interval that are configured on the local machine. If the HELLO message is received from the master, the master configurations will be used to keep consistent protocol operations on the ring network.
- The RERP control VLAN does not include vlan 1 and vlan 4094.
- Each RERP region must have one and only one master and at the same time at most one backup.

- With intersected rings configured, the failure interval of the sub-ring must be more than the one of the main-ring. It is necessary to set the failure interval of the sub-ring twice as the main-ring.
- To prevent the loop interruption during the process of configuration modification, you shall shutdown one of the RERP port in this ring and use the **no shutdown** command when modifying the RERP configurations of a ring.
- After the RERP port is enabled, it is set as the trunk port automatically, and the native VLAN is set as the control VLAN in the corresponding ring automatically. The modification of trunk and native VLAN attribute for the RERP port is prohibited. After the RERP port is disabled, it is still trunk port and the native VLAN restores to 1.
- After adding the AP port to the RERP ring, the operation of adding AP members to the AP port, removing AP members and AP port can not be implemented. The AP port shall exit from the RERP ring to execute the above operation.
- Fail to enable IGMP Snooping on the device with RERP enabled. Or the RERP cannot work normally.

5.2.2 Configuring RERP Globally

The protocol messages can be processed normally when the global RERP is enabled.

In the global configuration mode, follow these steps to enable RERP:

Command	Function
DES-7200(config)# **rerp enable**	Turn on the global RERP function switch.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command turns off the global RERP.

Note

After setting primary and secondary ports, the port forwarding status is controlled no matter whether RERP global switch is turned on. For example, when RERP is disabled, the slave port of master will still in the blocked status to prevent the rings due to parameter configuration error.

5.2.3 Configuring RERP Detection Interval

The Master needs to send the RERP detection message on regular basis to check the health conditions of the loop. In the configuration mode, follows these steps to set the RERP detection interval:

Command	Function

Command	Function
DES-7200(config)# **rerp hello-interval** *interval*	Configure the detection interval within the range 1-6s, 1s by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

5.2.4 Configuring RERP Failure Time

If the secondary port of the master does not receive the detection message from the primary port in a certain period, it considers the fault of the loop, and then the master forces the secondary port to enter the learning forwarding status. In addition, the address refresh waiting time of the Transit and Backup is also that value.

In the global configuration mode, follow these steps to configure the RERP failure time:

Command	Function
DES-7200(config)# **rerp fail-interval** *num*	Configure the failure interval within the range 3-18s, 3 s by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

Note The failure interval must be greater than or equal to three times of the detection interval. Once an intersection ring is configured, the timeout time of the sub ring should be two times of the major ring.

5.2.5 Configuring RERP Region

An RERP region is uniquely identified with an integer, and up to 64 regions can be configured on a machine. While the RERP region is configured, it also specifies the device to support the region and enter the RERP region configuration mode.

In the privileged mode, follow these steps to configure the RERP region:

Command	Function
DES-7200(config)# **rerp region** *num*	Create an RERP region and enter the RERP region configuration mode. The range of *num* is 1-64.

5.2.6 Configuring RERP Ring

Each device plays only one role in a RERP ring. Only one master device and one backup device can be configured in a RERP ring.

In the global configuration mode, follow these steps to configure the RERP region role:

Command	Function
DES-7200(config)# **rerp region** *num*	Create an RERP region and enter the RERP domain configuration mode.
DES-7200 (config-rerp)# **ring** *num* **role** [**master | backup | transit**] **ctrl-vlan** *vid* **primary-port interface** *interface-id* **secondary-port interface** *interface-id*	Configure the role of the device in the RERP ring, control VLAN and primary/secondary port.

Note

When a port joins a RERP ring, it is automatically set to be a trunk port, the native VLAN is automatically set to be the control VLAN. Modifying the trunk port and native VLAN is prohibited. After the port leaves from the RERP ring, it is still a trunk port, but the native VLAN is restored to VLAN 1.

5.2.7 Configuring Edge Nodes

Two rings have two intersect nodes and share a link. The devices located in the two ends of the link are called edge nodes.

In the global configuration mode, follow these steps to configure edge nodes:

Command	Function
DES-7200(config)# edge-**ring num role** [**primary-edge**|**secondary-edge**] ctrl-vlan *vid* **shared-port interface** *interface-id* **sub-port interface** *interface-id*	Configure edge nodes

Note

1. The shared port must be configured in advance in a RERP ring. That is to say, a RERP ring must be configured before you configure this command.
2. When configuring the RERP intersect ring, it is worth mentioning that one primary master ring only supports one sub-ring. Or the RERP ring data forwarding control will fail. To this end, the network topology shall be carefully planned before configuring the RERP.

5.2.8 Configuring the Control VLAN for the Edge Ring Supported on the Major Ring

To transmit the packets from the edge ring on the port of the major ring, set the edge ring on the major ring.

In the global configuration mode, follow these steps to configure the control VLAN for the edge ring on the major ring:

Command	Function
DES-7200(config)# **rerp region** *num*	Create an RERP region and enter the RERP domain configuration mode at the same time.
DES-7200(config-rerp)# **major-ring** *num* **edge-ring-vlan** *vid*	Set the control VLAN for the edge ring on the major ring.

Note

The major ring must have been existed.

5.3 Viewing RERP Information

The following RERP-related information can be viewed:

- View RERP configuration and status
- View RERP packet statistics

5.3.1 Viewing RERP Configuration and Status

In the privileged mode, run the following command to view the RERP configuration and status of the device:

Command	Function
DES-7200# **show rerp**	View the RERP configuration and status of the device

In the example below, the **show rerp** command is used to view the RERP configuration and status of the device.

```
DES-7200# show rerp

rerp state                    : enable

rerp admin hello interval  : 1(*1s)

rerp admin fail interval   : 3(*1s)

rerp edge interval         : 1(*300 ms)

rerp local bridge          : 001a.a902.fe0b

---------------------------------

region 1

ring                       : 1

rerp oper hello interval   : 1

rerp oper fail  interval   : 3

ring master                    : 001a.a902.fe0b

ctrl-vlan                      : 100

edge-vlan                      :

role                       : master

primary-port                   : GigabitEthernet 0/4(forwarding)

secondary-port                 : GigabitEthernet 0/21(down)
```

5.3.2 Viewing RERP Packet Statistics

In the privileged mode, run the following command to view the RERP packet statistics:

Command	Function
DES-7200# **show rerp statistics region** *num* **ring** *ring_id*	View the RERP packet statistics
DES-7200# **clear rerp statistics**	Clear the RERP packet statistics

The example below shows the RERP packet statistics:

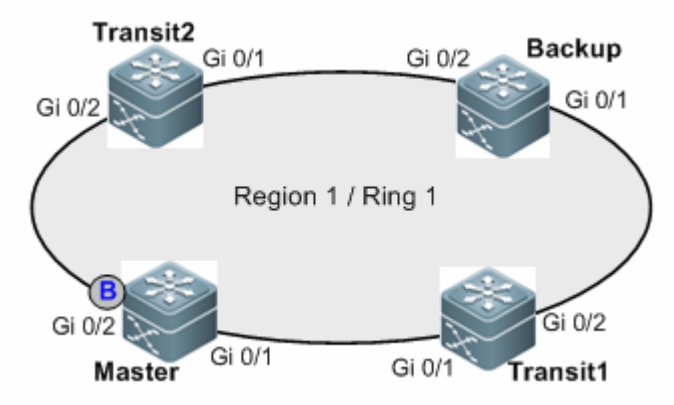
```
DES-7200# show rerp statistics region 1 ring 1
The statistics for region 1 ring 1 GigabitEthernet 0/4

TX hello packets       23   , RX hello packets        0

TX edge-hello packets   0    , RX edge-hello packets  0

TX flush packets        0    , RX flush packets       0

TX down packets        0    , RX down packets         0

TX up packets              0    , RX up packets           0

TX major fail packets   0    , RX major fail packets  0

TX major resume packets    0    , RX major resume packets 0

TX sub complete packets    0    , RX sub complete packets 0


The statistics for region 1 ring 1 GigabitEthernet 0/21

TX hello packets           0    , RX hello packets       23

TX edge-hello packets   0    , RX edge-hello packets    0

TX flush packets           0    , RX flush packets        0

TX down packets            0    , RX down packets         0

TX up packets          0    , RX up packets           0

TX major fail packets      0    , RX major fail packets   0

TX major resume packets0    , RX major resume packets  0

TX sub complete packets0    , RX sub complete packets  0
```

5.4 Typical RERP Configuration Examples

5.4.1 RERP Single Ring Configuration Examples

5.4.1.1 Topological Diagram

The following figure shows the topological diagram for the core network of a sci-tech park.



Topological diagram for RERP single ring

5.4.1.2 Application Requirements

It is required that this core network shall be able to implement rapid switchover upon link failure and avoid the failure of entire ring caused by single point failure.

5.4.1.3 Configuration Tips

Four core devices use RERP ring to realize ring protection of the sci-tech core network and rapid switchover in case of any link failure. The RERP ports (G0/1 and G0/2) of all nodes on the ring belong to the same control VLAN (VLAN 4000). G0/1 is configured as the primary port, while G0/2 is configured as the secondary port. The timer uses the default value. Roles of respective devices on the ring are shown above.

Note

On the RERP ring, the interface joining RERP ring must be a Trunk port, and its Native Vlan must be configured to the control VLAN of corresponding ring. In this example, all interfaces (G0/1 and G0/2) joining the RERP ring have been configured as Trunk ports, the Native VLAN has been configured to control VLAN (VLAN 4000). For detailed configurations, please refer to the section of "Interface Configuration" as shown in this manual.

Before configuring RERP, we must identify the roles of respective devices on RERP single ring, and then implement RERP configuration on respective devices according to the following steps:

1. Define the RERP domain.
2. Define the RERP ring and configure the role of this device on RERP ring, the control VLAN to which it belongs and the primary and secondary ports.
3. Enable the RERP.

5.4.1.4 Configuration Steps

- **RERP configurations on Master device**

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
DES-7200#configure terminal
```

! Create the RERP domain with ID being 1.

```
DES-7200(config)# RERP region 1
```

Step 2: Define the RERP ring.

! Enter the RERP domain configuration mode: configure the RERP ring with ID being 1, define the role of device as Master, control VLAN as VLAN 4000, and primary and secondary ports as G0/1 and G0/2 respectively.

```
DES-7200(config-rerp)# ring 1 role master ctrl-vlan 4000 primary-port
interface gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/2
DES-7200(config-rerp)#exit
```

Step 3: Enable the RERP.

```
DES-7200(config)#rerp enable
```

- **RERP configurations on Backup device**

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
DES-7200#configure terminal
```

! Create RERP domain with ID being 1

```
DES-7200(config)# RERP region 1
```

Step 2: Define the RERP ring.

! Enter the RERP domain configuration mode: configure the RERP ring with ID being 1, define the role of device as Backup, control VLAN as VLAN 4000, and primary and secondary ports as G0/1 and G0/2 respectively.

```
DES-7200(config-rerp)# ring 1 role backup ctrl-vlan 4000 primary-port
interface gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/2
DES-7200(config-rerp)#exit
```

Step 3: Enable the RERP.

```
DES-7200(config)#rerp enable
```

- **RERP configurations on Transit device**

Configurations on Transit 1 and Transit 2 are the same:

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
DES-7200#configure terminal
```

! Create the RERP domain with ID being 1.

```
DES-7200(config)# RERP region 1
```

Step 2: Define the RERP ring.

! Enter the RERP domain configuration mode: configure the RERP ring with ID being 1, define the role of device as Transit, control VLAN as VLAN 4000, and primary and secondary ports as G0/1 and G0/2 respectively.

```
DES-7200(config-rerp)# ring 1 role transit ctrl-vlan 4000 primary-port
interface gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/2
DES-7200(config-rerp)#exit
```

Step 3: Enable the RERP.

```
DES-7200(config)#rerp enable
```

5.4.1.5 Verify Configurations

Step 1: Connect the network cables as per the topological diagram, and use "**show**" command to verify the configurations.

- **Verify configurations of Master**

1. Verify the RERP configurations on Master device; key point: whether the secondary port remains in blocked state while the ring is healthy.

```
DES-7200#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f834.56f1
----------------------------------
region 1
ring                 : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master           : 00d0.f834.56f1
ctrl-vlan             : 4000
edge-vlan             :
role                 : master
primary-port          : GigabitEthernet 0/1(forwarding)
secondary-port        : GigabitEthernet 0/2(blocked)
```

➢ **Verify configurations of Backup**

2. Verify the RERP configurations on Backup device; key points: role of device, MAC address of Master device, and the state of primary and secondary ports.

```
DES-7200(config)#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f834.56f1
----------------------------------
region 1
ring                 : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master           : 00d0.f834.56f2
ctrl-vlan             : 4000
edge-vlan             :
role                 : backup
primary-port          : GigabitEthernet 0/1(forwarding)
secondary-port        : GigabitEthernet 0/2(forwarding)
```

➢ **Verify configurations of Transit**

3. Verify the RERP configurations on Transit device; key points: role of device, MAC address of Master device, and the state of primary and secondary ports.

```
DES-7200(config)#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f834.56f3
----------------------------------
region 1
ring                 : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master           : 00d0.f834.56f1
ctrl-vlan             : 4000
edge-vlan             :
role                 : transit
primary-port          : GigabitEthernet 0/1(forwarding)
secondary-port        : GigabitEthernet 0/2(forwarding)
```

Step 2: Disconnect the link between Master and Transit1 (simulating that the link between them is failed), and then verify RERP configurations on Master device; key point: the state of primary and secondary ports.

```
DES-7200#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f822.35ad
----------------------------------
region 1
ring                 : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master           : 00d0.f822.35ad
ctrl-vlan             : 4000
edge-vlan             :
role                 : master
primary-port          : GigabitEthernet 4/1(down)
secondary-port        : GigabitEthernet 4/2(forwarding)
```

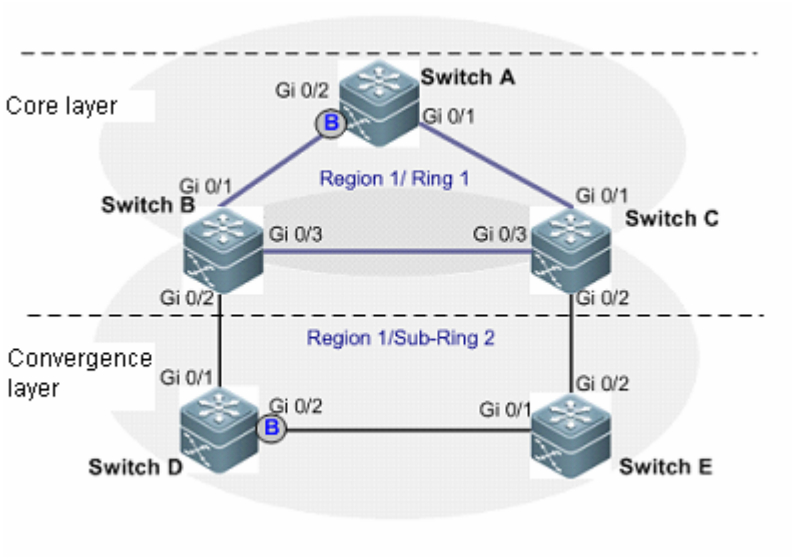
Step 3: Disconnect the link between Transit1 and Backup device (simulating that the link between them is failed), and then verify RERP configurations on Master device; key point: the state of primary and secondary ports.

```
DES-7200#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f822.35ad
----------------------------------
region 1
ring                 : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master           : 00d0.f822.35ad
ctrl-vlan             : 4000
edge-vlan             :
role                 : master
primary-port          : GigabitEthernet 4/1(forwarding)
secondary-port        : GigabitEthernet 4/2(forwarding)
```

5.4.2 RERP single-domain intersecting rings configuration example

5.4.2.1 Topological Diagram

As shown below, the convergence layer of Metropolitan Area Network accesses the core layer in the form of ring topology. The core layer network is a ring network.



Topological diagram for RERP single-domain intersecting rings

5.4.2.2 Application Requirements

Use the appropriate Ethernet ring link protection protocol which can allow fast convergence of the ring when it fails.

5.4.2.3 Configuration Tips

This example adopts RERP technology. The three devices at the core layer (Switch A, Switch B and Switch C) form the RERP primary ring, while four devices at the convergence layer (Switch B, Switch C, Switch D and Switch E) form the RERP subring. Two rings intersect.

The control VLAN of primary ring is VLAN4091, and the control VLAN of subring is VLAN4092. The timer uses the default value, and the roles of respective devices in the domain are shown in the following table.

Device	Role
Switch A	Master of primary ring

Switch B	Transit of primary ring, Primary-edge of subring
Switch C	Transit of primary ring, Secondary-edge of subring
Switch D	Master of subring
Switch E	Transit of subring

How to configure the single-domain intersecting rings:

1. Configure the interfaces joining RERP ring as Trunk ports and configure the Native VLAN to the control VLAN of corresponding ring.

Note

The Native VLAN of the shared ports of primary-edge and secondary-edge of RERP intersecting rings is the control VLAN of primary ring (conceptually, we treat the shared port as a port on the primary ring as a part of primary ring). The configuration steps are detailed in "Interface Configuration" of this manual.

2. Define the RERP domain.
3. Define the RERP ring and configure the role of this device on RERP ring, the control VLAN to which it belongs and the primary and secondary ports. During the configuration of intersecting rings, the following two points shall be paid attention to:
   a) The primary-edge and secondary-edge devices are transit devices on the primary ring. You must configure the shared-port and sub-port for the edge device.
   b) For a device on the primary ring, you must configure the control VLAN of subring supported by the primary ring, namely to join RERP port of this device into the control VLAN of subring.
   c) In the intersecting rings, the timeout interval of subring must be greater than that of primary ring. It is suggested to set the timeout interval on subring Master to a value being two times of the timeout interval of primary ring.
4. Enable the RERP.

5.4.2.4 Configuration Steps

- **Configure Switch A**

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
SwitchA#configure terminal
```

! Create the RERP domain with ID being 1.

```
SwitchA(config)# RERP region 1
```

Step 2: Configure the RERP ring.

! Enter the RERP domain configuration mode: configure RERP ring with ID being 1, define the role of device as Master, control VLAN as VLAN4091, and primary and secondary ports as G0/1 and G0/2 respectively.

```
SwitchA(config-rerp)# ring 1 role master ctrl-vlan 4091 primary-port interface
gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/2
```

! Configure the control VLAN of subring as supported by the primary ring.

```
SwitchA(config-rerp)#major-ring 1 edge-ring-vlan 4092
SwitchA(config-rerp)#exit
```

Step 3: Enable the RERP.

```
SwitchA(config)#rerp enable
```

- **Configure Switch B**

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
SwitchB#configure terminal
```

! Create the RERP domain with ID being 1.

```
SwitchB(config)# RERP region 1
```

Step 2: Configure the RERP ring.

! Enter the RERP domain configuration mode: configure the RERP primary ring with ID being 1, define the role of device as Transit, control VLAN as VLAN4091, and primary and secondary ports as G0/1 and G0/3 respectively.

```
SwitchB(config-rerp)# ring 1 role transit ctrl-vlan 4091 primary-port
interface gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/3
```

! Configure the RERP subring with ID being 2, define the role of device as Primary-edge, control VLAN as VLAN4092, and shared-port and sub-ports as G0/3 and G0/2 respectively.

```
SwitchB(config-rerp)# edge-ring 2 role primary-edge ctrl-vlan 4092
shared-port interface gigabitEthernet 0/3  sub-port interface
gigabitEthernet 0/2
```

! Configure the control VLAN of subring as supported by the primary ring

```
SwitchB(config-rerp)#major-ring 1 edge-ring-vlan 4092
```

```
DES-7200(config-rerp)#exit
```

Step 3: Enable the RERP.

```
SwitchB(config)#rerp enable
```

- **Configure Switch C**

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
SwitchC#configure terminal
```

! Create the RERP domain with ID being 1.

```
SwitchC(config)# RERP region 1
```

Step 2: Configure the RERP ring.

! Enter the RERP domain configuration mode: configure the RERP primary ring with ID being 1, define the role of device as Transit, control VLAN as VLAN4091, and primary and secondary ports as G0/1 and G0/3 respectively.

```
SwitchC(config-rerp)# ring 1 role transit ctrl-vlan 4091 primary-port
interface gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/3
```

! Configure the RERP subring with ID being 2, define the role of device as Secondary-edge, control VLAN as VLAN4092, and shared-port and sub-ports as G0/3 and G0/2 respectively.

```
SwitchC(config-rerp)#edge-ring 2 role Secondary-edge ctrl-vlan 4092
shared-port interface gigabitEthernet 0/3  sub-port interface
gigabitEthernet 0/2
```

! Configure the control VLAN of subring as supported by the primary ring.

```
SwitchC(config-rerp)#major-ring 1 edge-ring-vlan 4092
SwitchC(config-rerp)#exit
```

Step 3: Enable the RERP.

```
SwitchC(config)#rerp enable
```

- **Configure Switch D**

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
SwitchD#configure terminal
```

! Create the RERP domain with ID being 1.

```
DES-7200(config)# RERP region 1
```

Step 2: Configure the RERP ring.

! Enter the RERP domain configuration mode: configure RERP ring with ID being 2, define the role of device as Master, control VLAN as VLAN4092, and primary and secondary ports as G0/1 and G0/2 respectively.

```
SwitchD(config-rerp)# ring 2 role master ctrl-vlan 4092 primary-port interface
gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/2
DES-7200(config-rerp)#exit
```

! Set the timeout interval of subring to a value being two times of the timeout interval of primary ring. The timeout interval of primary ring is 3s by default, so the timeout interval of subring is set to 6s.

```
SwitchD(config)# rerp fail-interval 6
```

Step 3: Enable the RERP.

```
SwitchD(config)#rerp enable
```

- **Configure Switch E**

Step 1: Define the RERP domain.

! Enter the global configuration mode.

```
SwitchE#configure terminal
```

! Create the RERP domain with ID being 1.

```
SwitchE(config)# RERP region 1
```

Step 2: Configure the RERP ring.

! Enter the RERP domain configuration mode: configure the RERP ring with ID being 2, define the role of device as Transit, control VLAN as VLAN4092, and primary and secondary ports as G0/1 and G0/2 respectively.

```
SwitchE(config-rerp)# ring 2 role transit ctrl-vlan 4092 primary-port
interface gigabitEthernet 0/1 secondary-port interface gigabitEthernet 0/2
SwitchE(config-rerp)#exit
```

Step 3: Enable the RERP.

```
SwitchE(config)#rerp enable
```

5.4.2.5 Verify Configurations

Step 1: Connect the network cables as per the topological diagram, and use "show" command to verify the configurations.

- **Configurations of Switch A**

Verify the RERP configurations on Master device of primary ring; key point: whether the secondary port remains in blocked state while both rings are healthy.

```
SwitchA#show rerp
```

```
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f822.35ad
---------------------------------
region 1
ring                 : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master           : 00d0.f822.35ad
ctrl-vlan             : 4091
edge-vlan             : 4092
role                 : master
primary-port          : GigabitEthernet 0/1(forwarding)
secondary-port        : GigabitEthernet 0/2(blocked)
```

- **Configurations of Switch B**

Verify the RERP configurations on the primary-edge device; key points: roles of device on the primary ring and subring, and port state.

```
SwitchB#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f822.1120
---------------------------------
region 1
ring                 : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master           : 00d0.f822.35ad
ctrl-vlan             : 4091
edge-vlan             : 4092
role                 : transit
primary-port          : GigabitEthernet 0/1(forwarding)
secondary-port        : GigabitEthernet 0/3(forwarding)

ring                 : 2
rerp oper hello interval : 1
rerp oper fail  interval : 6
ring master           : 00d0.f822.3416
ctrl-vlan             : 4092
edge-vlan             :
role                 : primary-edge
```

```
shared-port            : GigabitEthernet 0/3(forwarding)
sub-port               : GigabitEthernet 0/2(forwarding)
```

- **Configurations of Switch C**

Verify the RERP configurations on the secondary-edge device; key points: roles of device on the primary ring and subring, and port state.

```
SwitchC#show rerp
rerp state             : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f834.56f0
----------------------------------
region 1
ring                  : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master            : 00d0.f822.35ad
ctrl-vlan              : 4091
edge-vlan              : 4092
role                  : transit
primary-port           : GigabitEthernet 0/1(forwarding)
secondary-port         : GigabitEthernet 0/3(forwarding)

ring                  : 2
rerp oper hello interval : 1
rerp oper fail  interval : 6
ring master            : 00d0.f822.3416
ctrl-vlan              : 4092
edge-vlan              :
role                  : secondary-edge
shared-port            : GigabitEthernet 0/3(forwarding)
sub-port               : GigabitEthernet 0/2(forwarding)
```

- **Configurations of Switch D**

Verify the RERP configurations on Master device of subring; key point: whether the secondary port remains in blocked state while the ring is healthy.

```
SwitchD(config)#show rerp
rerp state             : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 6(*1s)
rerp local bridge      : 00d0.f822.3416
----------------------------------
region 1
```

```
ring                 : 2
rerp oper hello interval : 1
rerp oper fail  interval : 6
ring master           : 00d0.f822.3416
ctrl-vlan             : 4092
edge-vlan             :
role                 : master
primary-port          : GigabitEthernet 0/1(forwarding)
secondary-port        : GigabitEthernet 0/2(blocked)
```

- **Configurations of Switch E**

Verify the RERP configurations on Transit device of subring; key points: role of device, MAC address of Master device, and the state of primary and secondary ports.

```
SwitchE(config)#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f834.56f3
----------------------------------
region 1
ring                 : 2
rerp oper hello interval : 1
rerp oper fail  interval : 6
ring master           : 00d0.f822.3416
ctrl-vlan             : 4092
edge-vlan             :
role                 : transit
primary-port          : GigabitEthernet 0/1(forwarding)
secondary-port        : GigabitEthernet 0/2(forwarding)
```

Step 2: Disconnect the link between SwitchA and SwitchC (simulating that the non-public link on primary ring is failed), and then verify the RERP configurations on Master device of primary ring; key point: the state of primary and secondary ports of SwitchA.

```
SwitchA#show rerp
rerp state            : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge      : 00d0.f822.35ad
----------------------------------
region 1
ring                 : 1
```

```
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master            : 00d0.f822.35ad
ctrl-vlan              : 4091
edge-vlan              : 4092
role                  : master
primary-port           : GigabitEthernet 0/1(down)
secondary-port         : GigabitEthernet 0/2(forwarding)
```

Step 3: Restore the link between SwitchA and SwitchC and disconnect the link between SwitchB and SwitchC (simulating that the public link is failed), and then verify the RERP configurations on Master device.

1) Verify the RERP configurations on the Master device of primary ring; key point: state of primary and secondary ports of SwitchA (Master of primary ring).

```
SwitchA#show rerp
rerp state             : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 3(*1s)
rerp local bridge       : 00d0.f822.35ad
-----------------------------------
region 1
ring                  : 1
rerp oper hello interval : 1
rerp oper fail  interval : 3
ring master            : 00d0.f822.35ad
ctrl-vlan              : 4091
edge-vlan              : 4092
role                  : master
primary-port           : GigabitEthernet 0/1(forwarding)
secondary-port         : GigabitEthernet 0/2(forwarding)
```

From the above information, we can learn that the primary ring is failed, and the master device unblocks its secondary port which was blocked originally.

2) Verify the RERP configurations on the Master device of subring; key point: state of primary and secondary ports of SwitchD (Master of subring).

```
SwitchD#show rerp
rerp state             : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 6(*1s)
rerp local bridge       : 00d0.f822.3416
```

```
----------------------------------
region 1
ring                  : 2
rerp oper hello interval : 1
rerp oper fail  interval : 6
ring master            : 00d0.f822.3416
ctrl-vlan              : 4092
edge-vlan              :
role                  : master
primary-port           : GigabitEthernet 0/1(forwarding)
secondary-port         : GigabitEthernet 0/2(blocked)
```

From the above information, we can learn that the state of primary and secondary ports of subring master remains unchanged. The primary ring provides two backup links for the subring. When the public link fails, the subring can transmit data through another link provided by the primary ring. Therefore, there is no need to change the state of subring master.

Step 4: Restore the link between SwitchB and SwitchC and disconnect the link between SwitchC and SwitchE (simulating that the non-public link on subring is failed), and then verify the RERP configurations on Master device of subring; key point: the state of primary and secondary ports of SwitchD.

```
SwitchD#show rerp
rerp state             : enable
rerp admin hello interval: 1(*1s)
rerp admin fail interval : 6(*1s)
rerp local bridge       : 00d0.f822.3416
----------------------------------
region 1
ring                  : 2
rerp oper hello interval : 1
rerp oper fail  interval : 6
ring master            : 00d0.f822.3416
ctrl-vlan              : 4092
edge-vlan              :
role                  : master
primary-port           : GigabitEthernet 0/1(forwarding)
secondary-port         : GigabitEthernet 0/2(forwarding)
```

5.4.2.6 Notes for RERP configuration

1. Each ring can have only one Master (master device).
2. Each ring can have only one Backup (backup device), or no backup device.

3. The port joining RERP ring must be a Trunk port operating in full duplex mode. During practical application, we also need to configure the Control VLAN as the Native VLAN of Trunk port.

4. The primary and secondary ports of RERP do not support layer-3 interface or member port of AggregatePort. In addition, if the primary and secondary ports are further configured as routed ports or Aggregate member ports, the primary and secondary member ports will be removed.

5. Control VLAN is the VLAN specially used to exchange RERP information. For the security of ring network, the control VLAN must be a VLAN not created on the device, so as to avoid potential malicious attacks from outside network. The control VLAN cannot be configured to VLAN1 and VLAN4094.

6. Devices on the same RERP ring have the same Region ID, Ring ID and Control VLAN.

7. During actual configuration, the subring edge device or secondary-edge device must not be the master device of primary ring, namely the master device of primary ring must not be deployed on the intersecting point of two rings. If you configure the edge device as the master of primary ring and if its secondary port is connected to the public link, the public link will be blocked while the ring is complete.

8. In the circumstance of intersecting rings, the timeout interval of subring must be two times greater than the timeout interval of primary ring.

9. While modifying RERP configurations, you must first shut down a RERP port of one device on the ring to avoid a loop during this process, and then "no shutdown" this port after completing the modification.

6 REUP Configuration

6.1 REUP Overview

6.1.1 Understanding REUP

The Rapid Ethernet Uplink Protection protocol(REUP) protects Ethernet uplink rapidly.

Ports are configured in pair on the ends of an uplink, with one being active and the other being standby. When two ports are up, one of them is set to be backup. For details, refer to section Configure REUP Preemption Mode and Delay.

By default, the standby port is in backup status, which cannot forward packets. When the port in forward status is down, the backup port transfers to health status and forwards packets. Moreover, the REUP advertises address update messages to upstream devices for updating MAC address, so that data interruption can be restored in 50ms in case of a link failure.

The REUP and STP are mutually exclusive on a port. In this case, the STP runs on downstream and the REUP runs on upstream for uplink backup and problem protection. The REUP offers basic link redundancy even if the STP is disabled while enabling millisecond-level fault recovery.

6.1.2 Default REUP Configuration

The following table shows default REUP configuration:

Item	Default value
REUP	Disabled
Preemption mode	Off
Preemption delay	35 seconds
Mac update transit	Disable
Mac update receive	Disabled

6.1.3 REUP Configuration Guide

Before configuring the REUP, note that:

- A port belongs to only one REUP pair. Each active link has only one standby link and vice versa. The active link and the standby link must be different ports.
- The REUP supports Layer2 physical port and Layer2 AP port, not AP member port.
- The primary port can be of different type than the secondary port. So do their rates. For example, you can set the AP port as the primary port and the physical port as the secondary port.
- The STP is disabled on the port with the REUP enabled. The port with the REUP configured does not participate in STP. BPDU penetrate transmission is supported when the STP is disabled.
- A device can be configured with up to 16 REUP pairs and 8 address update groups. Each address update group has up to four member ports. A port belongs to only one address update group.
- It is necessary to disable modifying the attributes of a port after the REUP is configured successfully on it.

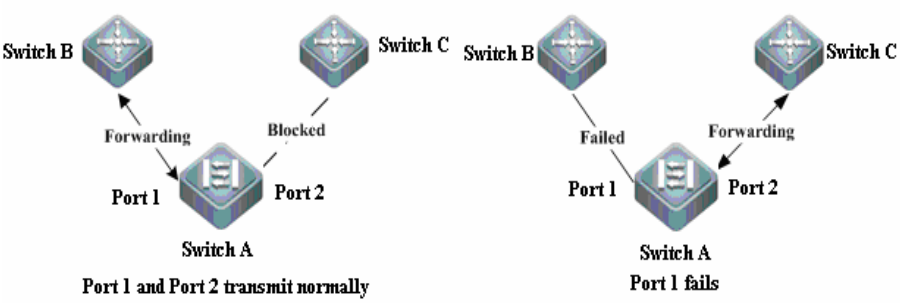
6.2 Configuring REUP

6.2.1 Configuring Dual Link Backup

You can configure a REUP pair by specifying one port as the standby port of another port. When two links are up, one is active (forwarding packets), and the other is standby (not forwarding packets). If the active link fails, the standby link becomes active and begins to forward packets. After the active link recovers from the fault, it becomes standby and does not forward any packets. Certainly, you can set the link recovered from the fault to preempt the currently active link.

As shown in Figure-1, for example, Switch A's port 1 and port 2 are connected to the upstream switches B and C. REUP is enabled on port 1 and port 2. Port 1 is active for forwarding packets; port 2 is backup. Switch C does not forward any packets from Switch A. Once port 1 fails, port 2 starts to forward packets. If port 1 recovers from the fault, it becomes backup.

Figure-1 REUP topology



In the privileged EXEC configuration mode, execute the following command to configure a REUP pair:

Command	Function
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config) # **interface** *interface-id*	Enter the interface configuration mode.
DES-7200 (config-if) # **switchport backup interface** *interface-id*	Configure a Layer 2 physical port or a layer 2 AP port as a backup port
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show interfaces** [*interface-id*] **switchport backup** [**detail**]	Show the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

For example:

```
DES-7200# configure

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)# interface gigabitEthernet 0/1

DES-7200(config-if)# switchport backup interface gigabitEthernet 0/2

DES-7200(config-if)# show interface switchport backup

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State

------------------------------------------------------------

GigabitEthernet 0/1     GigabitEthernet 0/2     Active Up/Backup Down
```

6.2.2 Configuring the Preemption Mode and Delay

By configuring the preemption mode, you can determine the best available link. for bandwidth mode, the REUP will uses a link of larger bandwidth. For forced mode, the REUP will forcibly use a reliable and stable link.

To avoid frequent active-standby link switching, you can define preemption delay. After two links recover, link switching occurs after the delay.

In the privileged Exec mode, execute the following commands to configure the preemption mode and delay:

Command	Function
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config) # **interface** *interface-id*	Enter the interface configuration mode.
DES-7200 (config-if) # **switchport backup interface** *interface-id*	Configure a Layer 2 physical port or a layer 2 AP port as a backup port.
DES-7200(config-if)# **switchport backup interface** *interface-id* **preemption mode** { **forced|bandwidth|off** }	Configure the preemption mode: Forced: The primary port always preempts the secondary port. Bandwidth: Use the port of higher bandwidth. Off: Disable preemption.
DES-7200(config-if)# **switchport backup interface** *interface-id* **preemption delay** *delay-time*	Configure preemption delay, which takes effect only in forced and bandwidth modes.
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show interfaces** [*interface-id*] **switchport backup** [**detail**]	Show the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

For example:

```
DES-7200# configure terminal

Enter configuration commands, one per line. End with CNTL/Z.

DES-7200 (config) # interface gigabitEthernet 0/1

DES-7200 (config-if) # switchport backup interface gigabitEthernet 0/2 preemption mode forced
```

```
DES-7200 (config-if) # switchport backup interface gigabitEthernet 0/2 preemption
delay 50

DES-7200 (config-if) # show interfaces switchport backup detail

Switch Backup Interface Pairs:

Active Interface        Backup Interface        State

------------------------------------------------------------

GigabitEthernet 0/1     GigabitEthernet 0/2     Active Up/Backup Down

Interface Pair : Gi0/1, Gi0/2

Preemption Mode : forced

Preemption Delay : 50 seconds

Bandwidth : Gi0/1(1000 Mbits), Gi0/2(10 Mbits)
```

Note

1. The bandwidth of an AP port is the number of its members whose link is up multiplying the speed of the members.
2. Once the STP is enabled on the uplink, the preemption delay should be larger than 35 seconds.

6.2.3 Configuring the VLAN Load Balancing

VLAN load balancing allows two ports of REUP pair to forward data packets of mutually exclusive VLANs, thus making maximum use of link bandwidth.

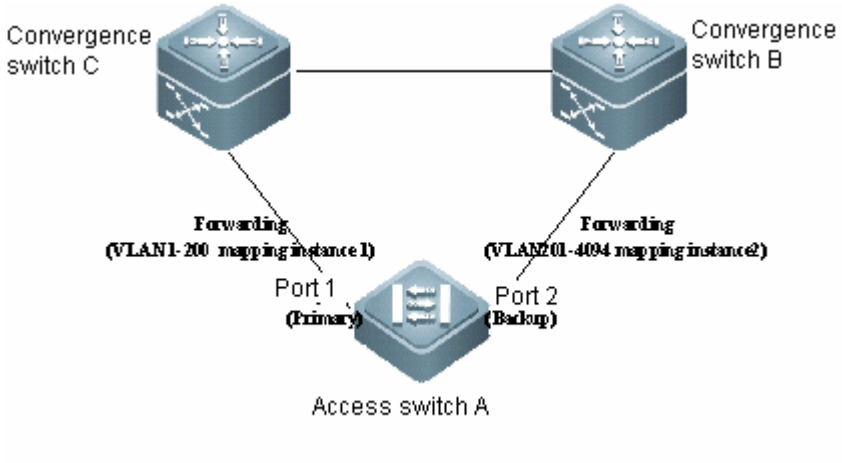


Fig 3 Topology in which both links for load balancing are normal

As shown in Fig 3: REUP is configured on Port 1 and Port 2 of Switch A; REUP VLAN load balancing is enabled to map VLAN 1-200 to instance 1 and other VLANs to

instance 2; the packets of VLAN 1-200 (instance 1) will be transmitted via Port 1, and packets of all other VLANs (instance 2) will be transmitted via Port 2.

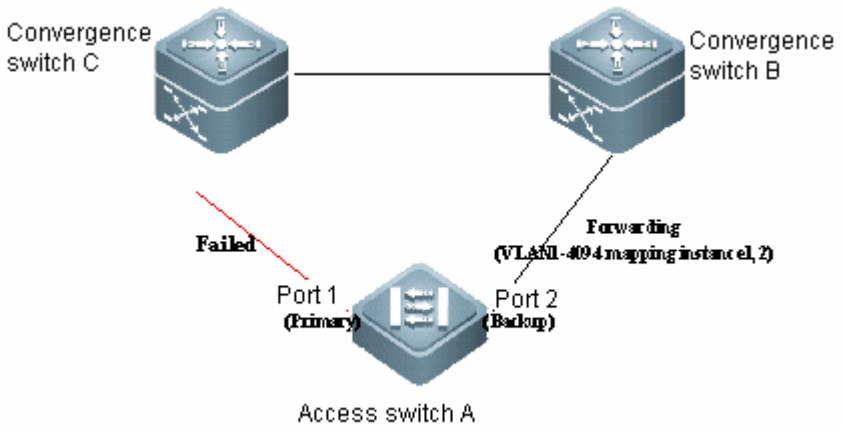


Fig 4 Topology in which one link for load balancing is failed

When one of the ports is failed, the other port will be responsible for forwarding packets of all VLANs. After the failed port has recovered and functions normally within the preemption delay, it will take over the packets of its responsible VLANs from another port.

In privileged mode, execute the following steps to configure REUP VLAN load balancing.

Command	Function
DES-7200# **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **switchport backup interface** *interface-id* **prefer instance** *standby-interface-instance-range*	Configure a layer-2 port as the backup port, and specify the packets of which VLAN mapping instance will be forwarded by the backup port.
DES-7200(config-if)# **end**	Return to privileged mode.
DES-7200# **show interface** [*interface-id*] **switchport backup**	Show the configurations.
DES-7200# **copy running-config startup-config**	Save configurations.

For example:

```
DES-7200# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200(config)#spanning-tree mst configuration
DES-7200(config-mst)#instance 1 vlan 1-200
```

```
DES-7200(config-mst)#exit
DES-7200(config)#show spanning-tree mst configuration
Multi spanning tree protocol : Enable
Name    :
Revision : 0
Instance  Vlans Mapped
-------- ---------------------------------------------
0       : 201-4094
1       : 1-200
-----------------------------------------------------
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# switchport backup interface gigabitEthernet 0/2 prefer
instance 1
DES-7200(config-if)# end
DES-7200# show interfaces switchport backup
DES-7200(config-if)#show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface        Backup Interface        State
------------------------------------------------------------------
GigabitEthernet 0/1   GigabitEthernet 0/2   Active Up/Backup Down

Instances Preferred on Active Interface:Instance 0,2-64
             Mapping VLAN 201-4094
Instances Preferred on Backup Interface:Instance 1
             Mapping VLAN 1-200
```

Note The instance mapping in REUP VLAN load balancing is centrally controlled by the MSTP module. For details about instance configuration, please refer to "MSTP Configuration Guide".

6.2.4 Configuring MAC Address Updating

6.2.4.1 Introduction to MAC Address Updating

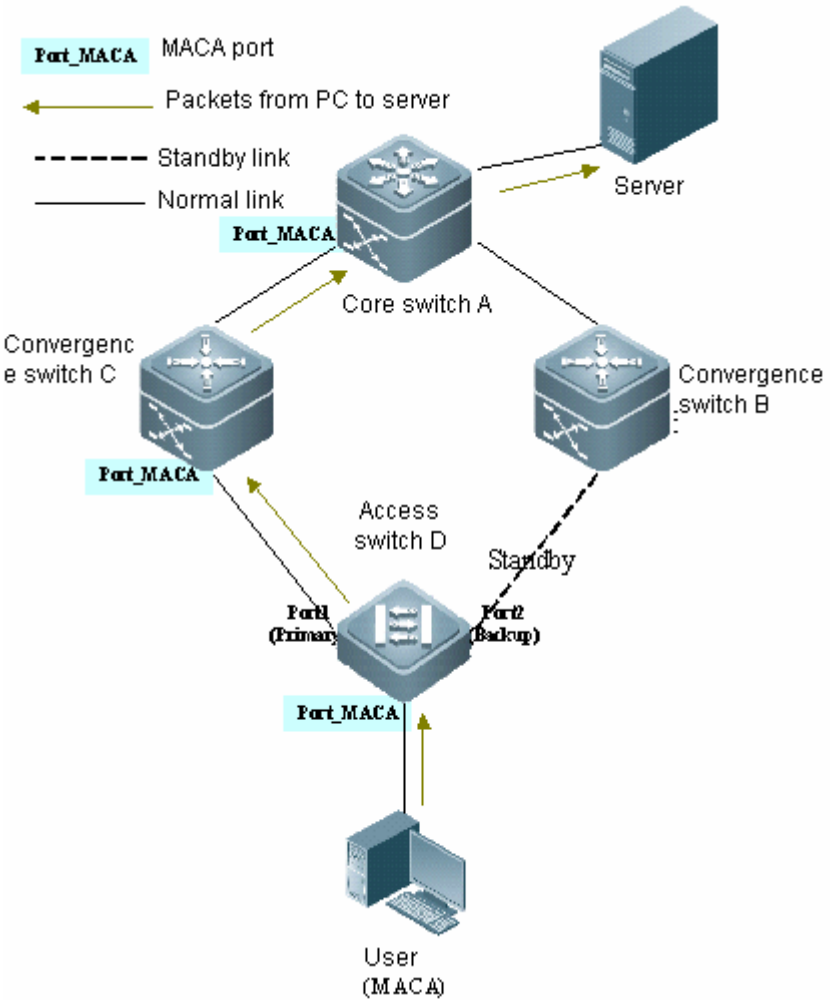


Fig 5 Normal working state of REUP

As shown in Fig 5, REUP dual-link backup is enabled on Gi0/1 and Gi0/2 of Switch D. Port Gi0/1 is the active port. During the process of normal communication, Switch A will learn the MAC address of PC from the port (Gi0/3) connected to Switch C.

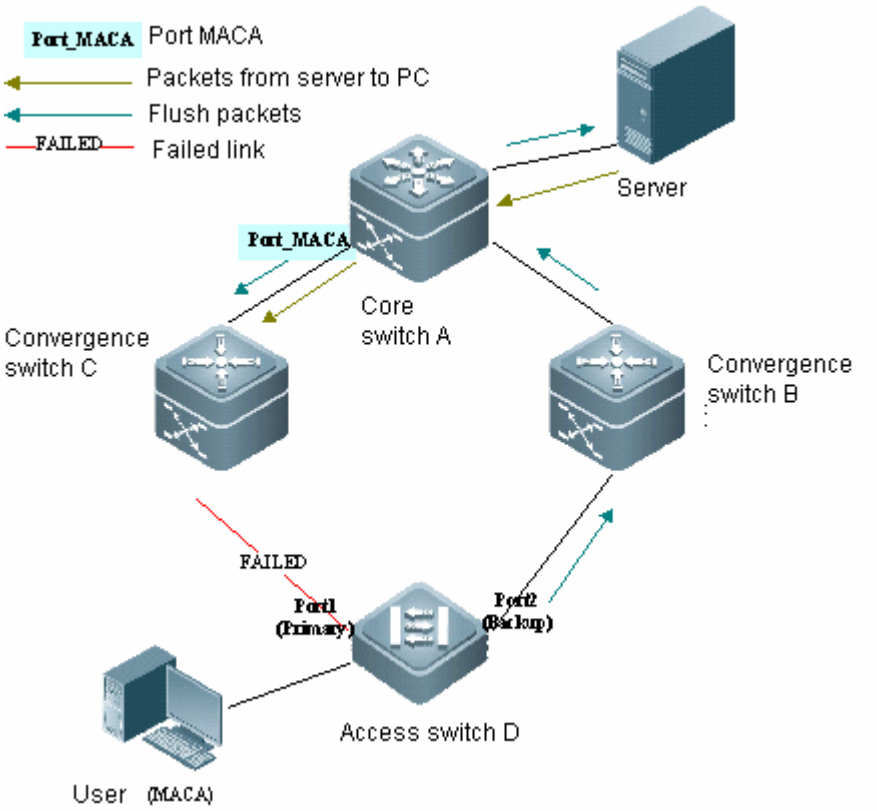


Fig 6 Failed state during the switchover

After port Gi0/1 of Switch D fails, port Gi0/2 will instantly become active and start to forward data packets. By this time, Switch A is temporarily unable to learn the MAC address of PC from port Gi0/4 connected to Switch B, and packets sent by the server to PC will be forwarded by Switch A to Switch C, causing packet loss.

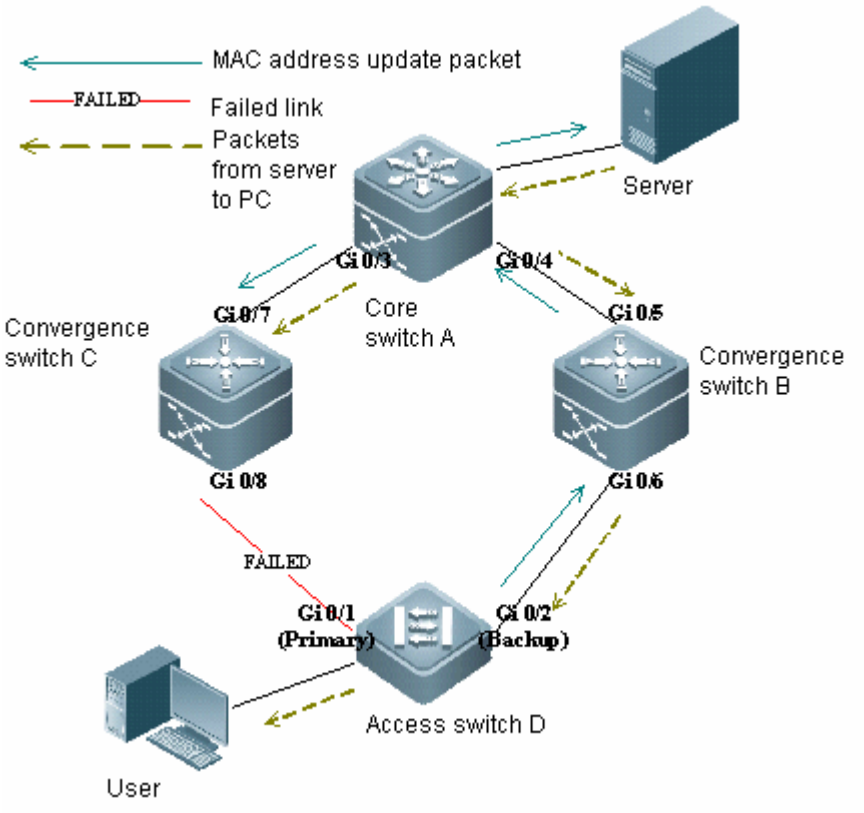


Fig 7 State after REUP sends MAC address updating message

To avoid the aforementioned defect, we need to enable MAC address updating on Switch D. While Gi0/2 starts to forward packets, Switch D will send MAC update message on Gi0/2. After Switch A receives such MAC address updating message, it will clear the MAC address on port Gi0/3, so that Switch A can forward the packets transmitted from server to PC to the port connected to Switch B, thus quickening the convergence of packet forwarding.

To reduce the side effect of flooding caused by MAC address updating, we have introduced the MAC address update group, which means that multiple ports will be included in the group. When one port in this group receives the MAC address updating message, it will update the MAC address information on other ports within this group.

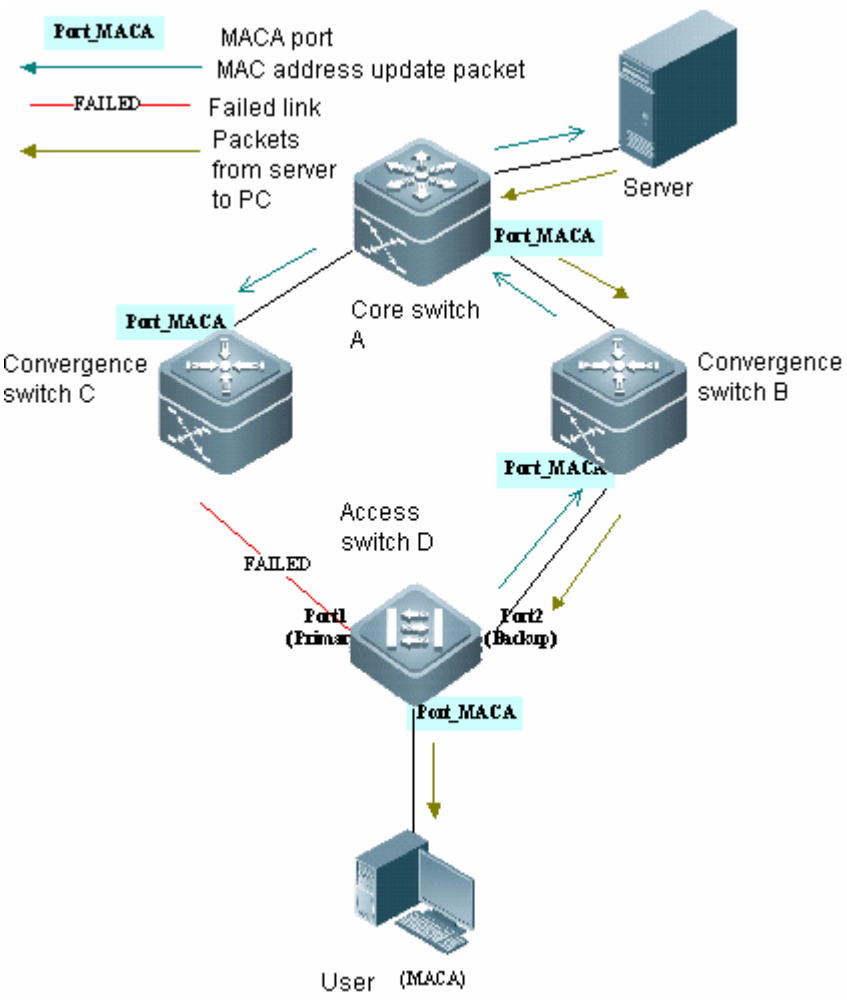


Fig 8 State after REUP sends MAC address updating packet

To support up-stream devices which don't support MAC address updating message, when Gi0/2 changes to forwarding state, Switch D will send MAC address updating packet on behalf of user PC, so that Switch A can update the MAC address of user PC to Gi0/4, thus recovering downlink data transmission on Switch A.

6.2.4.2 Configuring MAC Address Updating

To enable the MAC address updating function, enable the function of sending MAC address message on the switch.

In the privileged EXEC configuration mode, follow these steps to function of sending MAC address message on the switch:

Command	Function
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config) # **mac-address-table move update transit**	Enable the function of sending the MAC address updating message.

DES-7200(config)# **mac-address-table move update max-update-rate** *pkts-per-second*	(Optional) Configure the maximum number of MAC address updating packets sent per second. Range: 0-32000; default: 150.
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **mac-address-table move update transit vlan** *vlanid*	(Optional) Configure the VID for the interface to send MAC address update message. By default, MAC address updating message is sent in the default VLAN of port.
DES-7200(config-if)# **end**	Return to privileged mode.
DES-7200# **show mac-address-table move update**	Show the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

Meanwhile, enable all switches on the switched path to receive MAC address updating messages, and join all ports on the switched path to the same MAC address updating group.

In privileged mode, execute the following steps to enable the switch to receive MAC address updating message and address updating group.

Command	**Function**
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200 (config) # **mac-address-table move update receive**	Enable the function of receiving the MAC address updating message.
DES-7200(config)# **no mac-address-table move update receive vlan** *vlan-range*	(Optional) Configure the VLAN range for the device to handle MAC address updating message. By default, MAC address updating message is handled in all VLANs.
DES-7200(config)# **interface** *interface-id*	Etner the interface configuration mode.
DES-7200(config-if)# **mac-address-table update group** [*number*]	Add the port to the MAC address updating group. By default, add the port to the first MAC address updating group.
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show mac-address-table update group**	Show the configuration.
DES-7200# **copy running-config startup-config**	Save the configuration.

For example, as shown in Fig 5, enable the REUP dual link backup function on port 1 and port 2 of switch D.

```
DES-7200 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200 (config)# interface gigabitEthernet0/1
DES-7200 (config-if)# switchport backup interface gigabitEthernet 0/2
DES-7200 (config-if)# end
DES-7200 # show interface switchport backup detail
Switch Backup Interface Pairs:
Active Interface      Backup Interface      State
GigabitEthernet 0/1   GigabitEthernet 0/2   Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : off
Preemption Delay : 35 seconds
Bandwidth : 100000 Kbit (Gi0/1), 100000 Kbit (Gi0/2)
```

Enable the function of sending the MAC address updating on Switch D.

```
DES-7200 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200 (config)# mac-address-table move update transit
DES-7200 (config)# end
DES-7200 # show mac-address-table move update
Mac address table move update status:
Transit:enable
Receive:disable
Pair: Gi0/2,Gi0/1
Members            Status    Transit Count    Last Transit Time
-----------------------------------------------------------------
Gi0/2              Up        0
Gi0/1              Down      0
```

Enable the function of receiving the MAC address updating message on Switches B, C and A, and add all ports on the switched path to the same MAC address updating group.

Apply the following configurations on Switch A

```
DES-7200 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200 (config)# mac-address-table move update receive
DES-7200 (config)# interface range gigabitEthernet 0/3-4
DES-7200 (config-if-range)# mac-address-table update group
DES-7200 (config-if-range)# end
DES-7200 # show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:0
Group member  Receive Count   Last Receive Switch-ID   Receive Time
------------------------------------------------------------
Gi0/3              0               0000.0000.0000
Gi0/4              0               0000.0000.0000
```

Apply the following configurations on Switch B:

```
DES-7200 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200 (config)# mac-address-table move update receive
DES-7200 (config)# interface range gigabitEthernet 0/5-6
DES-7200 (config-if-range)# mac-address-table update group
DES-7200 (config-if-range)# end
```

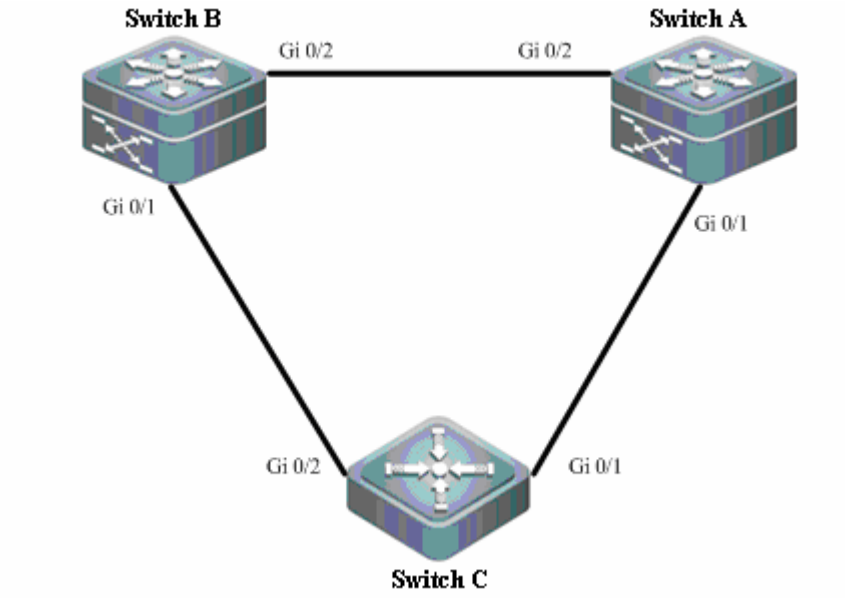
Apply the following configurations on Switch C:

```
DES-7200 # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
DES-7200 (config)# mac-address-table move update receive
DES-7200 (config)# interface range gigabitEthernet 0/7-8
DES-7200 (config-if-range)# mac-address-table update group
```

```
DES-7200 (config-if-range)# end
```

6.2.4.3 Typical REUP Applications

Figure-5 Typical REUP application topology



As shown in the above figure, Switch C connects to Switch A and Switch B through Gi0/1 and GI0/2. To enable rapid bi-directional convergence, enable the dual link backup function on Switch C, enable the function of receiving the MAC address updating message on Switch A and Switch B, and add the ports along the switching path to the MAC address updating group.

Configuration on Switch C:

```
DES-7200 # configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)# interface gigabitEthernet 0/1

DES-7200(config-if)# switchport backup interface gigabitEthernet 0/2

DES-7200(config-if)# exit

DES-7200(config)# mac-address-table move update transit

DES-7200(config)# end

DES-7200# show mac-address-table move update

Mac address table move update status:

Transit:enable

Receive:disable
```

```
Pair: Gi0/1,Gi0/2

Members            Status    Transit Count    Last Transit Time

-----------------------------------------------------------

Gi0/1              Standby   0

Gi0/2              Up        1                Wed Aug 20 10:51:34 2008
```

Configuration on Switch A and Switch B:

```
DES-7200 # configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

DES-7200(config)# mac-address-table move update receive

DES-7200(config)# interface range gigabitEthernet 0/1 - 2

DES-7200(config-if-range)# mac-address-table update group

DES-7200(config-if-range)# end

DES-7200# show mac-address-table update group detail

Mac-address-table Update Group:1

Received mac-address-table update message count:0

Group member        Receive Count    Last Receive Switch-ID      Receive Time

-----------------------------------------------------------

Gi0/1               0                0000.0000.0000

Gi0/2               0                0000.0000.0000
```

6.3 Configuring Link State Tracking

With Link State Tracking, when upstream links have failed, the downstream devices can be advertised to switch over the link. By configuring upstream ports and downstream ports of link state tracking group, Link State Tracking binds the link state of multiple downstream ports to multiple upstream ports. When all upstream links in the tracking group have failed, the downstream ports will be shut down, so that the packet transmission over upstream link can be switched from primary link to the backup link.

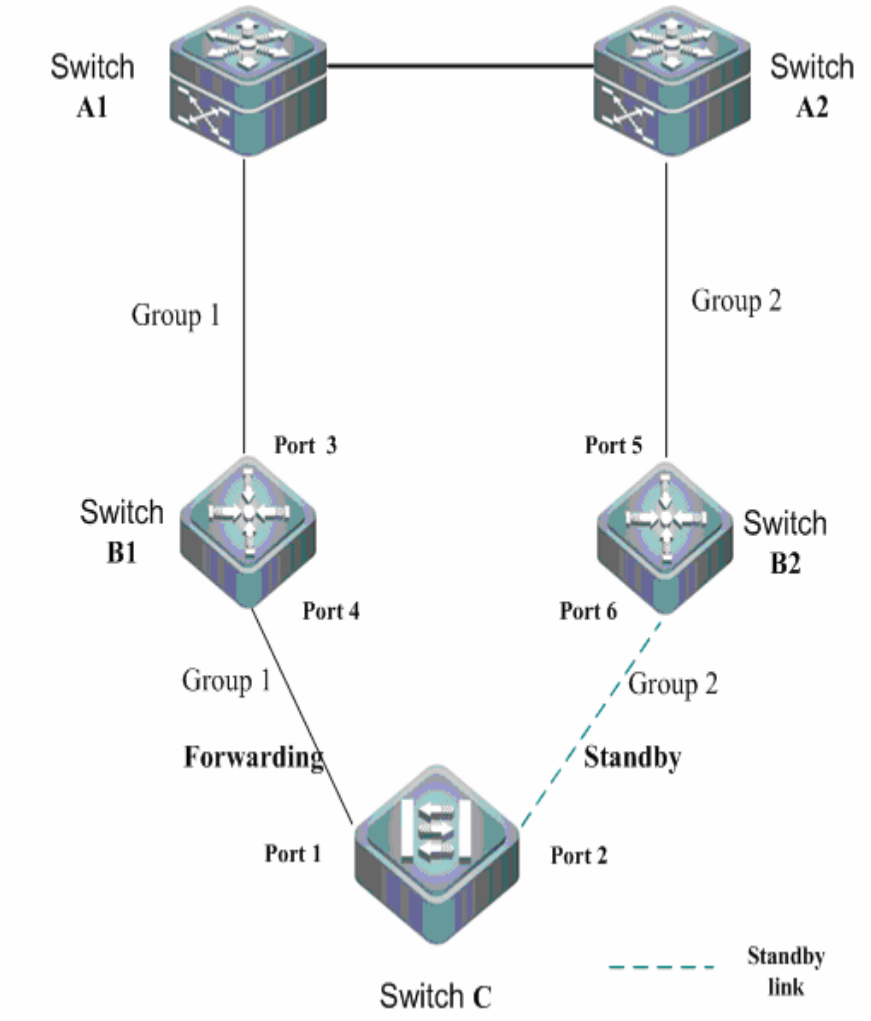


Fig 10 Link state tracking configuration example

As shown in Fig 10: port 4 of Switch B1 is configured as the downstream port of group 1, and port 3 is configured as the upstream port; port 6 of Switch B2 is configured as the downstream port of group 2, and port 5 is configured as the upstream port; REUP dual-link backup is enabled on port 1 and port 2 of Switch C.

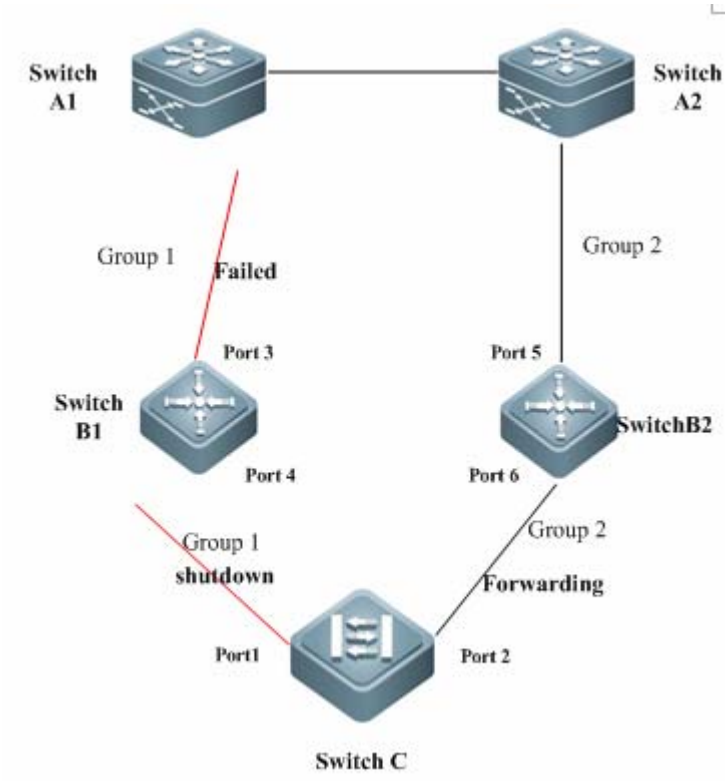


Fig 11 Topology in which the upstream links on primary link are failed

When upstream link of Switch B1 is failed, Link State Tracking will instantly shut down the downstream port 4, so that the packet transmission on the upstream link of Switch C can be switched to Switch B2.

In privileged mode, execute the following steps to configure Link State Tracking.

Command	Function
DES-7200 # **configure terminal**	Enter the global configuration mode.
DES-7200(config)# **link state track** [*number*]	Enable a link state group. The range of "number" is 1-2. By default, the first link state group will be enabled (default number is 1).
DES-7200(config)# **interface** *interface-id*	Enter the interface configuration mode.
DES-7200(config-if)# **link state group** [*number*] {**upstream** | **downstream**}	Configure the upstream ports and downstream ports of link state group. The range of "number" is 1-2. By default, the first link state group will be joined (default number is 1).
DES-7200(config-if)# **end**	Return to the privileged mode.
DES-7200# **show mac-address-table update group**	Show the configuration.

DES-7200# **copy running-config startup-config**	Save the configuration.

For example: On Switch B1, configure port 4 as the downstream port and port 3 as the upstream port of link state group 1.

```
DES-7200# configure terminal
DES-7200(config)# link state track 1
DES-7200config)# interface fastethernet 0/4
DES-7200(config-if)# link state group 1 downstream
DES-7200(config)# exit
DES-7200(config-if)# interface fastethernet 0/3
DES-7200(config-if)# link state group 1 upstream
DES-7200(config-if)# end
```

Verify the state of Link State Group.

```
DES-7200# show link state group detail
Link State Group:1  Status: Enabled, UP
Upstream Interfaces :Gi0/3(Up)
Downstream Interfaces : Gi0/4(Up)
Link State Group:2  Status: Disabled, Down
Upstream Interfaces :
Downstream Interfaces :
(Up):Interface up  (Dwn):Interface Down  (Dis):Interface disabled
```

6.4 REUP Configuration Example

6.4.1 Topological Diagram

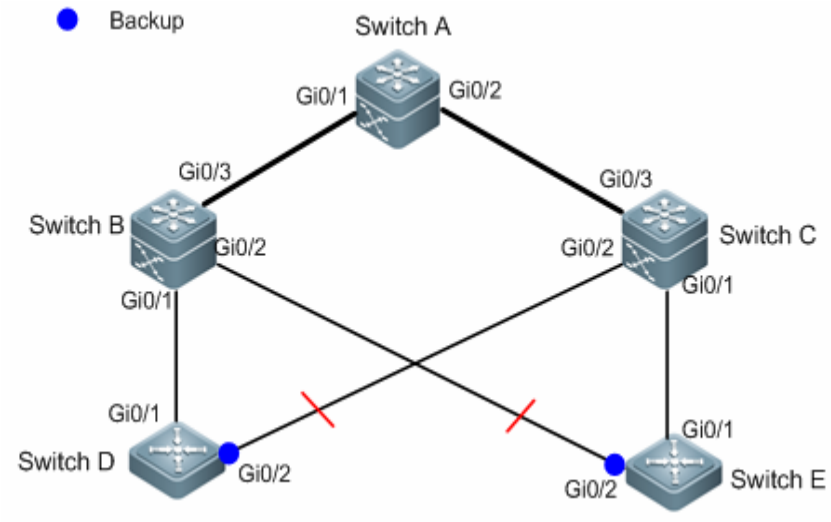


Fig 12 Topological diagram for REUP configuration

6.4.2 Application Requirements

When downstream devices are connected to upstream devices, service interruption may be easily caused by the single point failure on the single upstream link. Generally, dual upstream links are used. One downstream device (Switch D/E) is connected to two upstream devices (Switch B and Switch C) to furthest avoid single point failure and enhance network reliability. The specific requirements are shown below:

1. Downstream devices (Switch D/E) reach the upstream device (Switch A) through two upstream links to realize redundant backup of the link.
2. Downstream devices (Switch D/E) shall allow rapid bidirectional convergence in the case of link failure.
3. G0/2 of Switch E is a 100M interface, and G0/1 is a 1000M interface. When the failed link is restored, the upstream link with greater bandwidth shall be selected.

6.4.3 Configuration Tips

Applying REUP will meet all the above application needs:

1. Configure REUP dual-link backup on downstream devices (Switch D/E) to allow redundant backup of the primary link and backup link.
2. Configure REUP MAC address update on the corresponding devices to achieve rapid bidirectional convergence of the network: enable the downstream devices (Switch D/E) to send MAC address update messages; enable the upstream devices (Switch A/B/C) to receive MAC address update messages and join all ports into the same address update group.
3. Configure REUP preemption mode to enable the priority use of upstream link with greater bandwidth.

6.4.4 Configuration Steps

Trunk links are used to connect devices. For interface related configurations, please refer to "Interface Configuration" section in this manual.

- Configurations on Switch D

Step 1: Configure REUP pair (Gi0/1 is the primary port and Gi0/2 is the secondary port)

```
SwitchD > enable
SwitchD # configure terminal
SwitchD (config)# interface GigabitEthernet 0/1
SwitchD(config-if-GigabitEthernet 0/1)# switchport mode trunk
```

```
SwitchD(config-if-GigabitEthernet 0/1)#switchport backup interface
GigabitEthernet 0/2
SwitchD(config-if-GigabitEthernet 0/1)# exit
```

Step 2: Enable Switch D to send MAC address update message

```
SwitchD (config)# mac-address-table move update transit
```

- Configurations on Switch E

Step 1: Configure REUP pair (port 1 is the primary port and port 2 is the secondary port)

```
SwitchE> enable
SwitchE # configure terminal
SwitchE (config)# interface GigabitEthernet 0/1
SwitchE (config-if-GigabitEthernet 0/1)# switchport mode trunk
SwitchE (config-if-GigabitEthernet 0/1)# switchport backup interface
GigabitEthernet 0/2
```

Step 3: Configure preemption mode

! Configure preemption mode as bandwidth mode

```
SwitchE (config-if-GigabitEthernet 0/1)# switchport backup interface
gigabitEthernet 0/2 preemption mode bandwidth
```

! Configure preemption delay as 40 seconds

```
SwitchE (config-if-GigabitEthernet 0/1)# switchport backup interface
gigabitEthernet 0/2 preemption delay 40
SwitchE (config-if-GigabitEthernet 0/1)# exit
```

Step 2: Enable Switch E to send MAC address update message

```
DES-7200(config)# mac-address-table move update transmit
```

- Configurations on Switch B

Step 1: Enable Switch B to send MAC address update message

```
SwitchB # configure terminal
SwitchB (config)# mac-address-table move update receive
```

Step 2: Join all ports on REUP switched path to the same MAC address update group

In this example, Gi0/1 and Gi0/3 are interfaces on the upstream switched path of SwitchD, and Gi0/3 and Gi0/2 are interfaces on the upstream switched path of SwitchE. Since one interface can only join one address update group, we can join Gi0/1, Gi0/2 and Gi0/3 into the same address update group.

```
DES-7200(config)# interface range gigabitEthernet 0/1 – 3
SwitchB(config-if-range)#switchport mode trunk
SwitchB (config-if-range)# mac-address-table update group 1
SwitchB (config-if-range)# end
```

- Configurations on Switch C

Same as the configurations on Switch B.

- Configurations on Switch A

Step 1: Enable Switch A to send MAC address update message

```
SwitchA # configure terminal
SwitchA (config)# mac-address-table move update receive
```

Step 2: Join all ports on REUP switched path to the same MAC address update group

```
SwitchA (config)# interface range gigabitEthernet 0/1 – 2
SwitchA (config-if-range)# switchport mode trunk
SwitchA (config-if-range)# mac-address-table update group 1
SwitchA (config-if-range)# end
```

6.4.5 Verify configurations

- Displaying REUP configurations on Switch D

Step 1: Display the dual-link backup state of ports on Switch D

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface     State
----------------   ----------------   --------------------
Gi4/1              Gi4/2             Active Up/Backup Standby
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off                       //REUP preemption mode is
disabled
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)
```

As shown above, when links function normally (both primary and secondary ports of Switch D are Link Up), the secondary port of Switch D will maintain Standby state.

Step 2: Disconnect the uplink on the primary port of Switch D and then verify device state

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface     State
----------------   ----------------   --------------------
```

```
Gi4/1             Gi4/2            Active down/Backup up
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)
```

As shown above, when the uplink on primary port of Switch D is failed, the backup port will switch to forwarding state (UP) to transmit packets.

Step 3: Restore the uplink on the primary port of Switch D and then verify device state

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface     State
---------------   ---------------   --------------------
Gi4/1             Gi4/2            Active Standby /Backup up
Interface Pair : Gi4/1, Gi4/2
Preemption Mode : Off
Preemption Delay : 35 seconds
Bandwidth : Gi4/1(1000 Mbits), Gi4/2(1000 Mbits)
```

As shown above, since REUP preemption mode hasn't been configured on Switch D, when the uplink on primary port is restored, the secondary port will still maintain forwarding state and the primary port will go into standby state.

- Displaying REUP configurations on Switch E

Step 1: Display the dual-link backup state of ports on Switch E

```
SwitchE#show interfaces switchport backup detail
Switch Backup Interface Pairs:
Active Interface   Backup Interface     State
---------------   ---------------   --------------------
Gi4/1             Gi4/2            Active Up/Backup Standby

Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth            //REUP bandwidth based preemption mode
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

As shown above, when links function normally (both primary and secondary ports of Switch E are Link Up), the secondary port of Switch E will maintain Standby state.

Step 2: Disconnect the uplink on the primary port of Switch E and then verify device state

```
SwitchD#show interfaces switchport backup detail
Switch Backup Interface Pairs:
```

```
Active Interface   Backup Interface     State
---------------   ---------------   --------------------
Gi0/1             Gi0/2             Active down/Backup up
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

As shown above, when the uplink on primary port of Switch E is failed, the backup port will switch to forwarding state (UP) to transmit packets.

Step 3: Restore the uplink on the primary port of Switch D and then verify device state

After the uplink is restored and before the delay time runs out, immediately verify the dual-link backup state of device. The primary port goes into Standby state, and the secondary port remains in forwarding state, as shown below:

```
SwitchE#show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface    Backup Interface    State
----------------   ----------------  -----------------
Gi0/1                Gi0/2            Active Standby/Backup Up
```

After the 40-second delay time runs out, CLI will print the following LOG information:

```
*Apr 14 22:08:45: %REUP_INTF-5-PREEMPT: Preempting interface Gi0/2 in reup
pair (Gi0/1, Gi0/2), preemption mode is bandwidth
```

Verify the dual-link backup state of device again. Sicne REUP bandwidth based preemption mode is configured, REUP will preempt the link with greater bandwidth (namely the uplink on Gi0/1).

```
SwitchE#show interfaces switchport backup
Switch Backup Interface Pairs:
Active Interface   Backup Interface     State
---------------   ---------------   --------------------
Gi0/1             Gi0/2             Active Up/Backup Standby
Interface Pair : Gi0/1, Gi0/2
Preemption Mode : bandwidth
Preemption Delay : 40 seconds
Bandwidth : Gi0/1(1000 Mbits), Gi0/2(100 Mbits)
```

- Displaying REUP configurations on the upstream devices

Display information about MAC address update group on Switch A

```
SwitchA#show mac-address-table update group detail
Mac-address-table Update Group:1
Received mac-address-table update message count:5
```

```
Group member Receive Count  Last Receive Switch-ID   Receive Time
-----------  --------      --------------------    ----------
Gi0/1         2        00d0.f822.35aa   Thu Aug 20 13:42:16 2009
Gi0/2         3        00d0.f822.33ad   Thu Aug 20 13:43:55 2009
```

Display information about MAC address update group on Switch B

```
SwitchB#show mac-address-table update group detail

Mac-address-table Update Group:1
Received mac-address-table update message count:5
Group member Receive Count  Last Receive Switch-ID   Receive Time
-----------  --------      --------------------    ----------
Gi0/1          1        00d0.f822.35ad   Thu Aug  20 13:43:50 2009
Gi0/2          1        00d0.f822.33aa   Thu Aug  20 13:42:44 2009
Gi0/3          3        00d0.f822.35ad   Thu Aug  20 13:43:32 2009
```

Display information about MAC address update group on Switch C

```
SwitchC#show mac-address-table update group detail

Mac-address-table Update Group:1
Received mac-address-table update message count:6
Group member Receive Count  Last Receive Switch-ID   Receive Time
-----------  --------      --------------------    ----------
Gi0/1          1        00d0.f822.35aa   Thu Aug  20 13:43:51 2009
Gi0/2          1        00d0.f822.33ad   Thu Aug  20 13:42:43 2009
Gi0/3          3        00d0.f822.35aa   Thu Aug  20 13:43:31 2009
```

7 RLDP Configuration

7.1 RLDP Overview

7.1.1 Understanding RLDP

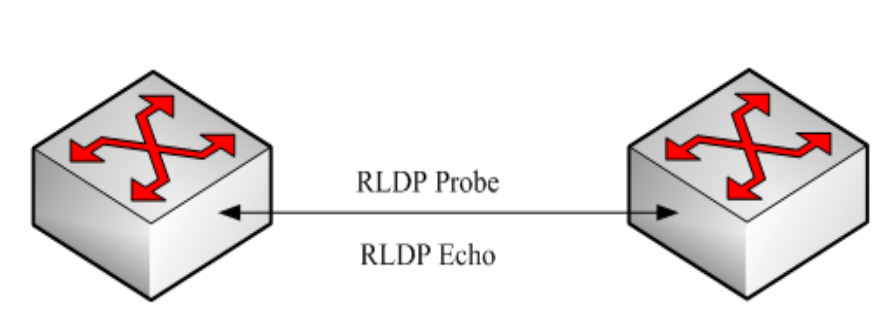
The Rapid Link Detection Protocol (RLDP) is one of DES-7200's proprietary link protocol designed to detect Ethernet link fault quickly.

General Ethernet link detection mechanism only makes use of the status of the physical connections and detects the connectivity of the link via the auto-negotiation of the physical layer. This detection mechanism has restrictions and sometimes cannot provide reliable link detection information for the user. For example, if the optical fiber receiving line pair on the optical interface is misconnected, due to the existence of the optical converter, the related port of the device is "linkup" physically but actually the corresponding layer-2 link cannot work for communications. Here is another example. There is an intermediate network between two Ethernet devices. Due to the existence of the network transmission relay devices, the same problem may occur if those relay devices are faulty.

The RLDP enables easy detection of Ethernet device link fault, including the one-way link fault, two-way link fault and loop link fault.

The RLDP implements the detection by exchanging the RLDP messages at the two ends of the link, as shown in Figure-1:

Figure-1:



The RLDP defines two protocol messages: Probe message and Echo message. The RLDP sends the Probe message of this port to the port with RLDP

configured and in linkup status on regular basis, and waits for the Echo message from the neighbor port and waits for the Probe message sent by the neighbor ports. If a link is correct both physically and logically, a port shall be able to receive the Echo message of the neighbor port as well as the Probe message of the neighbor port. Otherwise, the link is considered abnormal.

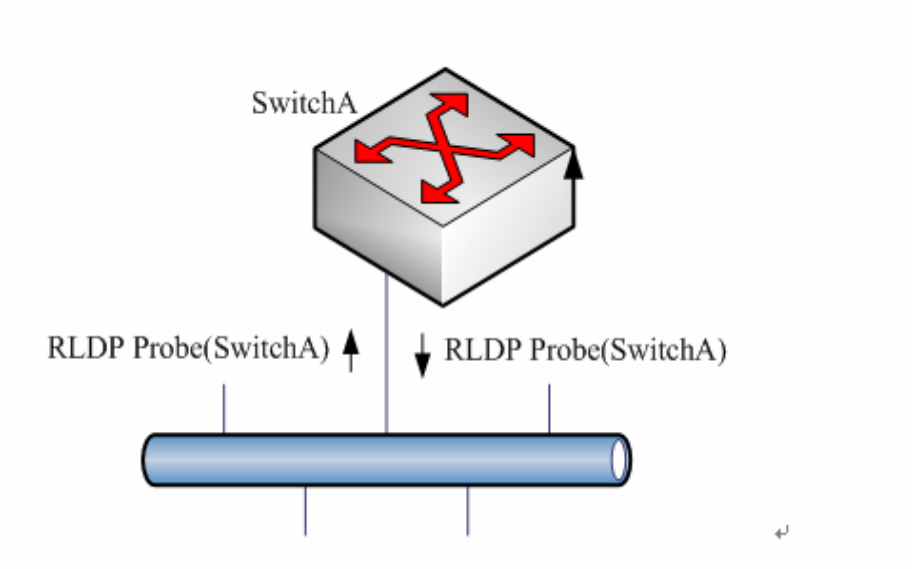
Note

To make use of the one-way detection and two-way detection functions of the RLDP, it is necessary to ensure the RLDP is enabled on the ports at both ends of the link. And, it is not allowed for a port with RLDP enabled to connect multiple neighbor ports. Otherwise, the RLDP cannot detect the health conditions of every neighbor link.

7.1.2 Typical Application

Loop detection:

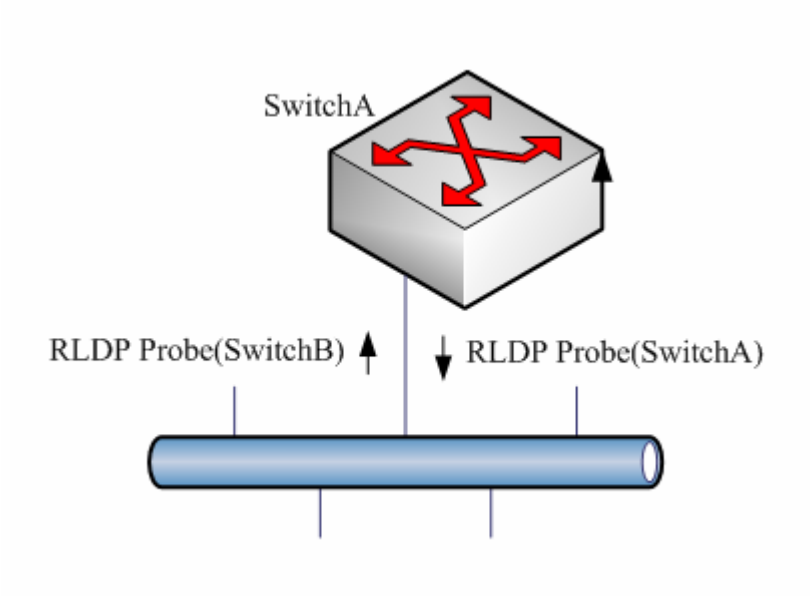
Figure-2: Loop detection



The so-called loop fault means that a loop appears on the links connected with the port. A shown above, on a port the RLDP receives the RLDP message sent from its machine, so the port is considered as loop fault. So, the RLDP deals with the fault according to the user configurations, including alarming, setting port violation, turning off the SVI with that port, turning off the port learning forwarding, and more.

One-way link detection:

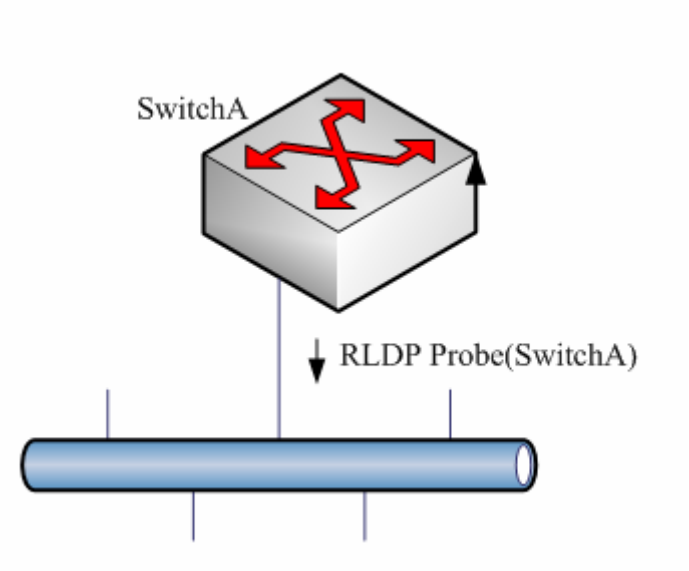
Figure-3: One-way link detection



The so-called one-way link detection means the link connected with the port can receive message only or send messages only (due to misconnection of the optical receiving line pair, for example). As shown above, the RLDP only receives the detection message from the neighbor port on a port, so it is considered one-way link fault. So, the RLDP deals with the fault accordingly according to the user configurations. In addition, if the port cannot receive any RLDP detection message, it is also considered one-way link fault.

Two-way link detection:

Figure-4：Two-way link detection



This means that fault occurs at the frame transmission/receiving at both ends of the link. As shown above, the port of the device sends the RLDP probe message but has never received the Echo message or the Probe message from

the neighbors. So, it is considered two-way link fault. From the nature of the fault, the two-way fault actually includes the one-way fault.

Note

If the party at one of the two link ends has not enabled the RLDP, the diagnosis also shows two-way or one-way link fault. So, in configuring two-way link detection or one-way link detection, the administrator shall make sure that the RLDP is enabled at both ends to avoid the incorrect diagnosis information.

7.2 Configuring RLDP

The following sections describe how to configure RLDP.

- RLDP defaults
- Configure global RLDP
- Configure port RLDP
- Configure RLDP detection interval
- Configure the RLDP maximum detection times
- Restore the RLDP status of the port

7.2.1 RLDP defaults

Global RLDP status	DISABLE
Port RLDP status	DISABLE
Detection interval	2S
Maximum detection times	3

Caution

- The RLDP can be configured only on the basis of the switching interface (including AP) and the routing interface.
- All RLDP frames are untagged.
- In the RLDP fault processing type, the block function and the STP are mutually exclusive. In other words, if the fault processing type configured on the port is "block", it is recommended to disable STP; otherwise, since the STP cannot recognize one-way link, possibly the STP allows port forwarding but the RLDP is configured with port blocking.

7.2.2 Configuring RLDP Globally

The RLDP works on the port only when the global RLDP is enabled.

In the global configuration mode, follow these steps to enable RLDP:

Command	Function
DES-7200(config)# **rldp enable**	Turn on the global RLDP function switch.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command turns off the global *RLDP*.

7.2.3 Configuring RLDP on the Port

The RLDP operation is port-based, so the user needs to explicitly configure which ports shall run RLDP. In configuring the port RLDP, it is required to specify the diagnosis type and the troubleshooting method for the port at the same time. The diagnosis types include unidirection-detect, bidirection-detect and loop-detect. The troubleshooting methods include warning, block, shutdown-port, and shutdown-svi.

In the configuration mode, follow these steps to configure the RLDP on the port:

Command	Function
DES-7200(config)# **interface** *interface-id*	Enter the interface mode.
DES-7200(config-if)# **rldp port** {**unidirection-detect** | **bidirection-detect** | **loop-detect** } {**warning** | **shutdown-svi** | **shutdown-port** | **block**}	Enable the RLDP on the port and configure the diagnosis type and troubleshooting method at the same time.
DES-7200(config-if)# **end**	Return to the privileged mode.

The **no** option of the command disables the RLDP on the port and the configured detection types one by one.

In the example below, the RLDP is configured on GigabitEthernet 0/5, and multiple diagnosis types and troubleshooting methods are specified:

```
DES-7200# configure terminal
DES-7200(config)# interface gigabitEthernet 0/5
DES-7200(config-if)# rldp port unidirection-detect
shutdown-svi
DES-7200(config-if)# rldp port bidirection-detect warning
```

```
DES-7200(config-if)# rldp port loop-detect block
DES-7200(config-if)# end
DES-7200# show rldp interface gigabitEthernet 0/5
port state     : normal
local bridge   : 00d0.f822.33ac
neighbor bridge : 0000.0000.0000
neighbor port  :
unidirection detect information:
action : shutdown svi
state  :  normal
bidirection detect information :
action : warnning
state  :  normal
loop detect  information    :
action : block
state  :  normal
```

Several precautions in configuring port detection:

- The routing interface does not support the shutdown-svi error handling method, so this method is not executed in case of the occurring of detection error.
- In configuring loop detection, the neighbor devices downward connected with the port cannot enable the RLDP detection; otherwise, the port cannot have correct detection.
- If the block method is configured on the aggregated port and the link detection error happens, do not change the member port relations of the aggregate port before the port reset detection; otherwise, the forwarding status of the member interface may have unexpected effects of forwarding status.
- If the RLDP detects link error, alarm information will be given. The user can send the alarm information to the log server by configuring the log function. At least 3 levels of log shall be ensured.
- You are recommended to specify the diagnosis type of the loop detection to shutdown-port for the reason that for some devices, even if the device detects the loop and specifies the block port, a large amount of packets will be sent to the CPU for the hardware chip limitation.

7.2.4 Configuring RLDP Detection Interval

The port with the RLDP function enabled will send the RLDP Probe messages on a regular basis.

In the global configuration mode, follow these steps to configure the RERP detection interval:

Command	Function
DES-7200(config)# **rldp detect-interval** interval	Configure the detection interval within the range 2-15s, 3s by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

7.2.5 Configuring the Maximum RLDP Detection Times

If the port with RLDP enabled cannot receive messages from neighbors in the maximum detection period (maximum detection times X detection interval), that port will be diagnosed as faulty. See the Overview for details of the fault types.

In the global configuration mode, follow these steps to configure the RERP maximum detection times:

Command	Function
DES-7200(config)# **rldp detect-max** Num	Configure the maximum detection times, num range 2-10, 2 by default.
DES-7200(config)# **end**	Return to the privileged mode.

The **no** option of the command restores the value to its default.

Note The maximum detection times only take effect in the unidirectional link detection and bidirectional link detection, and will not take effect if only loop detection is enabled on a port.

7.2.6 Restoring the RLDP Status of the Port

The port with shutdown-port troubleshooting method configured cannot resume the RLDP detection actively after a fault occurs. If the user confirms the fault removed, run the recovery command to restart the RLDP on the shutdown port. This command sometimes may make the other ports with detection errors resume.

In the privileged mode, follow these steps to resume the RLDP detection of the port:

Command	Function
DES-7200# **rldp reset**	Make any port with RLDP detection failure resume the detection.

Note

The **errdisable recover** command can be used in the global configuration mode to restart, instantly or at fixed time, the RLDP detection of the port that is set violation by RLDP. It is worth mentioning that when there are some relay devices between rldp ports, if you use **errdisable recover interval** to restore the fault timely, you need to set the value of rldp detection time greater than that of **errdisable recover interval**, that is, the value of detect-interval* detect-max total time is greater than that of **errdisable recover interval** to prevent error judgment.

7.3 Viewing RLDP Information

The following RLDP-related information can be viewed:

- View the RLDP status of all ports
- View the RLDP status of the specified port

7.3.1 Viewing the RLDP Status of All Ports

In the privileged mode, run the following commands to view the RLDP global configuration and the port detection information with RLDP detection configured:

Command	Function
DES-7200# **show rldp**	View the RLDP global configuration and the port detection information with RLDP detection configured

In the example below, the **show rldp** command is used to view the detection information of all RLDP ports:

```
DES-7200# show rldp
rldp state            : enable
rldp hello interval   : 2
rldp max hello        : 3
rldp local bridge     : 00d0.f8a6.0134
-----------------------------------------------
interface GigabitEthernet 0/1
port state:normal
neighbor bridge       : 00d0.f800.41b0
neighbor port         : GigabitEthernet 0/2
unidirection detect information:
action                : shutdown svi
```

```
state                : normal

interface GigabitEthernet 0/24
port state:error
neighbor bridge      : 0000.0000.0000
neighbor port        :
bidirection detect information :
action               : warnning
state                : error
```

As shown above, port GigabitEthernet 0/1 is configured with unidirection detection. No error is detected now, and the port status is normal. Port GigabitEthernet 0/24 is configured with bidirection detection, and bidirection fault is detected.

7.3.2 Viewing the RLDP Status of the Specified Port

In the privileged mode, run the following command to view the RLDP detection information of the specified port:

Command	Function
DES-7200# **show rldp interface** interface-id	View the RLDP detection information of interface-id.

In the example below, the **show rldp interface GigabitEthernet** *0/1* command is used to view the RLDP detection information of port fas0/1:

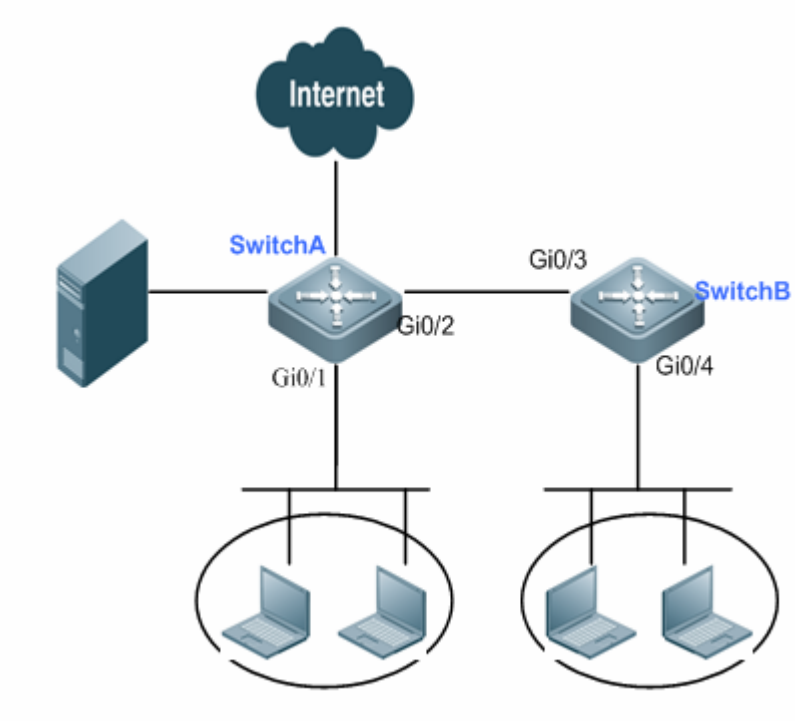
```
DES-7200# show rldp int GigabitEthernet 0/1
port state     :error
local bridge   : 00d0.f8a6.0134
neighbor bridge : 00d0.f822.57b0
neighbor port  : GigabitEthernet 0/1
unidirection detect information:
action: shutdown svi
state :  normal
bidirection detect information :
action : warnning
state :  normal
loop detect  information   :
action: shutdown svi
state :  error
```

As shown above, the port GigabitEthernet 0/1 is configured with three detection types: unidirection detection, bidirection detection and loop detection. The troubleshooting methods are shutdown-svi and warning. Error is found in loop detection so the current port status is error. Accordingly, the SVI of the port is shutdown.

7.4 Typical RLDP Configuration Example

7.4.1 RLDP Fault Detection and Handling

7.4.1.1 Topological Diagram



Topological diagram for RLDP application

7.4.1.2 Application Requirements

As shown above, users from respective departments of the enterprise access network through Switch A and Switch B. Due to network interruption caused by link failure or such non-device factors as the contrived network loop, RLDP loop detection and unidirectional/bidirectional link detection must be configured to instantly locate and handle faults, so that the network can be recovered instantly and the losses caused by network failure can be reduced. Major needs include:

- The loop error or unidirectional/bidirectional link failure detected can be handled as per the fault-handling method configured.
- If the port configured with "shutdown-port" fault-handling is failed, the RLDP detection can be recovered and all failed ports can start detection again.

7.4.1.3 Configuration Tips

1. After enabling global RLDP, enable RLDP on the port and configure diagnosis type and fault-handling method.

Note: For loop detection, RLDP cannot be enabled on the downlink port (the port connecting with department users or servers); for unidirectional/bidirectional link detection, RLDP must be enabled on the port connecting with peer device. If the port is a routing port, only the fault-handling method of warning, block or shutdown-port can be used, and shutdown-svi is not supported.

2. In privilege mode, use "rldp reset" command to enable all failed ports to start RLDP detection again.

7.4.1.4 Configuration Steps

Step 1: Enable RLDP on the device.

! Enable global RLDP on Switch A.

```
SwitchA#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
SwitchA(config)#rldp enable
```

! Configurations of Switch B are the same as above.

Step 2: Configure diagnosis type and fault-handling method on the port.

! Enable RLDP on the ports of Switch A; configure loop detection and fault-handling method as "block" on port Gi 0/1 and configure unidirectional link detection and fault-handling method as "warning" on port Gi 0/2.

```
SwitchA(config)#interface gigabitEthernet 0/1
SwitchA(config-if)#rldp port loop-detect block
SwitchA(config-if)#exit
SwitchA(config)#interface gigabitEthernet 0/2
SwitchA(config-if)#rldp port unidirection-detect warning
SwitchA(config-if)#exit
```

! Enable RLDP on the ports of Switch B; configure loop detection and fault-handling method as "block" on port Gi 0/4 and configure bidirectional link detection and fault-handling method as "shutdown-port" on port Gi 0/3.

```
SwitchB(config)#interface gigabitEthernet 0/4
SwitchB(config-if)#rldp port loop-detect block
SwitchB(config-if)#exit
SwitchB(config)#interface gigabitEthernet 0/3
SwitchB(config-if)#rldp port bidirection-detect shutdown-port
SwitchB(config-if)#exit
```

Step 3: Restore RLDP detection on the port.

! Execute "rldp reset" command on Switch A.

```
SwitchA#rldp reset
```

! Configurations of Switch B are the same as above.

7.4.1.5 Verify Configurations

Display RLDP information about all ports on the device.

! RLDP information of all ports on Switch A

```
SwitchA#show rldp
rldp state       : enable
rldp hello interval: 3
rldp max hello    : 2
rldp local bridge  : 00d0.f822.33aa
----------------------------------
Interface GigabitEthernet 0/2
port state     : normal
neighbor bridge : 00d0.f800.41b0
neighbor port   :  GigabitEthernet 0/3
unidirection detect information:
    action: warning
    state : normal

Interface GigabitEthernet 0/1
port state     : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
loop detect information   :
    action: block
    state : normal
```

! RLDP information of all ports on Switch B

```
SwitchB#show rldp
rldp state       : enable
rldp hello interval: 3
rldp max hello    : 2
rldp local bridge  : 00d0.f800.41b0
----------------------------------
Interface GigabitEthernet 0/3
port state     : normal
neighbor bridge : 00d0.f822.33aa
```

```
neighbor port   :  GigabitEthernet 0/2
bidirection detect information:
    action: shutdown-port
    state : normal

Interface GigabitEthernet 0/4
port state     : normal
neighbor bridge : 0000.0000.0000
neighbor port   :
loop detect information    :
    action: block
    state : normal
```

8 TPP Configuration

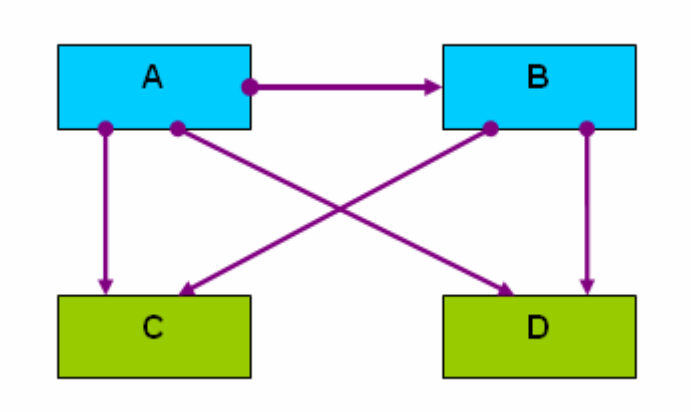
8.1 TPP Overview

The Topology Protection Protocol (TPP) is a topology stability protection protocol. The network topology is rather fragile. Illegal attacks in the network may cause abnormal CPU utilization on network devices, frame path blocked, etc. These are apt to cause network topology oscillation. The topology protection aims to stabilize the network topology by detecting the abnormalities (high CPU utilization, frame buffer abnormal, etc.) and detecting the abnormalities of neighbor devices. The interaction with neighbor devices is implemented by sending specific abnormity advertisement. This function has rather high priority and can effectively prevent network topology oscillation.

8.2 TPP Application

The topology protection is generated to address the network topology turbulence that my be caused in the MSTP or VRRP and other distributed network protocol. The MSTP, VRRP and other protocols work with the message notification mechanism to automatically maintain the network topological structure and automatically adapt to the topological change in the network. This on the other hand results in the aptness to attacks. When malicious network attacks arrive, transient interruption of timed messages may be caused due to high CPU utilization or frame path blocking, causing error fluctuation of the network topology and great harm to the normal communication in the network. The topology protection function minimizes such unnecessary fluctuations. It works with the other distributed protocols (MSTP, VRRP, etc.) to make the network more stable and reliable.

Figure-1:



As shown in the above dual-core topology, A and B are the L3 convergence devices, and C and D are the L2 access devices. A is the MSTP root bridge. The topology protection functions of all the devices are enabled.

The CPU of the L3 convergence device A is extremely busy due to network attack, resulting in that the BPDU packets cannot be sent. The topology protection function detects the exception and sends the exception advertisement packet to its neighbors. B, C, and D all receive the advertisement and adopt the anti-vibration measures.

The CPU of B is extremely busy under the attack of a large number of packets and cannot send or receive packets normally. After detecting the exception, B sends the exception advertisement to all its neighbors. A receives the exception advertisement but does not process it further because B finds the exception has not effect on B according to its source. The downstream C and D receive the exception advertisement and perform further defense activities to ensure the reliability of the network topology, because they find the exception will affect the topology calculation.

8.3 TPP Configuration

Configuring TPP involves global function configuration and port function configuration. The global function configuration is used to enable the topology protection function of the device. By default, the global topology protection function is enabled. Here, it will detect the running conditions of the local and neighbor devices and perform treatment for the abnormities that occur. However, it does not notify the local running conditions to neighbor devices. The port function configuration is used to enable the topology protection function of the port. When the topology protection function is enabled on the port, it indicates that the opposite neighbor device is concerning about the running conditions of this machine. When the local device becomes abnormal, this will be notified to the opposite neighbor device of the port. By default, the topology protection function is disabled on all ports.

Note

The topology protection function is suitable for the point-to-point link network, and adjacent network devices must enable the topology protection function. Besides, during the TPP configuration, you often need to use cpu topology-limit to configure the threshold for CPU utilization detection. When the CPU utilization exceeds the threshold, the system generates the topology protection advertisement. We suggest a middle to high value, such as 50–70, so that the TPP can judge the network conditions more accurately. If the value is too small, the network topology may not switch when it should to switch due to TPP alarm. If the value is too large, the system may be too busy to generate the TPP alarm, causing the TPP invalid.

8.3.1 Configuring Topology Protection Globally

The global topology protection function is enabled by default. The **no** option of the command disables the global topology protection.

The configuration commands are as follows:

Command	Function
DES-7200> **enable**	Enter the privileged mode.
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **topology guard**	Enable the global topology protection
DES-7200(config)# **end**	Exit to the privileged mode.
DES-7200# **copy running-config startup-config**	Save the configuration.

The **no topology guard** command disables the global topology protection function on the device.

8.3.2 Configuring Topology Protection on the Port

The configuration commands are as follows:

Command	Function
DES-7200> **enable**	Enter the privileged mode.
DES-7200# **config terminal**	Enter the global configuration mode.
DES-7200(config)# **interface gi** *0/1*	Enter the interface configuration mode.
DES-7200(config-if)# **tp-guard port enable**	Enable the port topology protection function.

Command	Function
DES-7200(config-if)# **end**	Exit to the privileged mode.

The **no tp-guard port enable** command disables the topology protection on the port. This command is suitable only on layer-2 switching ports and routing ports.It is inapplicable to AP member ports.

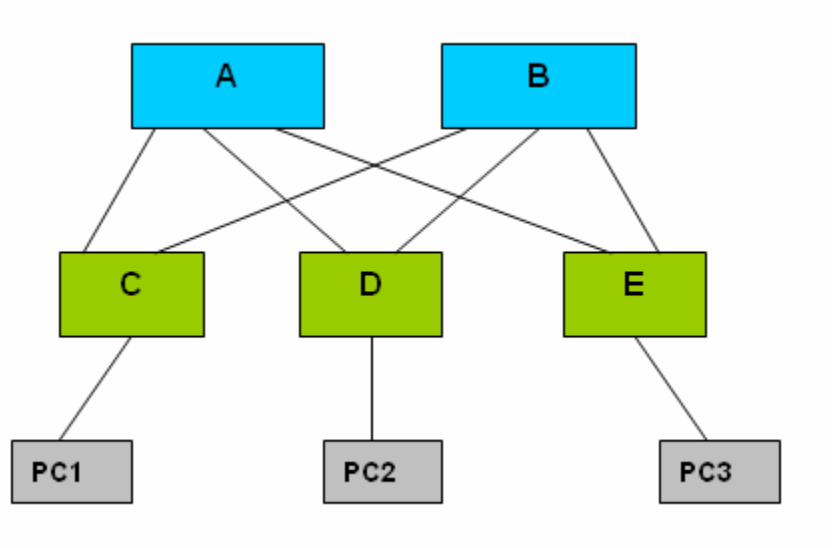
Note

The global topology protection is the global switch for the topology protection. When it is enabled, the device detects the running parameters of its own and monitors the running parameters of neighbor devices at the same time. When abnormity appears locally, it sends abnormity notification messages to the neighbor devices. When the port topology protection function is enabled, if abnormity occurs locally, it sends abnormity notification message to neighbor devices.

8.4 Typical TPP Configuration Examples

The figure below shows a dual-core networking topology:

Figure-2:



As shown in the figure, A and B are L3 convergence devices, while C, D and E are L2 access devices.

The MSTP enabled on A, B, C, D, and E, and VRRP enabled on A and B. The topology protection function enables the MSTP and VRRP to operate more reliable, avoiding unnecessary vibration of the network topology.

The global topology protection function is enabled on A, B, C, D, and E, and the topology protection function is enabled on all the ports..

8.5 View TPP information

The following TPP-related information can be viewed:

- View the TPP configuration and status of the device

8.5.1 Viewing the TPP configuration and status of the device

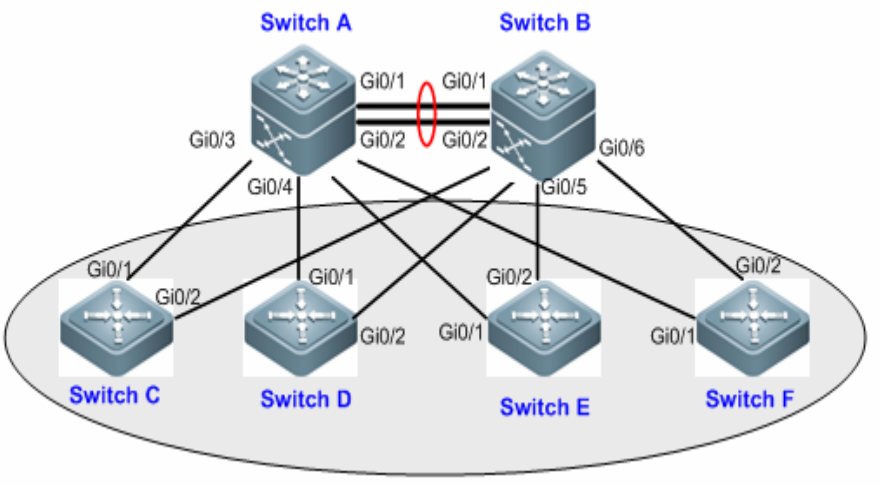
In the privileged mode, run the following command to view the TPP configuration and status of the device:

Command	Function
DES-7200# **show tpp**	View the TPP configuration and status of the device

```
DES-7200 #show tpp
tpp state          : enable
tpp local bridge   : 00d0.f822.35ad

      ----------------------------------
```

8.6 Typical TPP Configuration Example

8.6.1 Topology Diagram



Topologyl diagram for typical TPP application

8.6.2 Application Requirements

As shown above, the core layer of a park network adopts the typical MSTP+VRPP topological structure. The illegal attacks existing in the network may result in abnormal CPU utilization on network devices, frame path blocked and etc, thus leading to the network topology oscillation.

By applying TPP, MSTP and VRRP can operate more stably, thus avoiding unnecessary network topology oscillation.

8.6.3 Configuration Tips

Configure the following features on layer-3 core devices (Switch A/B) and layer-2 access devices (Switch C/D/E/F):

- Enable topology protection globally. This feature is enabled by default.
- Enable topology protection on the port connecting with devices, so that any local abnormality can be advertised to the neighbors in order to maintain topological stability.
- Configure the threshold for CPU utilization detection on each device. When CPU utilization of the device exceeds this threshold, the system will generate topology protection advertisement.

Note

It is suggested to configure this value to an above-average ratio, such as 50-70, so that TPP can precisely estimate the network situation. If this value is too low, the network topology cannot be switched due to the alert of TPP when it becomes necessary; if this value is too high, the system may be too busy to generate TPP alert, resulting in the failure of TPP function.

8.6.4 Configuration Steps

Only TPP configurations will be introduced below. For relevant configurations of MSTP+VRPP, please refer to "MSTP Configuration" and "VRRP Configuration" in the manual.

- **Configurations on Switch A/B**

  Step 1: Global topology protection is enabled by default. If it is disabled, use the following command to enable this function.

```
DES-7200# config terminal
DES-7200(config)# topology guard
```

Step 2: Enable topology protection on the interface.

! Enable topology protection on the AP ports connecting core devices.

```
DES-7200(config)#interface aggregateport 1
DES-7200(config-if-AggregatePort 1)#tp-guard port enable
```

! Enable topology protection on the ports connecting downlink devices.

```
DES-7200(config)#interface range gigabitEthernet 0/3-6
DES-7200(config-if-range)#tp-guard port enable
```

Step 3: Configure the threshold for detecting CPU utilization.

! When CPU utilization exceeds 60%, the system will generate topology protection advertisement.

```
DES-7200(config)#cpu topology-limit 60
```

- **Configurations on Switch C/D/E/F**

Step 1: Global topology protection is enabled by default. If it is disabled, use the following command to enable topology protection.

```
DES-7200# config terminal
DES-7200(config)# topology guard
```

Step 2: Enable topology protection on the interface.

```
DES-7200(config)#interface range gigabitEthernet 0/1-2
DES-7200(config-if-range)#tp-guard port enable
```

Step 3: Configure the threshold for detecting CPU utilization.

! When CPU utilization exceeds 60%, the system will generate topology protection advertisement.

```
DES-7200(config)#cpu topology-limit 60
```

8.6.5 Verification

- **Display TPP configurations**

Take the Switch A as the example for viewing TPP configurations. Key points: TPP state, TPP information of interface.

```
DES-7200#show tpp
tpp state        : enable      //Global TPP is enabled by default
tpp local bridge  : 00d0.f822.33aa
-----------------------------------
interface GigabitEthernet 0/3
port tpp state      : enable
interface GigabitEthernet 0/4
port tpp state      : enable
```

```
interface GigabitEthernet 0/5
port tpp state      : enable
interface GigabitEthernet 0/6
port tpp state      : enable
interface AggregatePort 1
port tpp state      : enable
```

- **Verification of TPP function**

  When spanning tree topology is stable, SwitchA is the root bridge, and the Gi 0/2 interface of Switch C is in Block state.

  Step 1: To simulate the scenario that Switch C is attacked by the downlink illegal users, we have configured BPDU Filter on port Gi0/3 of Switch B, so that port Gi0/2 of Switch C cannot receive BPDU packets. When TPP is not configured, port Gi0/2 of Switch C turns into Forwarding state, and the topology changes.

```
DES-7200#show spanning-tree sum

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
             Address     00d0.f834.56f0
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    Type  OperEdge
---------------- ---- --- ---------- -------- -----
Gi0/2           Desg FWD 20000     128     P2p   True
Gi0/1           Root FWD 20000     128     P2p   False

MST 1 vlans map : 10, 20
  Region Root Priority   4096
             Address     00d0.f834.56f0
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa

Interface       Role Sts Cost      Prio    Type  OperEdge
-----------     ---- --- ---------- -----    -----------
```

```
Gi0/2          Desg FWD 20000     128     P2p   True
Gi0/1          Root FWD 20000     128     P2p   False
```

Step 2: After completing TPP related configurations as per the steps shown herein, we simulates the scenario that Switch C is attacked by downlink illegal users who send excessive ARP packets to Switch C, causing CPU utilization to exceed the configured threshold. By this time, further configure BPDU Filter on port Gi0/3 of Switch B, so that the Gi0/2 of Switch C cannot receive BPDU packets. By displaying the state of spanning tree interface on Switch C, it can be found that the interface maintains the Block state. TPP has taken effect.

```
DES-7200#show spanning-tree summary

Spanning tree enabled protocol mstp
MST 0 vlans map : 1-9, 11-19, 21-29, 31-39, 41-4094
  Root ID    Priority    4096
             Address     00d0.f834.56f0
             this bridge is root
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa
             Hello Time   2 sec  Forward Delay 15 sec  Max Age 20 sec

Interface       Role Sts Cost      Prio    Type  OperEdge
-----------     ---- --- ---------- -----    -----------
Gi0/2          Altn BLK 20000     128     P2p   False
Gi0/1          Root FWD 20000     128     P2p   False

MST 1 vlans map : 10, 20
  Region Root Priority   4096
             Address     00d0.f834.56f0
             this bridge is region root

  Bridge ID  Priority    32768
             Address     00d0.f822.33aa

Interface       Role Sts Cost      Prio    Type  OperEdge
-----------     ---- --- ---------- -----    -----------
Gi0/2          Altn BLK 20000     128     P2p   False
Gi0/1          Root FWD 20000     128     P2p   False
```

9 NLB Group Configuration

9.1 Introduction to NLB Group

The user can use NLB Group to realize the feature that all servers under a certain cluster can receive IP packets sent to this cluster. As shown in Fig 1, after configuring cluster service on the device, packets sent to this cluster (IP address being 192.168.1.10) will reach master server and slave server respectively through Gi 0/1 and Gi 0/2.

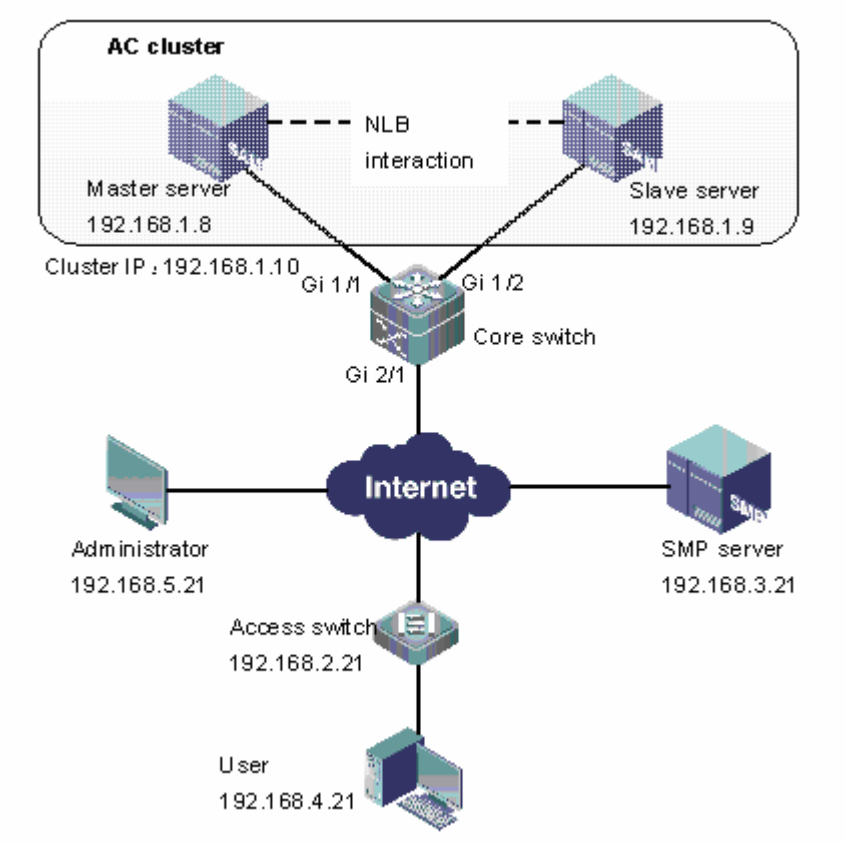


Fig 1 Application of cluster

9.1.1 Overview of NLB Group

NLB Group (also called cluster service) is a service developed to support Microsoft Network Load Balance (NLB). On the core switch shown in Fig 1, cluster service is not supported by default, namely all IP packets sent to the cluster cannot be sent to master and slave master at the same time. This is because the unicast packets have only one next-hop address. To allow master server and slave server to receive IP packets sent to the cluster, the cluster service must be configured on the device.

9.1.2 <Concept and terms of NLB GROUP>

9.1.2.1 <NLB>

Network Load Balance (NLB) is a load balancing technology provided in Windows 2000 Server and Windows Server 2003 of Microsoft. NLB uses a distribution algorithm to distribute loads to multiple hosts, so as to provide IP-based key services (such as Web, FTP, firewall, proxy, VPN and other Internet server applications). A single computer running Windows system can provide limited server reliability and scalability. However, by integrating two or more computers running Windows Server 2003, NLB can provide the performance and reliability needed by Web server and other key task servers.

9.1.2.2 <VRF>

The VPN to which the cluster belongs on the device. A VPN is a collection of sites sharing routes through VPN routing/forwarding (VRF) table.

9.1.2.3 <NLB-Address>

IP address of cluster. NLB allows all computers in the cluster to be addressed by a group of same cluster IP addresses.

9.1.2.4 <Reflector-Port>

Reflector port. To realize cluster service, the device uses a reflector port to send cluster IP packets to all computers in the cluster.

9.1.2.5 <Destination-Port>

Destination port. The destination port to which packets will be sent (namely the port connecting cluster and device), such as Gi 0/1 and Gi 0/2 shown in Fig 1.

Caution

1. The reflector port can only be a layer-2 switching port (you cannot configure L2AP as the reflector port), and no other configurations are allowed on the reflector port.
2. The cluster server shall communicate with the device through the SVI, rather than the Routed Port.

9.1.3 Working principle

Taking Fig 1 as the example, below we will introduce the working principle of cluster service:

Step 1: User sends IP packets (the destination IP address of such packets is the IP address of cluster: 192.168.1.10)

Step 2: IP packets reach the core switch through routing addressing

Step 3A: The scenario in which reflector port is needed: After IP packets enter into the core switch through Gi 2/1, they are sent to the reflector port, which will relay IP packets to the destination port (Gi 1/1, Gi 1/2).

Step 3B: The scenario in which reflector port is not needed: After IP packets enter into the core switch through Gi 2/1, they are directly routed to the destination port (Gi 1/1, Gi 1/2).

Step 4: IP packets are received by the master server and slave server in the AC cluster.

9.1.4 Protocol specification

NA

9.2 Default configurations

The following table describes the default configurations of NLB Group.

Function	Default setting
NLB Group service	Disabled

9.3 Configure NLB Group

9.3.1 Configure cluster attributes and specify the connection port

The user can execute the following steps to configure cluster service and specify the port connecting cluster and device:

Command	Function
DES-7200(config)# **nlb-group** *group-number* [**vrf** *vrf-name*] **ip** *nlb-address* [**reflector-port** *interface-name*]	Configure a group of cluster attributes, including VRF, cluster IP and the reflector port occupied by the cluster. If VRF keyword is not specified, it shall mean global VRF.
DES-7200(config)# **nlb-group** *group-number* **destination-port** *interface-name*	Configure the port connecting cluster and device.

To delete cluster attributes or connection port, use "**no nlb-group** *group-number* **vrf** *vrf-name* **ip** *nlb-address* **reflector-port** *interface-name*" or "**no nlb-group** *group-number* **destination-port** *interface-name"* global configuration command. To delete all cluster groups, execute "**no nlb-group all**" global configuration command.

To delete the entire cluster group (including attributes and connection port), execute "**no nlb-group** *group-number*" global configuration command.

Caution

1. You can configure up to 5 clusters for each switch, and up to 16 connection ports for each cluster.
2. Arp Check cannot be enabled on the cluster connection port. If Arp Check is enabled on the cluster connection port, the cluster IP may not be able to communicate with other ports.

9.3.2 View cluster service state

Command	Function
show nlb-group [*group_number*]	View the current configurations of the cluster

9.4 Typical NLB GROUP configuration example

9.4.1 Networking requirements

NA.

9.4.2 Network topology

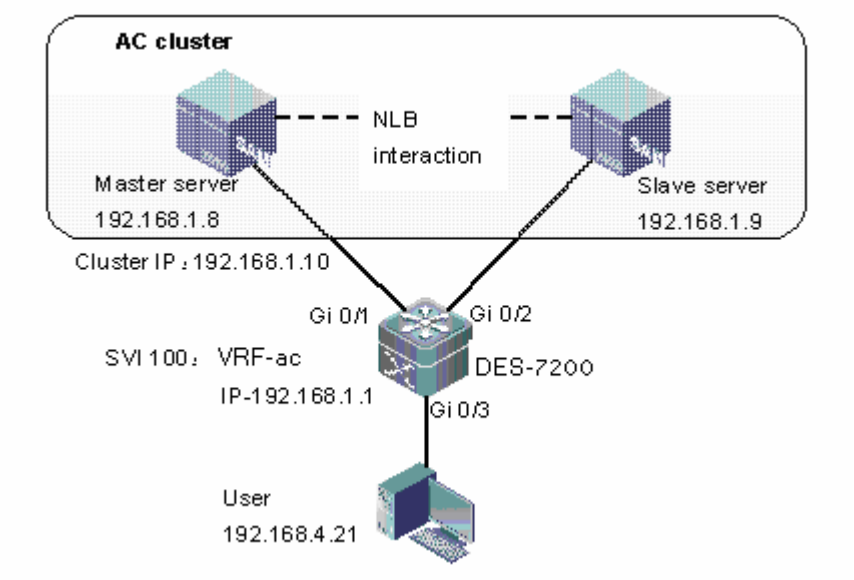


Fig 2 NLB Group network topology

9.4.3 Configuration tips

Cluster communicates with devices via SVI, but cannot communicate with Routed Port (this is because only SVI can send the same packet to multiple ports).

9.4.4 Configuration steps

1) Configure VLAN 100 to include Gi 0/1 and Gi 0/2 into VLAN 100

Enter global configuration mode

```
DES-7200# config terminal
```

Create VLAN 100

```
DES-7200(config)# vlan 100
DES-7200(config-vlan)# end
DES-7200(config)#
```

Enter interface configuration mode

```
DES-7200(config)# interface gigabitethernet 0/1
```

Include Gi 0/1 into VLAN 100

```
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport access vlan 100
DES-7200(config-if)# end
DES-7200(config)#
```

Enter interface configuration mode

```
DES-7200(config)# interface gigabitethernet 0/2
# Include Gi 0/2 into VLAN 100
DES-7200(config-if)# switchport mode access
DES-7200(config-if)# switchport access vlan 100
DES-7200(config-if)# end
```

2) Configure SVI 100 and assign the IP address of 192.168.1.1

```
DES-7200(config)#
```

Enter interface configuration mode

```
DES-7200(config)# interface vlan 100
DES-7200(config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# end
```

3) Configure VRF and the IP address of SVI 100

```
DES-7200(config)#
```

Create VRF “ac”

```
DES-7200(config)# ip vrf ac
```

Enter interface configuration mode

```
DES-7200(config)# interface vlan 100
```

Description: connect to ac

```
DES-7200(config-if)#description  connecting-to-ac
```

Enable VRF on the interface

```
DES-7200 (config-if)# ip vrf forwarding ac
```

Configure the IP address of interface

```
DES-7200 (config-if)# ip address 192.168.1.1 255.255.255.0
DES-7200(config-if)# end
```

3) Configure the attributes and connection port of cluster group

Configure cluster group 1, and select Gi 0/3 as the reflector port

```
DES-7200(config)#
```

```
DES-7200(config)# nlb-group 1 vrf ac ip 192.168.10.1 reflector-port
gigabitethernet 0/3
```

Configure the port connection cluster group 1 and device

```
DES-7200(config)# nlb-group 1 destination-port gigabitethernet 0/1, 0/2
```

9.4.5 Verification

In privilege mode, execute "show nlb-group" command to display configurations of the existing cluster group. The following example shows show to display the current state of cluster group 1 through "show nlb-group" command.

```
DES-7200# show nlb-group 1
group-number： 1
cluster-vrf: ac
cluster-ip: 192.168.1.10
destination-port : Gi 0/1, Gi 0/2, Gi 0/3
```

10 Redundancy Configuration for Management Module

This chapter describes how to configure the management module redundancy to implement nonstop forwarding(NSF) and the system file management method of the the management module.

This chapter includes:

1. Understanding redundant NSF of the management module
2. NSF configuration method

10.1 Understanding Redundant NSF of Management Module

10.1.1 Overview

NSF means that in the network device with the structure of separating control panel from forward panel, the control panel is planned to shut down(such as software upgrade) or not planned to shut down(such as software and hardware defect) while the forward panel goes on forwarding and there is no forward halt or topology fluctuation during the reboot of control side. NSF is an important part of High Availability Architecture

Caution DES-7200 series switch that support hot-plugging/unplugging of the management module implements NSF in the method of the management module redundancy.

In the machine which is installed with dual the management modules, the the master management module is used normally while the other backup one is the slave management module which is a substitute for the master one when the master one is broken off or requires for the switchover. It not only enlarges exchanging capacity but also offers management redundancy to improve the stability of device. In the running process of the device, if the the master management module does not work well, the device will switch to the slave one automatically without losing user's corresponding

configuration, which ensures that the network runs well. Generally, the slave management module does not join in the switch management but monitors the status of master one. These events below will trigger the management module switchover:

1) System suspend or reset due to hardware fault of the master management module

2) No heartbeat between two management modules

3) Manual switchover

When booting dual management modules at the same time or hot-plugging another when one board is enabled, they will do some batch synchronization configuration before they are in Active/Standby Hot status. At this time, if disturbance sources are configured, the slave management module will reboot and both are in Active/Boot Hot status. If all disturbance sources are cleared in Active/Boot Hot status, the slave one will reboot too and both are in Active/Standby Hot status. If new disturbance sources are configured in Active/Boot Hot status, this brings no influence and both are still in Active/Boot Hot status.

Now, the disturbance sources include the following entities:

Caution

- GVRP: GARP VLAN Registration Protocol, an application of the relationship between dynamic configuration and extended VLAN member .
- PVLAN: Private VLAN.
- MCAST: Multicast.
- DOT1X: 802.1x, which is used to control the authentication of user network access and provide authorization and accounting function.
- PTLVLAN: Protocol VLAN, VLAN classification technology based on package protocol type. It can divide the null VLAN ID of a protocol typet to a same VLAN.

Postscript: the dual managemetn panels are in Boot Cold/Boot Cold status if the system detects the in consistency of the software version of the dual ones when starting up. In other words, they can detect the other side respectively, but they are not in Active/Standby Hot status untill the automatic upgrade is finished and the slave one is reset. Finally, the software version of the dual the management modules is consistent.

10.1.2 NSF Advantages and Limits

The advantages of NSF technology implementation in network service are:

- Improving the network availability:

  NSF technology maintains the information of data forwarding and user session status in the process of device change.

- Preventing the neighbour from detecting link flap:

  The forwarding side does not reboot during the switchover, so the neighbour can not detect the link status change from Down to Up.

- Preventing routing flaps:

  The forwarding side maintains to forward and communicate during the switchover and the control side forms new forwarding list quickly without apparent substitution between the new and oil forwarding list, thus preventing routing flaps.

- User sessions will not be lost:

  User sessions built before the switchover will not be lost due to the synchronization in real time.

The limits of using NSF technology in the switch are:

- NSF works well on the premise that the software and hardware constitution of the dual the management modules are consistent.
- It should synchronizes the master and the slave management modules in batch to make them consistent, before which is the window period when NSF can not take effect.
- Not all the functions related with forwarding are synchronized. The switch function can be classified into the following types according to NSFsupporting degree:
  - High availability support function;
  - Real time synchronization of status information between master and the slave management module. For example, it synchronizes the control side function directly related with L2 forwarding in real time.
  - High availability compatibility function
  - These features do not support high availability for the status datas are not synchronized. However, when enabling high availability, these functions that starts to run from initialization can still be used after switching.
  - High availability incompatibility function

Caution

These features do not support high availability for the status datas are not synchronized. When enabling high availability, these functions can not be used, or it may lead to system abnormity. When enabling these functions, the system status is changed from Standby Hot to Boot Hot and the system can only synchronize running-config, such as GRRP.

10.1.3 Key Technology of NSF

The key technologies of implementing NSF include:

- **Status synchronization**

The the master management module synchronizes the running status with the slave one in order to enable the slave one to be a substitute for the master one at any time without noticeable changes.

- **Configuration synchronization**

It synchronizes the configurations of the functions that are not associated with NAF directly. The user configuration keeps consistent during the switchover by the synchronization of running-config and startup-config.

Conducting running-config when user configuration returns to the privileged mode from the global mode, while conducting startup-config synchronization when the user executes command write or copy to save the configuration.

It can not synchronize SNMP configuration automatically untill running-config synchronization is triggered by CLI configuration method.

Caution

You can configure auto-sync mode as the following steps. In the global configuration mode, execute command **redundancy** first and then **auto-sync { standard | startup-config | running-config }.** To view the current auto-sync mode, use **show redundancy auto-sync** in the privileged mode. To configure the auto-sync interval in an unit of second, execute command **redundancy** first and then **auto-sync time-period value.**

Auto-sync has three modes:

a) standard: synchronizes all the system files. In other words, it synchronizes both startup-config and running-config.

b) startup-config: synchronizes startup configuration file.

c) running-config: synchronizes configuration file of running time.

The **no** form of the command disables all the modes, making the configuration file out of auto-sync. By default , the mode of auto-sync is standard, which synchronizes both startup-config and running-config.

10.2 NSF Configuration Method

Caution

In the management module redundancy constitution methods, only the master management module supports all CLI commands, while the slave management module supports a few commands in user EXEC and privileged EXEC mode.

10.2.1 Configuring Redundant Management

This chapter includes:

- Automatic selection of the master management module

- Manual selection of the master management module

10.2.1.1 Automatic selection of the master management module

You can plug or unplug the the management modules while the switch is working. Based on the current conditions, the switch automatically selects an engine for its operation without normal data switching. In case of any conditions below during you use, the the master management module will be selected accordingly:

- If only one the management module is plugged when the switch is started up, the switch will select it as the the master management module no matter whether it is in slot M1 or M2.
- If both the management modules are plugged when the switch is started up, by default, the one in slot M1 will be selected as the master and the one in slot M2 as the slave for purpose of redundancy. Related prompt message will be provided.
- If only one the management module is plugged when the switch is started up, and the other the management module is plugged while the switch is in normal operation, the latter will be regarded as the the slave management module for purpose of redundancy, no matter whether it is slot M1 or M2. Related prompt message will be provided.
- If both the management modules are plugged when the switch is started up, and one of them is unplugged while the switch is in normal operation (or one becomes abnormal): if the unplugged the management module is the slave before it is unplugged (or abnormal), the switch only prompts that the the slave management module is unplugged (or becomes abnormal); if the unplugged the management module is the master before it is unplugged (or abnormal), the other the management module will turn from slave to master, and related prompt will be provided.

During the normal operation of the switch, the parameters must be saved when the configurations are done; otherwise, the configuration will be lost in case of master/salve switchover.

During the startup of the device inserted with two the management modules, if the main program of any the management module is incomplete or absent, the switch cannot start. The symptom is that the two boards restart repeatedly or suspend during the startup process.

During the startup of the device inserted with one the management module, if the management module with incomplete or absent CTRL program or main program is inserted before the success of the startup, the switch also cannot start.

Caution

In the above two case, remove the faulty the management modules. If the device is still abnormal, power off the switch and restart it.

During the batch backup of master and the slave management module, do not unplug the master one, or it will lead to data flow breakoff due to system reset. If the software of dual the management modules are abnormal during the period of batch backup, it will also lead to data flow breakoff due to system reset.

Please unplug one of the dual the management modules quickly if you want to unplug one of them when they are working simultaneously. Slow unplugging may make the management module work abnormally. Please make sure that the management module is plugged tightly and the screw id tightened.

10.2.1.2 Manual selection of the master management module

The DES-7200 series switch supports dual the management modules. You may select the master and the slave management modules by using the commands available in CLI.

In the privileged user mode, execute the following commands to forcibly switch over the the master management module:

Command	Meaning
redundancy force-switchover switch	This command is executed immediately without the necessity for global configuration mode.

For example, the current the master management module is the one in slot M1. When the following commands are executed, the the management module will be switched over to the the slave management module, and the one in slot M2 becomes the master.

```
DES-7200# redundancy  force-switchover switch
```

10.2.2 Configuring the Synchronization Mode

Run the following commands to configure the configuration files to be synchronized:

Command	Function
DES-7200(config)# **redundancy**	Enter the redundancy configuration mode
DES-7200**(config-red)# auto-sync** {**standard** | **running-config** | **startup-config**}	Configure the configuration files to be synchronized.
DES-7200#**show running-config**	Confirm the hot-backup started.
DES-7200#**show redundancy state**	Show the current redundancy operation mode.

10.2.3 Configuring the Heart-beat Check Time

Run the following command to configure the heart-beat check time between the master and the slave management modules.

Command	Function
DES-7200(config)# **redundancy**	Enter the redundancy configuration mode
DES-7200(config-red)# **switchover timeout** *timerout-period*	Control the heart-beat check time between the master and slave boards
DES-7200#**show running-config**	Confirm the hot-backup started.
DES-7200#**show redundancy state**	Show the current redundancy operation mode.

10.2.4 Resetting the Management Module

Run the following command to reset the specified the management module or both the master and salve ones.

Command	Function
DES-7200(config)#**redundancy reload {peer | shelf}**	peer: reset the slave management module only. shelf: reset both.

DES-7200

System Management Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

Note

The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products.

The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 File System Configuration

1.1 Overview

The file system offers a unified management of file crossing platforms, no matter what kinds of devices, storages and file transmission protocol are used.

Locally, there are many kinds of storage medias, for instance, USB and FLASH, which can be distributed on different boards like primary control module and secondary module. Users can exchange files with remote devices through xModem and TFTP protocols under file management commands.

Not all types of devices and all types of file systems support all file system commands described in this chapter, because they support different types of file operations. The Help command shows the storage medias and protocols supported by the file operation commands.

1.2 Basic Features of File System

The file system management offers an unified command interface for related file operations. It offers the following features:

- Use URL to locate a file
- Show the file system information
- Manage local files
- Transfer files through communications protocols

1.2.1 Using URL to Locate A File

The file system ues URL to uniformly locate the files and directories in the storage medias of local device or remote device. For example, you can copy a file by using the **copy** *source-url destination-url* command, which can be local or remote.

URL representation varies by commands.

Locate the file on the server

To locate the file on the server, use the following command:

tftp:[[*//location*]/*directory*]/*filename*

location: IP address or host name

/directory: position for file transmission. For instance, the file transmission directory specified by the TFTP server is C:\download, the file path specified by the device is the one under C:\download. tftp://192.168.0.1/binary/firmware.bin refers to the c:\download\binary\firmware.bin file on the TFTP server of the IP address of 192.168.0.1.

Note

TFTP transmits only the files in the size of less than 32M. To transmit the files in the size of larger than 32M, use the FTP protocol.

Locate the local file

To locate the local file from FLASH, USB and the FLASH of the control module of the device, use the [*prefix*]:[*directory/*]*filename* syntax. For example:

flash:/config.text: the configuration on the local FLASH

usb0:/backup/firmware.bin.bak: the file on the first USB

slave:/firmware.bin: the file under the root directory of the secondary control module

Note

Without prefix, the syntax refers to the file system type in the current path, for instance, usb0 under the root directory of USB0.

Note

When you use prefix to specify a local file, the path after ":" must be absolute path.

Description of URL prefix

URL prefix is used to specify a file system. Different devices and file operation commands can run different file systems. You can show the file system supported on the device by the **show file system** command.

The following table shows the URL prefixes:

Prefix	Description
flash:	FLASH, which can be used on all devices. The startup program is generally stored in the FLASH of a device when delivery.
Tftp:	TFTP server
xmodem:	Receive and send files through xModem
slave:	FLASH on the secondary control module of the rack-mounted device
Usb0:	The first USB device

Usb1:	The second USB device
sd0:	The first SD card

Note

Different file system commands and different platforms support different types of file system. For details, use the help information in the command line, for example:

```
WORD              Copy from current file system
  flash:          Copy from flash: file system
  running-config  Copy from current system configuration
  slave:          Copy from slave: file system
  startup-config  Copy from startup configuration
  tftp:           Copy from tftp: file system
  usb0:           Copy from usb0: file system
  usb1:           Copy from usb1: file system
  sd0:            Copy from sd0: file system
  xmodem:         Copy from xmodem: file system
```

Note

Given the limit of xModem, the size of the files transmitted through xModem will be slightly larger than the real file size.

1.2.2 Showing the File System Information

This command shows all the file systems supported on the device and their available spaces.

In the privileged mode, use the following command:

```
DES-7200#show file systems

File Systems:
       Size(b)       Free(b)       Type     Flags     Prefixes
   ------------   ------------   ---------   -------   ----------
*     33488896      16191488      flash       rw       flash:
            -             -      flash       rw       usb0:
            -             -      flash       rw       usb1:
            -             -      flash       rw        sd0:
```

```
                -            -       flash        rw       slave:
                -            -     network        rw        tftp:
                -            -     network        rw      xmodem:
---------------------------------------------------------------------
```

In this information, "*" means the active file system, size means the space of the file system and free means the available space.

Note

Free means the available space of the file system, not the size of the file to be stored. Since the file system has its own management overhead, the size of the files that the system finally can store is slightly less than the free space.

1.2.3 Managing Local Files

Local files refer to the ones storing in various storage medias on the device, for instance, FLASH, and USB. The system files such as main program, configuration, file, logs and web files are stored generally in FLASH. Some devices come with USB interface. The files on the U-shaped disc are also local files. For rich-mounted device with dual control modules, you can management the files in the FLASH of the secondary control module by the slave prefix of URL.

For local files, you can:

- Copy files
- Move files
- Delete files
- Crate directory
- Delete directory
- Show directory
- Show the current working path
- Modify the working path

These operations apply to slave-, USB-, or FLASH-type file systems.

Note

File name is case sensitive on the FLASH- and slave- file systems. For example, abc.txt and Abc.txt are different documents. On USB-type file system, however, file name is not case sensitive, namely abc.txt and Abc.txt are considered to be one document.

Note

Number and size of files will influence the startup speed and operation speed of files at a certain extend. Too many large files stored in FLASH will slow down the startup and update of devices. When the device starts for the first time, the waiting time of the **dir** command is longer. Generally, it is recommended to use the file system of less than 128M. When it is necessary to store a lot number of files, it is recommended to store them on U-shaped disc. After using the file system for a long period of time, clear some old and useless files by hand.

Note

Some files are important for normal operation. Deleting these files will cause malfunction. These important system files include:

- RCMS configuration file (/rcms_config.ini)
- Web management package (/web_management_pack.upd)
- Main program (for multi-boot-supported devices, the main program includes all the files in the boot system configuration)

The system will automatically recognize these files and trigger an alarm before you execute deletion operation. If you need to delete system files, the system will print WARN-level logs as below:

DES-7200# **delete** *firware.bin*

File [firmware.bin] is a system file. System may not work properly without it.

Are you sure you want to delete it? [no] yes

0:1:1:38 DES-7200: FS-4-SYSTEM_FILE_DELETED: System file [firmware.bin] deleted!

Note

The file name with path should be no more than 4096 bytes. Wildcard is not supported for file name and path.

1.2.4 Transmitting Files through Communication Protocols

Transmit files through TFTP:

You are allowed to upload and download files to the TFTP server.

In the CLI privileged mode, use the following command to download files:

```
DES-7200# copy tftp:[[//location]/directory]/filename
destnation-url
```

In the CLI privileged mode, use the following command to upload files:

```
DES-7200# copy source-url
tftp:[[//location]/directory]/filename
```

Transmit files through xModem:

In the CLI privileged mode, use the following command to download files:

```
DES-7200# copy xmodem:  destnation-url
```

In the CLI privileged mode, use the following command to upload files:

```
DES-7200# copy source-url xmodem:
```

1.3 Typical Configuration Example

1.3.1 Downloading Files from the TFTP Server

The following example shows how to download a.dat from the c:\download\ of the TFTP server to the local device:

Step 1: Run the TFTP Server on the host and select C:\download where the file to be downloaded locates.

Step 2: Use the ping command to test the connection between the device and the TFTP server.

Step 3: Log on the device, enter the privileged mode and run the command:

```
DES-7200#copy tftp://192.168.201.54/a.dat flash:
Destination filename [a.dat]?
Accessing tftp://192.168.201.54/a.dat
!!!!!!!!!!!!!!!!!!!!!
Transmission finished, file length 343040
```

Step 4: Run the dir command to show the files on the device.

```
DES-7200#dir
Directory of flash:/
   Mode Link     Size             MTime Name
-------- ---- --------- -------------------
------------------
          1   343040 2009-01-01 02:02:59 a.dat
          1  10838016 2009-01-01 00:08:38 firmware.bin
          1      399 2009-01-01 00:01:37 config.text
```

```
-------------------------------------------------------
----
3 Files (Total size 11181455 Bytes), 9 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes
(19MB) available.
```

1.3.2 Uploading Files to the TFTP Server

The following example shows how to upload a.dat to the c:\download\ of the TFTP server:

Step 1: Run the TFTP Server on the host and select C:\download where the file to be uploaded locates.

Step 2: Use the ping command to test the connection between the device and the TFTP server.

Step 3: Log on the device, enter the privileged mode and run the command:

```
DES-7200#copy flash:/a.dat tftp://192.168.201.54/a.dat
Accessing flash:a.dat...
!!!!!!!!!!!!!!!!!!!!
 Transmission finished, file length 343040
```

Step 4: Check the result.

1.3.3 Downloading Files through xModem

The following example shows how to download config.txt from PC throuhg xModem to the local device:

Step 1: Use serial cable to connect the seiral interface of PC and the serial interface of the device.

Step 2: Run the hyperterminal of Windows to connect to the console of the device.

Step 3: In the privileged mode, use the following command to download file:

```
DES-7200# copy xmodem: flash:/config.text
```

Step 4: In the Windows hyperterminal of local deivce, select Transmit files of Transmit menu.

Step 5: In the pop-up dialog box, select the file to download and xModem. Click Transmit. The Windows hyperterminal shows the transmission progress and packets.

Step 6: Run the dir command to show the files on the device.

```
Directory of flash:/
   Mode Link     Size             MTime Name
-------- ---- --------- -------------------
------------------
```

```
            1    343040 2009-01-01 02:02:59 a.dat
            1  10838016 2009-01-01 00:08:38 firmware.bin
            1       399 2009-01-01 00:01:37 config.text
-------------------------------------------------------------
----
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes
(19MB) available.
```

1.3.4 Uploading Files through xModem

The following example shows how to upload config.txt from the local device throuhg xModem to C:\Documents and Settings\ju of PC:

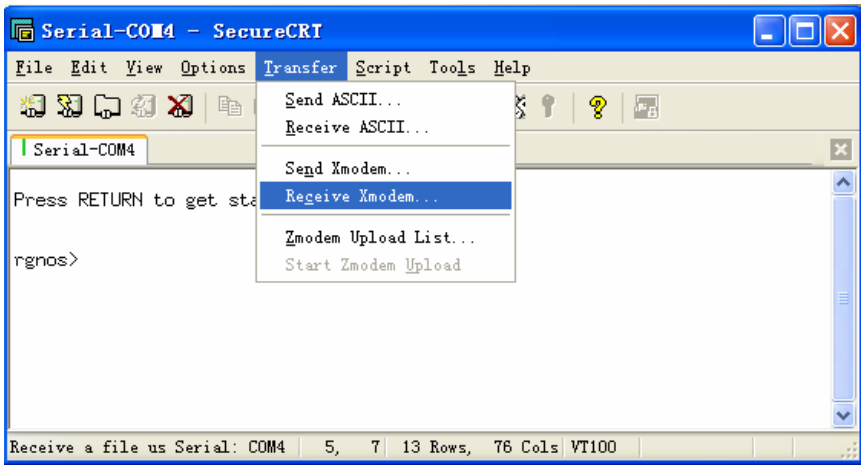
Step 1: Use serial cable to connect the serial interface of PC and the serial interface of the device.

Step 2: Run the hyperterminal of Windows to connect to the console of the device.

Step 3: In the privileged mode, use the following command to upload file:

```
DES-7200# copy flash:/config.text xmodem
```

Step 4: In the Windows hyperterminal of local device, select Receive files of Transmit menu, as shown below:



Step 5: In the pop-up dialog box, select the place to save the uploaded file and xModem. Click Receive. The Windows hyperterminal prompts to set the name used to store the file. Click OK.

Step 6: Check the configuration.

1.3.5 Moving Files from FLASH to USB

The following example shows how to move config.txt from FLASH to U-shaped disc inserting USB0 and save it in the backup directory of U-shaped disc:

```
Directory of flash:/
    Mode Link        Size                  MTime        Name
-------- ---- --------- ------------------- ------------------
               1      343040 2009-01-01 02:02:59       a.dat
               1    10838016 2009-01-01 00:08:38       firmware.bin
               1         399   2009-01-01 00:01:37       config.text
-----------------------------------------------------------------
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

Enter the root directory of U-shaped disc:

```
DES-7200#cd usb0:/
```

Confirm the current path:

```
DES-7200#pwd
usb0:/
```

Create backup directory on U-shaped disc:

```
DES-7200#mkdir backup
```

Copy the file to U-shaped disc:

```
DES-7200#copy flash:/config.text config.text
```

Check the result.

```
DES-7200#dir backup
Directory of usb0:/backup
   Mode Link     Size             MTime     Name
-------- ---- --------- -------------------
------------------
          1      399   2009-01-01 00:01:37  config.text
-----------------------------------------------------------
----
Total 33030144 bytes (31MB) in this device, 20488192 bytes
(19MB) available.
```

Command	Function
DES-7200# **rename flash:** *old_filename* **flash**: *new_filename*	Name the file named as *old_filename* to *new_filename*.

1.3.6 Moving Files from FLASH to SD Card

The following example shows how to move config.txt from FLASH to SD card and save it in the backup directory of SD card:

```
Directory of flash:/
    Mode Link         Size                      MTime         Name
-------- ---- --------- ------------------- ------------------
               1      343040 2009-01-01 02:02:59       a.dat
               1    10838016 2009-01-01 00:08:38       firmware.bin
               1         399    2009-01-01 00:01:37       config.text
-----------------------------------------------------------------
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.
```

Enter theroot directory of SD card:

DES-7200#**cd** sd0:/

Confirm the current path:

```
DES-7200#pwd
sd0:/
```

Create backup directory on the SD card:

```
DES-7200#mkdir backup
```

Make sure that the direcotry is created successfully:

```
DES-7200#dir
Directory of sd0:/
    Mode Link         Size                      MTime         Name
-------- ---- --------- ------------------- ------------------
    <DIR>     1      343040 2009-01-01 02:02:59       backup
-----------------------------------------------------------------
```

3 Files (Total size 11181455 Bytes), 0 Directories.

Total 33030144 bytes (31MB) in this device, 20492288 bytes (19MB) available.

Copy the file to the SD card:

DES-7200# copy flash:/config.text backup/config.text

Check the result:

DES-7200#dir backup

```
Directory of sd0:/backup
   Mode Link     Size             MTime     Name
-------- ---- --------- -------------------
------------------
          1      399   2009-01-01 00:01:37  config.text
-----------------------------------------------------------
----
Total 33030144 bytes (31MB) in this device, 20488192 bytes
(19MB) available.
```

1.3.7 Copying Files between USB and SD Card

The following example shows how to copy firmware_10_4.bin from U-shaped disc to SD card:

Check the available space on the SD card:

DES-7200#dir sd0:/

Directory of sd0:/

Mode Link Size MTime Name

-------- ---- --------- ------------------- ------------------

<DIR> 2 0 2035-02-11 23:24:34 backup/

1 7650112 2035-02-11 23:42:25 firmware.bin

---

1 Files (Total size 7650112 Bytes), 1 Directories.

Total 528482304 bytes (504MB) in this device, 475058176 bytes (453MB) available.

Copy the file from U-shaped disc to SD card:

DES-7200#copy usb0:/firmware_10_4.bin sd0:/firmware_10_4.bin

[OK 7,650,112 bytes]

Check the result:

DES-7200#dir sd0:/

Directory of sd0:/

Mode	Link	Size	MTime	Name
<DIR>	2	0	2035-02-11 23:24:34	backup/
	1	7650112	2035-02-11 23:42:25	firmware.bin
	1	7650112	2035-02-11 23:47:36	firmware_10_4.bin

2 Files (Total size 15300224 Bytes), 1 Directories.

Total 528482304 bytes (504MB) in this device, 459571200 bytes (438MB) available.

Copy the file from SD card to U-shaped disc:

DES-7200#copy sd0:/firmware_10_4.bin usb0:/new_firmware.bin

[OK 7,650,112 bytes]

Check the result:

DES-7200#dir usb0:/

Directory of usb0:/

Mode	Link	Size	MTime	Name
	1	7650112	2035-02-11 23:49:21	new_firmware.bin
	1	7650112	2035-02-11 23:45:42	firmware_10_4.bin

2 Files (Total size 15300224 Bytes), 0 Directories.

Total 528482304 bytes (504MB) in this device, 451784704 bytes (430MB) available.

1.3.8 Copying Files from the Primary Control Module to the Secondary Control Module

The following example shows how to copy firmware_10_4.bin from the primary control module to the secondary control module:

Check the FLASH space on the secondary control module:

```
DES-7200#dir slave:/
Directory of slave:/
   Mode Link     Size             MTime     Name
-------- ---- --------- -------------------
------------------
           1   11014633  2006-01-01 08:00:46  firmware.bin
           1    399      2006-01-01 08:01:37  config.text
------------------------------------------------------------
----
2 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 20488192 bytes
(19MB) available.
```

Copy firmware_10_4.bin from the primary control module to the secondary control module:

```
DES-7200#copy firmware_10.4.bin slave:/
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [ok 10,234,345 bytes]
```

Check the result:

```
DES-7200#dir slave:/
Directory of slave:/
   Mode Link     Size                MTime     Name
-------- ---- --------- -------------------
------------------
          1     11014633   2006-01-01 08:00:46  firmware.bin
          1     11025788   2008-01-01 08:00:46
firmware_10.4.bin
          1     399        2006-01-01 08:01:37  config.text
------------------------------------------------------------
----
3 Files (Total size 11181455 Bytes), 0 Directories.
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB)
available
```

1.3.9 Deleting Directories

The following example shows how to delete an unempty aaa directory:

Show the current directory status:

```
DES-7200#dir
Directory of flash:/
   Mode Link     Size                MTime     Name
-------- ---- --------- -------------------
------------------
          1      11014633 2006-01-01 08:00:46  firmware.bin
 <dir>    1      0        2006-01-01 08:00:00 aaa/
          1      399      2006-01-01 08:01:37 config.text
-----------------------------------------------------------
----
2Files (Total size 11015032 Bytes), 1 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB)
available
```

Check whether there is a file in aaa directory:

```
DES-7200#dir aaa
Directory of flash:/aaa
   Mode Link     Size                MTime     Name
-------- ---- --------- -------------------
------------------
         1         149  2006-01-01 08:01:37 backup.txt
-----------------------------------------------------------
----
1Files (Total size 149 Bytes), 0 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB)
available
```

The aaa directory is not empty. Delete the files first:

```
DES-7200# delete aaa/backup.txt
```

Delete the empty directory:

```
DES-7200# rmdir aaa
```

Check the result:

```
DES-7200#dir
Directory of flash:/
   Mode Link     Size                MTime     Name
-------- ---- --------- -------------------
------------------
         1     11014633 2006-01-01 08:00:46  firmware.bin
         1     399      2006-01-01 08:01:37 config.text
```

```
-------------------------------------------------------------
----
2Files (Total size 11015032 Bytes), 0 Directories
Total 33030144 bytes (31MB) in this device, 9563693 bytes (9MB)
available
```

2 Configuration File Management

2.1 Introduction to Configuration File Management

2.1.1 Overview

Along with the instant development of network, the network environment is getting more and more complicated, resulting more and more configuration information and higher and higher requirements on the network administrator. The change in configuration information may lead to unpredictable impacts on the entire network. Therefore, the monitoring of configuration change is of crucial importance. Currently, we can only determine whether the configurations have been change by copying the current running configuration file (running-config) and start-up configuration file (startup-config) and comparing the difference in command lines of both files. Although such a method can help identify changes in the configuration, there are still many defects. For example: the sequence of configuration changes cannot be identified; the network administrator cannot be notified in a timely manner; the relevant responsible personnel cannot be identified in the event of network failure caused by such configuration change. The configuration file management can remind the administrator of such configuration change through messages or logs, and also allows the comparison of configuration file.

2.1.2 Basic Characteristics

Configuration file management involves such basic characteristics as configuration change messaging/logging and configuration file comparison.

2.1.2.1 Configuration Change Logging

Configuration Change Logging provides a new approach for determining whether the configurations have changed. This approach can track the time of configuration change, configuration contents and the user making such configuration change, and it can also notify the network administrator in a real-time way.

2.1.2.2 Configuration File Comparison

The configuration file comparison function allows line-by-line configuration information comparison between two specified configuration files, and will output the configuration information which only exists in one of two configuration files. Through this function, the user can intuitively view added and deleted configuration information on the terminal.

2.1.3 Working Principle

By tracking each command applied, the system will log the corresponding user name, corresponding time, commands configured, configuration mode and etc, and then send the log to the remote log server through the notification mechanism. By looking up these records, we will understand whether the configurations have been changed, what the changes are and which user made such change.

There are two ways of configuration file comparison: 1) comparing the difference between two specified configuration files (the output difference information includes added and deleted configuration information: "+" mark for added information and "-" mark for deleted information); 2) comparing the difference between the specified configuration file and the existing configurations running on the device (the output difference information is the added configuration information in the specified configuration file).

Premises for using this function:

1) The format of the specified configuration file must meet the format requirements for configuration file (i.e., it can be used as the boot-up configuration file after being loaded into system flash).

2) The system memory must be larger than the size of two specified configuration files.

2.1.4 Protocol Specification

NA

2.2 Default Configurations

The following table describes the default configurations of configuration file management.

Function	Default setting
Configuration change logging	Disabled
Configuration change notification	Disabled
Entries reserved in the configuration log	100

2.3 Configure Configuration Change Logging

- (Required) Enable configuration change logging
- (Optional) Specify the maximum entries reserved in the configuration log
- (Optional) Enable key hiding
- (Optional) Enable configuration change notification
- View configuration change log information

2.3.1 Enable Configuration Change Logging

By default, the configuration change logging function is disabled. Enter privilege mode and execute the following steps to enable configuration change logging function.

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **archive**	Enter archive configuration mode.
DES-7200(config-archive)# **log config**	Enter archive log configuration mode.
DES-7200(config-archive-log-config)# **logging enable**	Enable configuration change logging.

To disable configuration change logging, execute "no logging enable" command in "log config" configuration mode.

Configuration example:

Enable configuration change logging.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# archive
DES-7200(config-archive)# log config
DES-7200(config-archive-log-config)# logging enable
```

2.3.1.1 Specify the Maximum Number of Entries Reserved in the Configuration Log

By default, the maximum number of entries reserved in the configuration log is 100. Enter privilege mode and execute the following steps to specify the maximum number of entries reserved in the configuration log.

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **archive**	Enter archive configuration mode.
DES-7200(config-archive)# **log config**	Enter archive log configuration mode.
DES-7200(config-archive-log-config)# **logging size** *entries*	Specify the maximum number of entries reserved in the configuration log (1-1000). The default value is 100.

To restore to the default setting, execute "no logging size" command in "log config" configuration mode.

Configuration example:

Specify the maximum number of entries reserved in the configuration log to 50.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# archive
DES-7200(config-archive)# log config
DES-7200(config-archive-log-config)# logging size 50
```

2.3.1.2 Enable Key Hiding

By default, keys are displayed in the configuration log. Enter privilege mode and execute the following steps to hide keys contained in the configuration log.

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **archive**	Enter archive configuration mode.
DES-7200(config-archive)# **log config**	Enter archive log configuration mode.
DES-7200(config-archive-log-config)# **hidekeys**	Hide keys contained in the configuration log.

To restore to the default setting, execute "no hidekeys" command in "log config" configuration mode.

Configuration example:

Hide keys contained in the configuration log.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# archive
DES-7200(config-archive)# log config
DES-7200(config-archive-log-config)# hidekeys
```

2.3.1.3 Enable Configuration Change Notification

By default, the configuration change notification function is disabled. Enter privilege mode and execute the following steps to enable configuration change notification function.

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **archive**	Enter archive configuration mode.
DES-7200(config-archive)# **log config**	Enter archive log configuration mode.
DES-7200(config-archive-log-config)# **notify syslog**	Enable configuration change notification.

To restore to the default setting, execute "no notify syslog" command in "log config" configuration mode.

Configuration example:

Enable configuration change notification.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# archive
DES-7200(config-archive)# log config
DES-7200(config-archive-log-config)# notify syslog
```

2.3.1.4 View Configuration Change Log Information

The following commands are provided to display configuration log information and memory usage status.

Command	Function
DES-7200# **show archive log config** {{**all** | *start-num* [*end-num*]} [**provisioning** | **contenttype** [**plaintext**]] | **statistics**}	Display configuration log information and memory usage status.

2.4 Configuration File Comparison

- Display the difference between two specified configuration files
- Display the difference between the specified configuration file and the existing configurations running on the device

2.4.1 Display the Difference Between Two Specified Configuration Files

Enter privilege mode and execute the following steps to display the difference between two specified configuration files:

Command	Function
show archive config differences [[*file1*] *file2*]	Display the difference between file1 and file2 by taking file1 as the base file.

If file1 and file2 are not specified, then the system will assume file1 as the existing configurations running on the device and file2 as the config.text in flash; if only file2 is specified, then the system will assume file1 as the existing configurations running on the device.

Configuration example 1:

Display the difference between config.bak and config.text in flash.

```
DES-7200# show archive config differences flash:config.bak flash:config.text
```

Configuration example 2:

If the configuration file is stored on the server or other network device, you can use TFTP to download to the local device before comparison. For example, to compare configbak.text on server 192.168.12.11 with config.text in the flash, assuming that configbak.text and config.text contain the following configuration information:

configbak.text	config.text
ip dhcp snooping information option ip dhcp snooping bootp-bind interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping limit rate 1000 ip dhcp snooping suppression snmp-server host 1.1.1.2 traps public snmp-server enable traps	ip dhcp snooping verify mac-address ip dhcp snooping information option interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping suppression snmp-server host 1.1.1.1 traps public snmp-server enable traps

```
DES-7200# show archive config differences flash:config.text
tftp://192.168.12.11/configbak.text
```

```
    + ip dhcp snooping bootp-bind
    interface GigabitEthernet 0/3
    +ip dhcp snooping limit rate 1000
  +snmp-server host 1.1.1.2 traps public
    -ip dhcp snooping verify mac-address
-snmp-server host 1.1.1.1 traps public
```

2.4.2 Display the Difference Between the Specified Configuration File and the Existing Configurations

Enter privilege mode and execute the following steps to display the difference between the specified configuration file and the existing configurations running on the device:

Command	Function
show archive config incremental-diffs [*file*]	Display the difference between file and the existing configurations running on device based on the parameter *file*.

If *file* is not specified, then the system will assume *file* as config.text in the flash.

Configuration example 1:

Display the difference between config.bak in flash and the existing configurations running on the device.

```
DES-7200# show archive config incremental-diffs flash:config.bak
```

Configuration example 2:

If the configuration file is stored on the server or other network device, you can use TFTP to download to the local device before comparison. For example, to compare configbak.text on server 192.168.12.11 with the existing configurations running on the device (in order to understand which configurations have been added), assuming that configbak.text and the existing configurations running on the device contain the following configuration information:

configbak.text	Existing configurations
ip dhcp snooping information option	ip dhcp snooping verify mac-address

ip dhcp snooping bootp-bind interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping limit rate 1000 ip dhcp snooping suppression snmp-server host 1.1.1.2 traps public snmp-server enable traps	ip dhcp snooping information option interface GigabitEthernet 0/3 ip dhcp snooping trust ip dhcp snooping suppression snmp-server host 1.1.1.1 traps public snmp-server enable traps

Display the difference between the specified configuration file and the existing configurations running on the device.

```
DES-7200# show archive config incremental-diffs tftp://192.168.12.11/configbak.text

    ip dhcp snooping bootp-bind
    interface GigabitEthernet 0/3
     ip dhcp snooping limit rate 1000
    snmp-server host 1.1.1.2 traps public
```

2.5 Typical Example of Configuration File Management

2.5.1 Networking Requirements

To timely track the configuration changes, assuming that the network administrator has the following needs:

1) Enable configuration change logging;

2) Specify the maximum number of entries reserved in the configuration log to 1000;

3) Hide keys contained in the configuration log;

4) Send configuration change log to the remote log server (IP: 192.168.12.11);

2.5.2 Network Topology

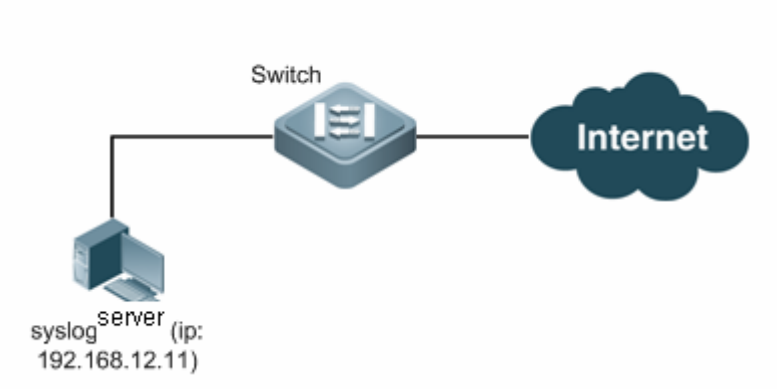


Fig 1 Configuration change log networking diagram

2.5.3 Configuration Tips

NA

2.5.4 Configuration Steps

1) Enable configuration change logging;

Enable configuration change logging function to track configuration changes

```
DES-7200# configure terminal
DES-7200(config)# archive
DES-7200(config-archive)# log config
DES-7200(config-archive-log-config)# logging enable
```

2) Specify the maximum number of entries reserved in the configuration log to 1000;

Specify the maximum number of entries reserved in the configuration log

```
DES-7200(config-archive-log-config)# logging size 1000
```

3) Hide keys contained in the configuration log

Hide keys contained in the configuration log

```
DES-7200(config-archive-log-config)# hidekeys
```

4) Send configuration change log to the remote log server (IP: 192.168.12.11)

Enable the function to send configuration change log to the remote log server

```
DES-7200(config-archive-log-config)# notify syslog
```

Configure remote log server

```
DES-7200(config-archive-log-config)# exit
DES-7200(config-archive)# exit
```

```
DES-7200(config)# logging server 192.168.12.11
```

2.5.5 Verification

View configuration log information

```
DES-7200(config)# show archive log config all

    idx   sess     user@line     datetime             logged command
      1     1   unknown@console  Mar 21 09:57:22   |  logging enable
      2     1   unknown@console  Mar 21 09:59:42   |  logging size 1000
      3     1   unknown@console  Mar 21 10:02:12   |  hidekeys
      4     1   unknown@console  Mar 21 10:02:26   |  notify syslog
      5     1   unknown@console  Mar 21 10:02:50   |  exit
      6     1   unknown@console  Mar 21 10:03:01   |  exit
```

View configuration log memory usage status

```
DES-7200(config)# show archive log config statistic

     Config Log Session Info:
        Number of sessions being tracked: 1
        Memory being held: 1270 bytes
        Total memory allocated for session tracking: 1270 bytes
        Total memory freed from session tracking: 0 bytes
   Config Log log-queue Info:
      Number of entries in the log-queue: 3
      Memory being held in the log-queue: 671 bytes
      Total memory allocated for log entries: 671 bytes
      Total memory freed from log entries: 0 bytes
```

3 System Management Configuration

3.1 CPU Utilization Display

3.1.1 Configuration Task List

- Show CPU utilization
- Configure CPU log limit threshold

3.1.2 Showing CPU Utilization

Use the **show cpu** command to show the total CPU utilization and the CPU utilization per process:

Command	Function
DES-7200# **show cpu**	Show CPU utilization.

By default, the switch name is DES-7200.

Below is the result of executing this command:

```
DES-7200#show cpu

 =====================================

     CPU Using Rate Information

 CPU utilization in five seconds: 25%

 CPU utilization in one minute  : 20%

 CPU utilization in five minutes: 10%

   NO   5Sec   1Min   5Min   Process

   0     0%     0%     0%    LISR INT

   1     7%     2%     1%    HISR INT

   2     0%     0%     0%    ktimer

   3     0%     0%     0%    atimer
```

```
  4     0%    0%    0%   printk_task
  5     0%    0%    0%   waitqueue_process
  6     0%    0%    0%   tasklet_task
  7     0%    0%    0%   kevents
  8     0%    0%    0%   snmpd
  9     0%    0%    0%   snmp_trapd
 10     0%    0%    0%   mtdblock
 11     0%    0%    0%   gc_task
 12     0%    0%    0%   Context
 13     0%    0%    0%   kswapd
 14     0%    0%    0%   bdflush
 15     0%    0%    0%   kupdate
 16     0%    3%    1%   ll_mt
 17     0%    0%    0%   ll main process
 18     0%    0%    0%   bridge_relay
 19     0%    0%    0%   d1x_task
 20     0%    0%    0%   secu_policy_task
 21     0%    0%    0%   dhcpa_task
 22     0%    0%    0%   dhcpsnp_task
 23     0%    0%    0%   igmp_snp
 24     0%    0%    0%   mstp_event
 25     0%    0%    0%   GVRP_EVENT
 26     0%    0%    0%   rldp_task
 27     0%    2%    1%   rerp_task
 28     0%    0%    0%   reup_event_handler
 29     0%    0%    0%   tpp_task
 30     0%    0%    0%   ip6timer
 31     0%    0%    0%   rtadvd
 32     0%    0%    0%   tnet6
```

```
33    2%    0%    0%    tnet

34    0%    0%    0%    Tarptime

35    0%    0%    0%    gra_arp

36    0%    0%    0%    Ttcptimer

37    8%    1%    0%    ef_res

38    0%    0%    0%    ef_rcv_msg

39    0%    0%    0%    ef_inconsistent_daemon

40    0%    0%    0%    ip6_tunnel_rcv_pkt

41    0%    0%    0%    res6t

42    0%    0%    0%    tunrt6

43    0%    0%    0%    ef6_rcv_msg

44    0%    0%    0%    ef6_inconsistent_daemon

45    0%    0%    0%    imid

46    0%    0%    0%    nsmd

47    0%    0%    0%    ripd

48    0%    0%    0%    ripngd

49    0%    0%    0%    ospfd

50    0%    0%    0%    ospf6d

51    0%    0%    0%    bgpd

52    0%    0%    0%    pimd

53    0%    0%    0%    pim6d

54    0%    0%    0%    pdmd

55    0%    0%    0%    dvmrpd

56    0%    0%    0%    vty_connect

57    0%    0%    0%    aaa_task

58    0%    0%    0%    Tlogtrap

59    0%    0%    0%    dhcp6c

60    0%    0%    0%    sntp_recv_task

61    0%    0%    0%    ntp_task
```

```
62    0%    0%    0%   sla_deamon

63    0%    3%    1%   track_daemon

64    0%    0%    0%   pbr_guard

65    0%    0%    0%   vrrpd

66    0%    0%    0%   psnpd

67    0%    0%    0%   igsnpd

68    0%    0%    0%   coa_recv

69    0%    0%    0%   co_oper

70    0%    0%    0%   co_mac

71    0%    0%    0%   radius_task

72    0%    0%    0%   tac+_acct_task

73    0%    0%    0%   tac+_task

74    0%    0%    0%   dhcpd_task

75    0%    0%    0%   dhcps_task

76    0%    0%    0%   dhcpping_task

77    0%    0%    0%   dhcpc_task

78    0%    0%    0%   uart_debug_file_task

79    0%    0%    0%   ssp_init_task

80    0%    0%    0%   rl_listen

81    0%    0%    0%   ikl_msg_operate_thread

82    0%    0%    0%   bcmDPC

83    0%    0%    0%   bcmL2X.0

84    3%    3%    3%   bcmL2X.0

85    0%    0%    0%   bcmCNTR.0

86    0%    0%    0%   bcmTX

87    0%    0%    0%   bcmXGS3AsyncTX

88    0%    2%    1%   bcmLINK.0

89    0%    0%    0%   bcmRX

90    0%    0%    0%   mngpkt_rcv_thread
```

```
 91     0%     0%     0%    mngpkt_recycle_thread

 92     0%     0%     0%    stack_task

 93     0%     0%     0%    stack_disc_task

 94     0%     0%     0%    redun_sync_task

 95     0%     0%     0%    conf_dispatch_task

 96     0%     0%     0%    devprob_task

 97     0%     0%     0%    rdp_snd_thread

 98     0%     0%     0%    rdp_rcv_thread

 99     0%     0%     0%    rdp_slot_change_thread

100     4%     2%     1%    datapkt_rcv_thread

101     0%     0%     0%    keepalive_link_notify

102     0%     0%     0%    rerp_msg_recv_thread

103     0%     0%     0%    ip_scan_guard_task

104     0%     0%     0%    ssp_ipmc_hit_task

105     0%     0%     0%    ssp_ipmc_trap_task

106     0%     0%     0%    hw_err_snd_task

107     0%     0%     0%    rerp_packet_send_task

108     0%     0%     0%    idle_vlan_proc_thread

109     0%     0%     0%    cmic_pause_detect

110     1%     1%     1%    stat_get_and_send

111     0%     1%     0%    rl_con

112    75%    80%    90%    idle
```

As shown in the above, the first three lines indicate the total CPU utilization in the last 5 seconds, 1 minute and 5 minutes respectively, including LISR, HISR and task. Below detains CPU utilization, where:

- No: number
- 5Sec: CPU utilization in the last 5 seconds
- 1Min: CPU utilization in the last 1 minute
- 5Min: CPU utilization in the last 5 minutes

- Process: process name

The first two lines indicate the CPU utilization of all LISRs and the CPU utilization of all HISRs respectively. All the lines starting the third line indicate the CPU utilization of processes. The last line indicates the CPU utilization of idle process. As with System Idle Process under Windows, it indicates an idle status. The above example shows that the CPU utilization of idle processes in the last 5 seconds is 75%, meaning that 75% CPU is available.

3.1.3 Configuring CPU Log Limit Threshold

To configure the CPU log limit threshold, execute the following command:

Command	Function
cpu-log log-limit *low_num high_num*	Configure the CPU log limit threshold.

By default the upper threshold is 100% and the lower threshold is 90%.

The following example sets the lower threshold to 70% and the higher threshold to 80%:

```
DES-7200# configure terminal                    // Enter the global configuration mode
DES-7200(config)# cpu-log log-limit 70 80    // Configure the CPU logging trigger threshold
```

If the CPU utilization is higher than 80%, the system prompts:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute : 95% , Using most cpu's task is ktimer : 94%
```

If the CPU utilization is lower than 70%, the system prompts:

```
Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: CPU utilization in one minute :68% , Using most cpu's task is ktimer : 60%

Oct 20 15:47:01 %SYSCHECK-5-CPU_USING_RATE: The CPU using rate has down!
```

3.2 System Memory Display

3.2.1 Configuration Task List

- Show the usage of system memory
- Configure the memory-lack exit-policy
- Show the usage of the protocol memory

3.2.2 Showing the Usage of System Memory

Use the **show memory** command to show the usage and status of system memory:

Command	Function
DES-7200# **show memory**	Show the usage of system memory.

By default, the switch name is DES-7200.

Below is the result of executing this command:

```
DES-7200#show memory

System Memory Statistic:

  Free pages: 13031

  watermarks : min 378, lower 756, low 1534, high 1912

  System Total Memory : 128MB, Current Free Memory : 54892KB

  Used Rate : 58%
```

The above information includes the following parts:

1. Free pages: the memory size of one free page is about 4k;

2. Watermarks(see the following table)

Parameter	Description
min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fail to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One route protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the **memory-lack exit-policy** command.
low	The memory resources are insufficient. The route protocol will be in OVERFLOW state if the low watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	A plenty of memory resources. Each route protocol attempts to restore the state from OVERFLOW to normal.

3. System total memory, current free memory and used rate.

3.2.3 Configuring the memory-lack exit-policy

Use the **memory-lack exit-policy** command to configure the exit policy of the route protocol if the lower watermark has been reached. The route protocol includes BGP, OSPF, RIP, PIM-SM.

memory-lack exit-policy [**bgp**|**ospf**|**pim-sm**|**rip]**

Command	Function
DES-7200(config)# **memory-lack exit-policy** [**bgp**|**ospf**|**pim-sm**|**rip**]	Configure the exit policy of the route protocol if the lower watermark has been reached.

Use the **no memory-lack exit-policy** command to restore the default configuration. By default, if the memory size reaches the lower watermark, the protocol that occupies the most memory exits.

If the system free memory decreases to the lower watermark, the system will disable one route protocol, releasing the memory resources to ensure the normal operation of other protocols.

You shall know what route protocols support the major network service. If the memory resources lack, you can disable the most unimportant protocol to ensure the normal operation of the major services.

For example, in a user network, the routes BGP learned are irrelevant to the major network service, you can use the **memory-lack exit-policy bgp** command.

Specifying the disabled route protocol as the exit policy can not help the system obtain enough memory resources.

3.2.4 Showing the Usage of the protocol memory

Use the **show memory protocol** command to display the usage of the memory protocol.

Below is the result of executing this command:

```
DES-7200# show memory protocols

================================

protocol      |memory(byte)

BGP            102000000

OSPF            24000000

RIP             10000000
```

PIM	50000000
LDP	20000000
Total	206000000

Caution

Different switches support different routing protocols, including BGP, OSPF, RIP, LDP, PIM, ISIS, and ect.

4 System Memory Display Configuration

4.1 System Memory Display Configuration Task List

- Show the usage of system memory
- Configure the memory-lack exit-policy
- Show the usage of the protocol memory

4.2 Showing the Usage of System Memory

Use the **show memory** command to show the usage and status of system memory:

Command	Function
DES-7200# **show memory**	Show the usage of system memory.

By default, the switch name is DES-7200.

Below is the result of executing this command:

```
DES-7200#show memory

System Memory Statistic:

  Free pages: 13031

  watermarks : min 378, lower 756, low 1534, high 1912

  System Total Memory : 128MB, Current Free Memory : 54892KB

  Used Rate : 58%
```

The above information includes the following parts:

1. Free pages: the memory size of one free page is about 4k;

2. Watermarks(see the following table)

Parameter	Description

Parameter	Description
min	The memory resources are extremely insufficient. It can only keep the kernel running. All application modules fail to run if the minimum watermark has been reached.
lower	The memory resources are severely insufficient. One route protocol will auto-exit and release the memory if the lower watermark has been reached. For the details, see the **memory-lack exit-policy** command.
low	The memory resources are insufficient. The route protocol will be in OVERFLOW state if the low watermark has been reached. In the overflow state, the routers do not learn new routes any more. The commands are not allowed to be executed when the memory lacks.
high	A plenty of memory resources. Each route protocol attempts to restore the state from OVERFLOW to normal.

3. System total memory, current free memory and used rate.

4.3 Configuring the memory-lack exit-policy

Use the **memory-lack exit-policy** command to configure the exit policy of the route protocol if the lower watermark has been reached. The route protocol includes BGP, OSPF, RIP, PIM-SM.

memory-lack exit-policy [**bgp**|**ospf**|**pim-sm**|**rip]**

Command	Function
DES-7200(config)# **memory-lack exit-policy** [**bgp**|**ospf**|**pim-sm**|**rip**]	Configure the exit policy of the route protocol if the lower watermark has been reached.

Use the **no memory-lack exit-policy** command to restore the default configuration. By default, if the memory size reaches the lower watermark, the protocol that occupies the most memory exits.

If the system free memory decreases to the lower watermark, the system will disable one route protocol, releasing the memory resources to ensure the normal operation of other protocols.

You shall know what route protocols support the major network service. If the memory

resources lack, you can disable the most unimportant protocol to ensure the normal operation of the major services.

For example, in a user network, the routes BGP learned are irrelevant to the major network service, you can use the **memory-lack exit-policy bgp** command.

Specifying the disabled route protocol as the exit policy can not help the system obtain enough memory resources.

4.4 Showing the usage of the protocol memory

Use the **show memory protocol** command to display the usage of the memory protocol.

Below is the result of executing this command:

```
DES-7200# show memory protocols

================================

protocol      |memory(byte)

BGP            102000000

OSPF            24000000

RIP             10000000

PIM             50000000

LDP             20000000
--------------------------------
Total          206000000
```

Caution

Different switches support different routing protocols, including BGP, OSPF, RIP, LDP, PIM, ISIS, and ect.

5 POE Management Configuration

5.1 Overview

PoE (Power Over Ethernet) is a mechanism that provides 45V~-57V DC to the remote PD devices (IP Phone, WLAN AP and Network Camera) via twisted pair cables.

The PSE (Power Sourcing Equipment) can transmit both data and current at the same time via Category 3/5 twisted pair cables (1, 3, 2, 6), with a maximum distance of 100m.

The switch supporting POE can provide the statistics of the power condition each port and the entire device, which can be shown by using a query command. At the same time, it also provides over-temperature protection. When the temperature inside the switch exceeds 80 Celsius degrees, the switch will trigger protection by turning off the PoE power supply to all ports. When the temperature inside the switch is lower than 60 Celsius degrees, the switch will restore the PoE power supply for all ports.

Caution

The POE line cards include7200-48P, 7200-24P, ect.

5.2 POE Configuration Management

This section includes:

- Remote power supply configuration
- Enable/disable the remote power supply of the port
- Set the minimum allowed voltage of the POE system
- Set the maximum allowed voltage of the POE system
- Set the power management mode of the switch
- Disconnection detection mode
- Show the port/system status

5.2.1 Remote power supply configuration

The switch supporting POE can automatically detect whether the device connected to a port is a standard PD device and supply power to the standard PD device.

You can enable or turn off the remote power supply of a port, set the minimum allowed voltage of the POE system, set the maximum allowed voltage of the POE system, set the power management mode of the switch, and set the disconnection detection mode by using the command line.

Table-1: Remote Power Supply Configuration

Device	Configuration	Default	Description
Switches supporting PoE	Enable/disable the PoE of the port	Disabled	-
	Set the maximum power of the power supply for the port	15.4w	-
	Set the minimum allowed voltage of the POE system	45v	-
	Set the maximum allowed voltage of the POE system	57v	-
	Power management mode of the switch	Auto	-
	Disconnection detection mode	AC	-
PD device	Correct connection with the electrical interface of the POE device	-	-

5.2.2 Enabling/Disabling the PoE of the Port

You can enable or disable the PoE feature of a port as needed by using the following commands. By default, the PoE is disabled. Please do the following configuration in the global mode.

Table-2: Enable/Disable the PoE Feature of a Port

Step 1	**Configure**	Enter the configuration mode
Step 2	**interface gigabitEthernet** *interface-id*	Select the port, enter the interface configuration mode, and specify the physical port to be configured.

Step 3	**poe enable** | **no poe enable**	Enable/disable the PoE of a port
Step 4	**End**	Return to privileged EXEC mode
Step 5	**show run**	Verify the configuration
Step 6	**copy running-config startup-config**	Save the settings into the parameter file.

For example, enable/disable the PoE of port 1 on line card 1:

```
DES-7200#
DES-7200# configure
DES-7200 (config)#interface gigabitEthernet  1/1
DES-7200(config-if)# poe enable
DES-7200(config-if)# no poe enable
DES-7200(config-if)# end
DES-7200#
```

5.2.3 Setting the Minimum Allowed Voltage of the POE System

Currently, the Ethernet port of the switch supporting POE can provide the minimum allowed voltage of 45V. You can set the minimum allowed voltage according to the actual need, within the range of 45000 mv to 47000 mv. When the output voltage is lower than the minimum allowed value due to reasons such as power faults, the equipment will automatically turn off the power supply of the devices connected to all ports.

You can use the following commands to set the minimum allowed voltage of the power supply of the port. Please do the following configuration in the global mode.

Table-3: Set the Minimum Allowed Voltage of the POE System

Step 1	**Configure**	Enter the configuration mode
Step 2	**poe-power lower** *lower* | **no poe-power lower**	Set the minimum allowed voltage of the POE system/restore the minimum allowed voltage to the default value
Step 3	**End**	Return to privileged EXEC mode
Step 4	**show run**	Verify the configuration
Step 5	**copy running-config startup-config**	Save the settings into the parameter file.

By default, the minimum output power of a port is 45v.

For example, set the minimum output power of the system to 46v.

```
DES-7200#
DES-7200# configure
```

```
DES-7200 (config)#poe-power lower 46
DES-7200 (config)# end
DES-7200#
```

5.2.4 Setting the Maximum Allowed Voltage of the POE System

The Ethernet port of the switch supporting POE can provide the maximum allowed voltage of 57V. You can set the maximum allowed voltage according to the actual need, within the range of 55000 mv~57000 mv. When the output voltage is higher than the maximum allowed value due to reasons such as power faults, the equipment will automatically turn off the power supply of the devices connected to all ports.

You can use the following commands to set the maximum allowed voltage of the power supply of the port. Please do the following configuration in the global mode.

Table-4: Set the Maximum Allowed Voltage of the POE System

Command	Description
Configure	Enter the configuration mode
poe-power upper *upper* | **no poe-power upper**	Set the maximum allowed voltage of the POE system/restore the maximum allowed voltage to the default value
End	Return to privileged EXEC mode
show run	Verify the configuration
copy running-config startup-config	Save the settings into the parameter file.

By default, the maximum output power of a port is 57v.

For example, set the maximum output power of the system to 56v.

```
DES-7200#
DES-7200# configure
DES-7200 (config)#poe-power upper 56
DES-7200(config-if)# end
DES-7200#
```

5.2.5 Setting the Power Management Mode of the Switch

The power management mode of the switch is used to allocate the power to the PD devices. When one PD device is connected to the equipment if the current power allocated has not exceeded the no_connect limit, the equipment will allocate power to the external PD device according to the power supply management mode. (POE has

one limit: no_connect. When the power allocated from the equipment exceeds the no_connect limit, the equipment will not supply power to any new PD devices.)

Currently, the PoE device uses the auto power management mode.

In the Auto mode, the power is allocated according to the detected port PD type. In the Auto mode, the equipment allocates power to classes 1~3 PD devices as follows: class1~4W, class2~7W, class3~15.4W and class0~15.4W.

This configuration is automatically performed by the switch without any user intervention.

5.2.6 Disconnect Detection Mode

The equipment supporting POE checks whether a previously connected device has been disconnected by using disconnect detection. The equipment supports two detection modes: AC and DC. AC detection mode deems that the connected PD device is disconnected when the current of a port is smaller than a fixed value for the specified period. DC detection mode works by detecting the voltage feature of the port.

You can use the following command to set the disconnect detection mode. Please make the following configuration in the global mode. You can also set this mode for a particular device.

Table-5: Disconnect Detection Mode

Command	Description
Configure	Enter the configuration mode
Poe disconnect-mode {**ac** | **dc**} | **no poe disconnect-mode**	Set the disconnect detection mode/restore the disconnect detection mode to the default value
End	Return to privileged EXEC mode
show run	Verify the configuration
copy running-config startup-config	Save the settings into the parameter file.

By default, the disconnection detection mode is the AC mode.

For example, set the disconnect detection mode to DC:

```
DES-7200#
DES-7200# configure
DES-7200 (config)#poe-disconnect-mode dc
DES-7200(config-if)# end
DES-7200#
```

5.2.7 Showing the Power Supply Status of the Port/System

The equipment supporting POE will scan the ports and the status of the entire POE system at periodical intervals, and save all the status information. You may view interface status by using **show** in privileged EXEC mode.

Command	Description
show poe interfaces gigabitEthernet [*interface-id*]	Show the power supply status of the specified port
show poe interfaces	Show the power supply status of all POE ports (the 24 ports depending on the power supply of the POE system)
show poe powersupply	Show the power supply status of the entire POE system
show running-config interface [*interface-id*]	Show the configuration of the current running interface.

For example, show the power status of the gigabitethernet 0/2 port:

```
Interface : Gi0/2
Port power enabled : ENABLE
Port connect status : OFF
Port PD Class : no PD devices
Port max power : 15.4W
Port current power : 0 mW
Port peak power : 0 mW
Port current : 0 mA
Port voltage : 48V
Port trouble cause : normal
```

Note: Port trouble cause means the power-off cause, as below:

Port trouble cause	Description
Normal	Normal power supply (LED green); AC/DC detects that the equipment is disconnected (LED off), Disable (LED off)
Overload during start-up	Power supply start-up, finding that the current is too large or is disconnected (LED orange)
port off due to overload event	PD device is disconnected due to overload (LED orange)
short circuit event	PD device is disconnected due to short circuit (LED red)
voltage is out of established bounds	Output voltage is turned off due to out of bounds (LED red)

Port trouble cause	Description
temperature rise too high	Turned off due to high-temperature protection (LED red)
power overload	Turned off due to power management (LED orange)

The following example shows the power supply status of the POE system:

```
DES-7200#show poe powersupply

PSE Total Power :1200.0 W
PSE Total Power Consumption : 0 W
PSE Available Power : 1200.0 W
PSE Peak Value : 0 W
PSE Min Allow Voltage : 45 V
PSE Max Allow Voltage : 57 V
PSE Disconnect Sense Mode : ac
```

6 Syslog Configuration

6.1 Overview

During the operation of a device, there are various state changes, such as the link status up/down, and various events occurring, such as receiving abnormal messages and handling abnormities. Our product provides a mechanism to generate messages of fixed format (log message) in case of status change or event occurring. These messages can be displayed in related windows (console, VTY, etc.) or recorded in related media (memory buffer, FLASH), or sent to a group of log servers in the network for the administrators to analyze and locate problems. Meanwhile, in order to make it easy for administrators to read and manage log messages, these log messages can be labeled time stamps and serial numbers, and is graded according to the priority of log information.

6.1.1 Log Message Format

The format of the our log message is as follows:

<priority> seq no: timestamp sysname: %severity

%ModuleName-severity-MNEMONIC: description

They are: <priority> Sequential number timestamp device name module name-severity – information type: abbre: information contents

Priority value = Device value *8 + Severity

For example:

```
<189> 226:Mar  5 02:09:10 DES-7200 %SYS-5-CONFIG_I: Configured from console
by console
```

Caution

The priority field is not attached to the log messages that are printed in the user window. It only appears in the log messages that are sent to the syslog server.

6.2 Log Configuration

6.2.1 Log Switch

The log switch is turned on by default. If it is turned off, the device will not print log information in the user window, or send log information to the syslog server, or record the log information in the related media (memory buffer, flash).

To turn on or off the log switch, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **logging on**	Turn on the log switch
DES-7200(config)# **no logging on**	Turn off the log switch

Caution

Do not turn off the log switch in general case. If it prints too much information, you can reduce it by setting different displaying levels for device log information.

6.2.2 Configuring the Device Displaying the Log Information

When the log switch is turned on, the log information will be displayed on the console and also sent to different displaying devices. To configure different displaying devices for receiving logs, run the following commands in the global configuration mode or privileged level:

Command	Function
DES-7200(config)# **logging buffered** [*buffer-size* | *level*]	Record log in memory buffer
DES-7200# **termninal monitor**	Allow log to be displayed on VTY window
DES-7200(config)# **logging** *host*	Send log information to the syslog sever in the network
DES-7200(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Record log on extended FLASH

Logging Buffered will record log information in the memory buffer. The memory buffer for log is used in recycled manner. That is, when it is full, the oldest information will be overwritten. To show the log information in the memory buffer, run **show logging** at the privileged user level. To clear the log information in the memory buffer, run **clear logging** at the privileged user level.

Terminal Monitor allows log information to be displayed on the current VTY (such as the telnet window).

Logging Host specifies the address of the syslog server that will receive the log information. Our product allows the configuration of at most 5 syslog servers. The log information will be sent to all the syslog servers at the same time.

Caution

To send the log information to the syslog server, it is required to turn on the timestamp switch or sequential number switch of the log information. Otherwise, log information will not be sent to the syslog server.

Logging File Flash: Record log information in FLASH. The filename for log shall not have any extension to indicate the file type. The extension of the log file is fixed as txt. Any configuration of extension for the filename will be refused.

More flash: filename command shows the contents of the log file in the flash.

Caution

Some devices support extended FLASH. If the device has extended FLASH, the log information will be recorded there. If the device has no extended FLASH, the log information will be recorded in the serial FLASH.

6.2.3 Enabling the Log Timestamp Switch of Log Information

To add or delete timestamp in log information, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **service timestamps** *message-type* [**uptime** | **datetime**]	Enable the timestamp in the log information
DES-7200(config)# **no service timestamps** *message-type*	Disable the timestamp in the log information

The timestamp are available in two formats: device uptime and device datetime. Select the type of timestamp appropriately.

Message type: log or debug. The "log" type means the log information with severity levels 0-6. The "debug" type means that with severity level 7.

Caution

If the current device has no RTC, the configured time is invalid, and the device automatically uses the startup time as the timestamp for the log information.

6.2.4 Enabling Switches in Log System

By default, the system name is not included in the log information. To add or remove the system name in the log information, perform the following commands in the global configuration mode.

Command	Function
DES-7200(config)# **no service sysname**	Cancel the system name in the log message.
DES-7200(config)# **service sysname**	Add the system name to the log message.

6.2.5 Enabling Log Statistics

By default, the log statistics function is disabled. To enable or disable the log statistics function, perform the following commands in the global configuration mode.

Command	Function
DES-7200(config)# **no logging count**	Disable the log statistics function and delete the statistics information
DES-7200(config)# **logging count**	Enable the log statistics function

6.2.6 Enabling the Sequential Number Switch of Log Information

By default, the log information has no sequential number. To add or delete sequential number in log information, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **no service sequence-numbers**	Delete sequential number in the log messages
DES-7200(config)# **service sequence-numbers**	Add sequential number to the log messages

6.2.7 Configuring Synchronization Between User Input and Log Output

By default, user input is asynchronous with log output. User input is interrupted if the log is output when the user is keying in characters. Use this command to configure synchronization between user input and log output in the line configuration mode:

Command	nction
DES-7200(config-line)# **logging synchronous**	Set synchronization between user input and log output.
DES-7200(config)# **no logging synchronous**	Delete synchronization between user input and log output.

6.2.8 Configuring Log Rate Limit

By default, log rate is not limited. Use this command to configure log rate limit in the global configuration mode:

Command	unction
DES-7200(config)# **logging rate-limit** *number*	Set log rate limit.
DES-7200(config)# **no logging rate-limit**	Delete the setting of log rate limit.

6.2.9 Configuring the Log Information Displaying Level

To limit the number of log messages displayed on different devices, it is possible to set the severity level of log information that is allowed to be displayed on those devices.

To configure the log information displaying level, run the following command in the global configuration mode:

Command	Function
DES-7200(config)# **logging console** *level*	Set the level of log information that is allowed to be displayed on the console
DES-7200(config)# **logging monitor** *level*	Set the level of log information that is allowed to be displayed on the VTY window (such as telnet window)
DES-7200(config)# **logging buffered** [*buffer-size* | *level*]	Set the level of log information that is allowed to be recorded in memory buffer
DES-7200(config)# **logging file flash:***filename* [*max-file-size*] [*level*]	Set the level of log information that is allowed to be recorded in extended flash
DES-7200(config)# **logging trap** *level*	Set the level of log information that is allowed to be sent to syslog server

The log information of our products is classified into the following 8 levels:

Level Keyword	Level	Description
Emergencies	0	Emergency case, system cannot run normally
Alerts	1	Problems that need immediate remedy
Critical	2	Critical conditions
Errors	3	Error message
Warnings	4	Alarm information
Notifications	5	Information that is normal but needs attention
Informational	6	Descriptive information
Debugging	7	Debugging messages

Lower value indicates higher level. That is, level 0 indicates the information of the highest level.

When the level of log information that can be displayed is set for the specified device, the log information that is at or below the set level will be displayed. For example, after the command logging console 6 is executed, all log information at or below level 6 will be displayed on the console.

By default, the log information that is allowed to be displayed on the console is at level 7.

By default, the log information that is allowed to be displayed on the VTY window is at level 7.

By default, the log information that is allowed to be sent to the syslog server is at level 6.

By default, the log information that is allowed to be recorded in the memory buffer is at level 7.

By default, the log information that is allowed to be recorded in the extended flash is at level 6.

The privileged command show logging can be used to show the level of log information allowed to be displayed on different devices.

6.2.10 Configuring the log information device value

The device value is one of the parts that form the priority field in the messages sent to the syslog server, indicating the type of device that generates the information.

To configure the log information device value, run the following command in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **logging facility** *facility-type*	Configure the log information device value
DES-7200(config)# **no logging facility** *facility-type*	Restore the default of the log information device value

The meanings of various device values are described as below:

```
Numerical Code       Facility
         0           kernel messages
         1           user-level messages
         2           mail system
         3           system daemons
         4           security/authorization messages
         5           messages generated internally by syslogd
         6           line printer subsystem
         7           network news subsystem
         8           UUCP subsystem
         9           clock daemon
        10           security/authorization messages
        11           FTP daemon
        12           NTP subsystem
        13           log audit
        14           log alert
        15           clock daemon
        16           local use 0  (local0)
        17           local use 1  (local1)
        18           local use 2  (local2)
        19           local use 3  (local3)
        20           local use 4  (local4)
        21           local use 5  (local5)
        22           local use 6  (local6)
        23           local use 7  (local7)
```

The default device value of our products is 23.

6.2.11 Configuring the Source Address of Log Messages

By default, the source address of the log messages sent to the syslog server is the address of the port that sends the messages. It is possible to fix the source address for all log messages through commands.

It is possible to directly set the source IP address of the log messages or the remote port of the log messages.

To configure the source address of the log messages, run the following command in the global configuration mode:

Command	Function

Command	Function
DES-7200(config)# **logging source interface** *interface-type interface-number*	Configure the source port of log information
DES-7200(config)# **logging source ip** *A.B.C.D*	Configure the source IP address of log messages

6.2.12 Setting and Sending User Log

By default, no log is output when a user logs in or out and executes configuration commands. To output user login/logoff logs or configuration command logs, execute the following commands in the global configuration mode:

Command	Function
DES-7200(config)# **logging userinfo**	Set user login/logoff log.
DES-7200(config)# **logging userinfo command-log**	Send a log when a configuration command is executed

6.3 Log Monitoring

To monitor log information, run the following commands in the privileged user mode:

Command	Function
DES-7200# **show logging**	View the log messages in memory buffer as well as the statistical information of logs
DES-7200# **show logging count**	View the statistical information of logs in every modules
DES-7200# **clear logging**	Clear the log messages in the memory buffer
DES-7200# **more flash:***filename*	View the log files in the extended flash

Caution

The format of the timestamp in the output result of **show logging count** is the format in the latest log output.

6.3.1 Examples of Log Configurations

Here is a typical example to enable the logging function:

```
DES-7200(config)# interface gigabitEthernet 0/1
DES-7200(config-if)# ip address 192.168.200.42 255.255.255.0
```

```
DES-7200(config-if)# exit
DES-7200(config)# service sequence-numbers              //Enable sequence number
DES-7200(config)# service timestamps debug datetime     //Enable debug
information timestamp, in date format
DES-7200(config)# service timestamps log datetime       //Enable log information
timestamp, in date format
DES-7200(config)# logging 192.168.200.2                 //Specify the syslog
server address
logging trap debugging                                  //The log information of
all levels will be sent to syslog server
DES-7200(config)# end
```

7 Module Hot-Plugging/ Unplugging

7.1 Overview

Caution

The DES-7200 series switches support hot-plugging/unplugging of modules. You may plug and unplug modules while the device is powered on, without affecting the normal system operation or other modules.

7.2 Module Hot-Plugging/Unpluggin g Configuration

This chapter includes:

- Plugging or Unplugging Modules
- Installing or Uninstalling Modules
- View module information

7.2.1 Plugging or Unplugging Modules

You may plug or unplug modules while the device is operating (hot-plugging/unplugging). The operation of the other modules will not be affected. After the module is plugged in the slot, the management software of the device attempts to install its driver.

Caution

If the slot has been installed with another module driver, it is required to delete the original driver before installing the new module. You may execute the **show version module** command to get the related information.

Please plug the module tightly in the slot and tighten the screw. The module may not work well if it is loosely plugged.

You may plug modules while the switch is operating (hot-plugging/unplugging), which will not affect the operation of the other modules. The related configuration will be reserved when the module is unplugged, and it is possible to continue the setting of the module. When the module is re-plugged, the module will be automatically activated. All the configurations take effect automatically.

7.2.2 Installing or Uninstalling Modules

In addition to automatic installation of module driver after the module is plugged, you may also install the module driver manually. After the installation, all configurations for the slot will be done for the type of the installed module. Even if the module is unplugged, you can still configure it without loss of the configuration.

In the global configuration mode, execute the following commands to install a module manually:

Command	Meaning
configure terminal	Enter the global configuration mode.
install *slot-num moduletype*	Install the module of a specified type in a slot
end	Return to the privileged mode.

Caution

The installation of driver does not need physical presence of the module. This means that you may "pre-configure" the device. You may use the **install** command to virtualize the module of a specified type and then configure it. When the module is plugged, all configurations take effect automatically.

You can uninstall an operating module. Once uninstalled, all configurations for it will be lost, and the module is disabled. To restore that module, you may "install" its driver manually, or unplug and then plug it again.

In the global configuration mode, execute the following commands to uninstall a module manually:

Command	Meaning
configure terminal	Enter the global configuration mode.
no install *slot-num*	Uninstall the module in a slot
End	Return to the privileged mode.

7.2.3 Viewing module information

In the privileged user mode, execute the following commands to check the details of a

module so as to uninstall it manually:

Command	Meaning
show version module detail	View module information

```
DES-7200# show version module detail
Device  : 1
Slot    : 1
User Status:     installed
Software Status: ok
Online Module :
       Type    : 7200-24G
       Ports   : 24
       Version : 01-01-05-02
Configured Module :
    Type    : 7200-24G
    Ports   : 24
    Version : 01-01-05-02

Device  : 1
Slot    : 2
User Status:     installed
Software Status: ok
Online Module :
   Type    : 7200-2XG
    Ports   : 2
    Version : 01-01-05-02
Configured Module :
    Type    : 7200-2XG
    Ports   : 2
    Version : 01-01-05-02

Device  : 1
Slot    : 3
User Status:     installed
Software Status: ok
Online Module :
Type    : 7200-24
    Ports   : 24
    Version : 01-01-05-02
Configured Module :
    Type    : 7200-24
    Ports   : 24
    Version : 01-01-05-02

Device  : 1
Slot    : 4
User Status:     installed
    Software Status:  none
    Online Module :
    Type    :
```

```
Ports   : 0
Version :
Configured Module :
Type    : 7200-24
Ports   : 24
Version :
Device  : 1
Slot    : M1
Status  : master
Online Module :
Type    : 7200-CM1
Ports   : 0
Version : 01-01-05-02
```

8 LCD Configuration

8.1 Overview

The LCD display is a visual display that features simple and easy operation with buttons. The user can know the running status of the device at a glance even if the user has no knowledge about the CLI commands. When abnormity occurs with the device operation, the displaying immediately notifies the abnormity to the users.

The state information shown by the LCD includes the switch name, duration of work, CPU utilization ratio (Supervisor Engine), memory utilization ratio (Supervisor Engine), temperature (Supervisor Engine and Line Card), fan and the working state of power supplies.

Generally, the device prints the information circularly.

A user can use keys to show desired state information. The LCD provides the following four key:

- Menu key (Menu): Show a menu.
- Selection key (Enter): Select an item.
- Page Up key (Pgup): Page up.
- Page Down key (Pgdn): Page down,

When there is an unexpected condition in a module, for example, the CPU utilization ratio is too high, and then the LCD keeps showing the warning information. The information will not disappear from the display until the user pushes the selection key (enter).

8.1.1 LCD Key Introduction

When the switch prints state information circularly, each page displays for a fixed period. If a user pushes one of the four keys, then the following condition will occur.

1. Menu: Stop the current displaying and show the main menu. Stops showing the menu and shows the state beginning at this page.
2. Selection key (enter): The key does not work.
3. Page Up key (Pgup): Shows the content of the previous screen. If the information of a state is not fully shown in one screen, then it can be shown in multiple screens.

If the first screen is not currently shown, then push the key Pgup to show the previous screen of the current content. If the first screen is shown, then push the key Pgup to show the last screen of the state information.

4. Page Down key (Pgdn): Shows the content of next screen. If the information of a state is not fully shown in one screen, then it can be shown in multiple screens. If the last screen is not currently shown, then push the key Pgdn to show the next screen of the current content. If the last screen is shown, then push the key Pgdn to show the first screen of the state information.

Press Menu to show the main menu, and the selected line will be highlighted. If there is no button pressing operation, it returns to the circular displaying again and display the next screen since the previous displaying. If a key is pressed, the following condition may occur:

1. Menu: Stop the current displaying and show the main menu.
2. Selection key (enter): Select the currently selected menu item. If there is a submenu in the menu item, then the submenu is shown. If a menu item indicates the information of a state, then the state information is shown.
3. Page Up key (Pgup): Shows the content of the previous screen.

All the menu items of a menu page are circularly organized. The previous item of the first menu item is the last item. The next item of the last item is the first item. If a menu is currently shown and the selected menu is not in the first line of the screen, when you push the Pgup key, the content of the screen will not change, the selected menu item will move up a line and the selected line is still the first line.

The state information that menu items point to are also circularly organized. The previous screen of the first screen is the last screen and the next screen of the last screen is the first screen. If the content of a menu item is currently shown, then Pgup shows the content of the previous screen. When the content of a menu item is shown, push the key enter to return to the menu page.

4. Page Down key (Pgdn): Shows the content of next screen.

If a menu is currently shown and the selected menu is not in the last line of the screen, when you push the Pgdn key, the content of the screen will not change, the selected menu item will move down a line and the selected line is still the last line.

If the content of a menu item is currently shown, then Pgdn shows the content of the next screen. When the content of a menu item is shown, push the key enter to return to the menu page.

If warning messages are required to be shown in the LCD, then the display shows generated warning messages. If a warning message needs being shown in multiple screens, then the display shows the content of the warning message in screens circularly. If multiple warning messages are generated at the same time, then various

warning messages are shown in turn and then the content of the newest warning message is shown circularly. The condition will not end until the user types the selection key (enter) to stop showing the warning message. If you push one of the four keys when a warning is shown, the following condition will occur:

1. Menu key (Menu): Stops showing the warning message and begins to show the main mp
2. Selection key (enter): Stops showing the current warning message. If there is no updated warning message, then returns to the circular display mode. If there is an updated warning message, the new warning message is shown.
3. Page Up key (Pgup): All the warning messages are circularly organized. The previous screen of the first screen is the last screen of the previous warning message. The next screen of the last screen is the first item of the next warning message. Pgup shows the content of the previous screen. If the first screen of the first warning message is currently shown, the shown content will not change.
4. Page Down key (Pgdn): Warning messages are circularly organized. Pgdn shows the content of the next screen. If the last screen of the last warning message is currently shown, the shown content will not change.

8.2 LCD Configuration Task List

LCD can be used at once without configuration, but you can also modify the display parameters of LCD according to your actual needs. The following section describes the configuration options of LCD:

1. Configure LCD display language
2. Configure warning message queue length
3. Configure memory usage warning threshold

😐 Product Support	LCD configuration is only supported by DES-7200 series switch products.

8.2.1 Configuring LCD Display Language

To configure which language shall be used by LCD to display information, execute the following command in global configuration mode:

Command	Function

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **lcd language** { **chinese** | **english** }	Configure LCD display language.

To restore LCD display language to the default setting, execute "**no lcd language**" in global configuration mode.

Configuration example:

Configure LCD display language to English.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# lcd language english
```

Note

Apart from certain customized products, the LCD display language is by default Chinese.

8.2.2 Configuring Warning Information Queue Length

After the warning messages are generated, LCD will display the latest warning message all the while until the OK button is pressed. After that, you can browse history warning messages through the menu. Use this command to configure the number of warning messages. By default, our products can save 100 history warning messages. To configure the number of history warning messages, execute the following command in global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **lcd trap-number** *num*	Configure the number of warning messages.

To restore the number of history warning messages to the default setting, execute "**no trap-number**" command in global configuration mode.

Configuration example:

Configure to record 200 warning messages generated recently.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# lcd trap-num 200
```

8.2.3 Configuring Memory Usage Warning Threshold

System memory is an important resource in system operation. When the available system memory is insufficient, many important services won't be able to run normally. The continual drop in system memory may indicate certain faults. Therefore, the administrator generally expects that the device can give an alarm when system memory has dropped to a certain extent. The LCD module can give an alarm when the memory usage is excessively high.

By default, when system memory usage reaches 80%, the warning message will be displayed on the LCD, while you can also change this value through configuration. However, during system operation, transiently high memory usage may be encountered frequently (for example, memory-consuming calculation is running by this time), which shall be considered normal. Therefore, it is not suggested to set memory usage warning threshold to a low value in order to avoid frequent memory usage warning.

To configure memory usage warning threshold (%), execute the following command in global configuration mode:

Command	Function
DES-7200# **configure terminal**	Enter global configuration mode.
DES-7200(config)# **memory-rate rising-threshold** *num*	Configure memory usage warning threshold (%)

To restore memory usage warning threshold (%) to the default setting, execute "**no memory-rate rising-threshold**" command in global configuration mode.

Configuration example:

Configure to display the warning message when memory usage exceeds 60%.

```
DES-7200# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
DES-7200(config)# memory-rate rising-threshold 60
```

8.3 LCD Configuration Instance

Execute the following command to configure LCD display language:

```
DES-7200(config)# lcd language english              //Set display language to
English
```

Execute the following command to configure the number of history warning messages:

```
DES-7200(config)# lcd trap-number 200              //Set the number of history
warning messages to 200
```

Execute the following command to configure memory threshold:

```
DES-7200(config)# memory-rate rising-threshold 60 //Configure to give an alarm when
memory usage exceeds 60%
```

9 USB/SD Configuration

9.1 Overview

This document describes USB/SD storage devices (mainly U disk/SD). The system only recognizes the U-disk/SD card partitioned by FAT. Other file systems cannot be identified.

After inserting a U disk/SD, the system prompts that U disk/SD is found. The files in this U disk/SD card can be positioned and accessed through URL, such as usb0:/abc/1.txt or sd0:/abc/1.txt.

Caution

Version 10.4 (2) and the later versions support the access to U disk/SD by URL. For earlier software, use the mount path of the file system to position and access U disk/SD, such as using /mnt/usb0 to access the USB device on port 0, and using /mnt/sd to access the SD card. The mount path is prompted when the device is inserted, or is displayed when users run the show usb.

9.2 Inserting the Device

Just insert a USB device into the USB slot. Messages as below are displayed if the system finds the device and loads the driver.

```
*Jan 1 00:09:42: %USB-5-USB_DISK_FOUND: USB Disk <Mass Storage> has been inserted to USB port 0!

*Jan 1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount usb0 (type: FAT32), size: 1050673152B (1002MB)
```

<USB Mass Storage Device> is the name of the found device; usb0 is the first USB device, and size is the partition size. This U-disk has 1002 MB space.

Just insert an SD card into an SD slot. Messages as below are displayed if the system finds the device and loads driver.

```
*Jan 1 00:09:42: %USB-5-USB_DISK_PARTITION_MOUNT: Mount sd (type: FAT32), size: 1050673152B (1002MB)
```

SD is the first SD partition and size is the partition size. This SD card has 1002 MB space.

9.2.1 Using the Device

After loading U disk/SD card to the system, directly run file system commands (dir, copy, del, and others) to operate U disk/SD card. Operations below show how to copy the file of U disk/SD card to flash.

Enter the U disk partition.

```
DES-7200# cd usb0:/

Enter the SD card partition.

DES-7200# cd sd0:/
```

Copy the a.txt file in U disk to device's root directory.

```
DES-7200# copy a.txt usb0:/b.txt
```

Copy the a.txt file in the SD card to device's root directory.

```
DES-7200# copy a.txt sd0:/b.txt
```

Run the **dir** command. The result shows that the b.txt file has been added to the USB/SD card.

For other operation commands, see the "File System Management" section.

Caution

If there are multiple partitions in U disk/SD card, only the first FAT partition can be accessed through the device.

Note

Only the version 10.4(2) and the later versions allow users to access U disc/SD card by URL. For the earlier versions, use path to position and access the device. Example:

Access the U disk partition:

```
DES-7200# cd /mnt/usb0
```

Access the SD card partition:

```
DES-7200# cd /mnt/sd0
```

Copy a.txt under root directory to U disk.

```
DES-7200# copy flash:/mnt/usb0/a.txt  flash:/a.txt
```

Copy a.txt under root directory to SD card.

```
DES-7200# copy flash:/mnt/sd/a.txt  flash:/a.txt
```

9.2.2 Showing USB Device/SD Card Information

Command	Function
DES-7200# **show usb**	Show the USB device information of the system
DES-7200# **show sd**	Show the SD device information of the system

In the CLI command mode, use the **show usb**/ **show sd** command to view the USB / SD device information of the system. The displayed information is as follows:

```
DES-7200# show usb

Device: Mass Storage:

ID: 0

URL prefix: usb0

Disk Partitions:

usb0(type:FAT32)


Size : 131,072,000B(125MB)

Available size：  1,260,020B（1.2MB）


DES-7200# show usb

Device: Mass Storage:

ID: 1

URL prefix: sd0

Disk Partitions:

SD (type: FAT32)


Size: 131,072,000B (125MB)

Available size：  1,260,020B（1.2MB）
```

USB Mass Storage Device is the name of the device.

URL means which prefix can be used by U disk/SD card to access U disk/SD card.

Size means the available space in U disk/SD card that can be accessed.

Available size means the remaining space in U disk/SD card.

9.2.3 Unplugging USB Device/SD Card

Before pulling out USB device/SD card, run the command on the CLI to uninstall the device in case system is using the USB device/SD card to avoid an error.

Command	Function
DES-7200# **usb remove** *device_ID*	Uninstall the USB device with ID Device_ID
DES-7200# **sd remove** *device_ID*	Uninstall the SD device with ID Device_ID

As shown above, IDO indicates a USB device, and ID1 indicates SD card. The commands below can uninstall the corresponding USB device and SD card.

```
DES-7200# usb remove 0
```

After the uninstall command is used, the system will print:

OK, now you can pull out the device 0.

```
*Jan 1 00:18:16: %USB-5-USB_DISK_REMOVED: USB Disk <Mass Storage> has been removed
from USB port 0!

DES-7200# sd remove 1
```

After the uninstall command is used, the system will print:

OK, now you can pull out the device 1

Now, users can pull out the USB device/SD card.

Sometimes, it may lead to failure to uninstall the device for the device is being used. Wait a while, and then run the uninstall command to pull out the device.

Caution

Be sure to uninstall the device first and then unplug the device to prevent the system error.

9.3 USB/SD Faults

Assume that the system prints the following message:

```
*Jan 2 00:00:39: %USB-3-OHCI_ERR: USB1.0 controller is not available now.
```

USB/SD 1.0 controller is not available, while 2.0 USB/SD card is still available. In this case, reset the whole system to use corresponding version U disk/SD card.

Assume that the system prints the following message:

```
*Jan 2 00:00:39: %USB-3-EHCI_ERR: USB2.0 controller is not available now.
```

USB/SD 2.0 controller is not available, while 1.0 U disc/SD card is still available. In this case, reset the whole system to use corresponding version U disk/SD card.

DES-7200

WEB Management Configuration Guide

Version 10.4(3)

DES-7200 Configuration Guide

Revision No.: Version 10.4(3)

Date:

Preface

Version Description

This manual matches the firmware version 10.4(3).

Target Readers

This manual is intended for the following readers:

- Network engineers
- Technical salespersons
- Network administrators

Conventions in this Document

1. Universal Format Convention

Arial: Arial with the point size 10 is used for the body.

Note: A line is added respectively above and below the prompts such as caution and note to separate them from the body.

Format of information displayed on the terminal: Courier New, point size 8, indicating the screen output. User's entries among the information shall be indicated with bolded characters.

2. Command Line Format Convention

Arial is used as the font for the command line. The meanings of specific formats are described below:

Bold: Key words in the command line, which shall be entered exactly as they are displayed, shall be indicated with bolded characters.

Italic: Parameters in the command line, which must be replaced with actual values, shall be indicated with italic characters.

[ ]: The part enclosed with [ ] means optional in the command.

{ x | y | ... }: It means one shall be selected among two or more options.

[x | y | ...]: It means one or none shall be selected among two or more options.

//:Lines starting with an exclamation mark "//" are annotated.

3. Signs

Various striking identifiers are adopted in this manual to indicate the matters that special attention should be paid in the operation, as detailed below:

 **Caution**	Warning, danger or alert in the operation.

 **Note**	Descript, prompt, tip or any other necessary supplement or explanation for the operation.

 **Note**	The port types mentioned in the examples of this manual may not be consistent with the actual ones. In real network environments, you need configure port types according to the support on various products. The display information of some examples in this manual may include the information on other series products, like model and description. The details are subject to the used equipments.

1 WEB Management Configuration

1.1 Understanding the WEB Management

1.1.1 WEB Management Overview

WEB management uses the browser such as IE to manage the network devices like the switch or router.

1.1.2 Working Principles

WEB management includes the management of WEB server and WEB client. The WEB server is integrated in the device to receive and process the requests from the client (reading WEB files or executing command requests) as well as return the processing result to the client. The WEB client usually refers to the browser like IE.

1.1.3 Working Principles

NA

1.2 Default Configuration

The following table describes the default configuration for WEB management.

Features	Default value
WEB service	Off

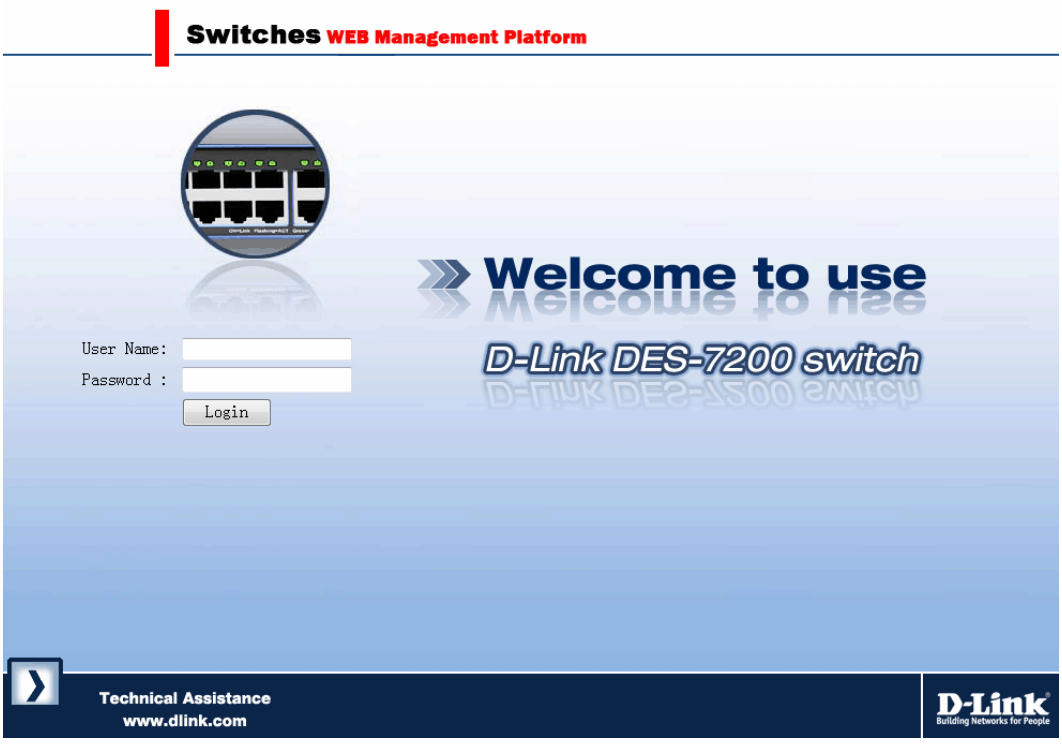
Note

To enable the WEB services, refer to the following section of The Typical Example of WEB Management. In order to authenticate the WEB configuration by using the Enable method, directly input the Enable password and no need to enter the user name for the authentication.

1.3 Configuring WEB Management

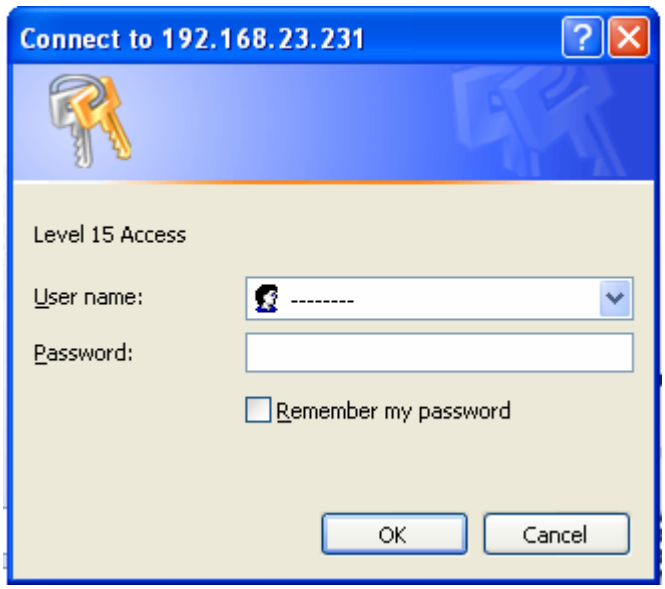
Enter the management IP address of the device in the address bar of the browser, such as http://192.168.1.200. Press Enter to display the following page.

Figure 1-1 Original Page



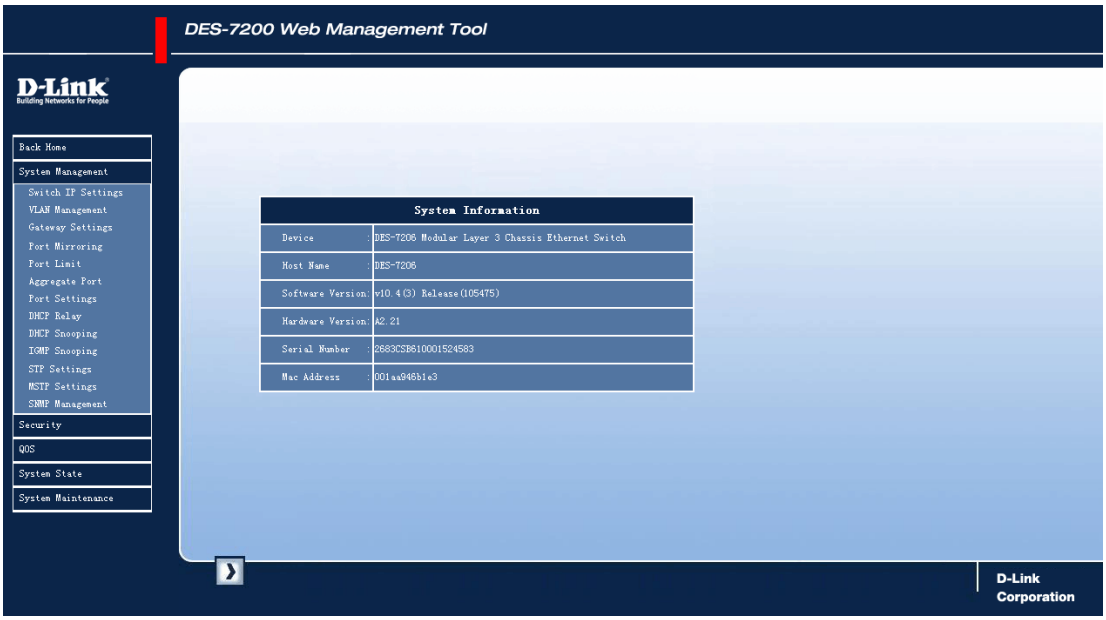
Select a type of the languages and click Login to display the authentication dialog box. Enter the user name and password in this dialog box.

Figure 1-2 Logon the authentication dialogue box



If the authentication succeeds, enter the main page of the WEB management as follows:

Figure 1-3 Main page of WEB management platform



Note

If WEB management is authenticated by using Enable, directly enter Enable password and no need to enter the user name.

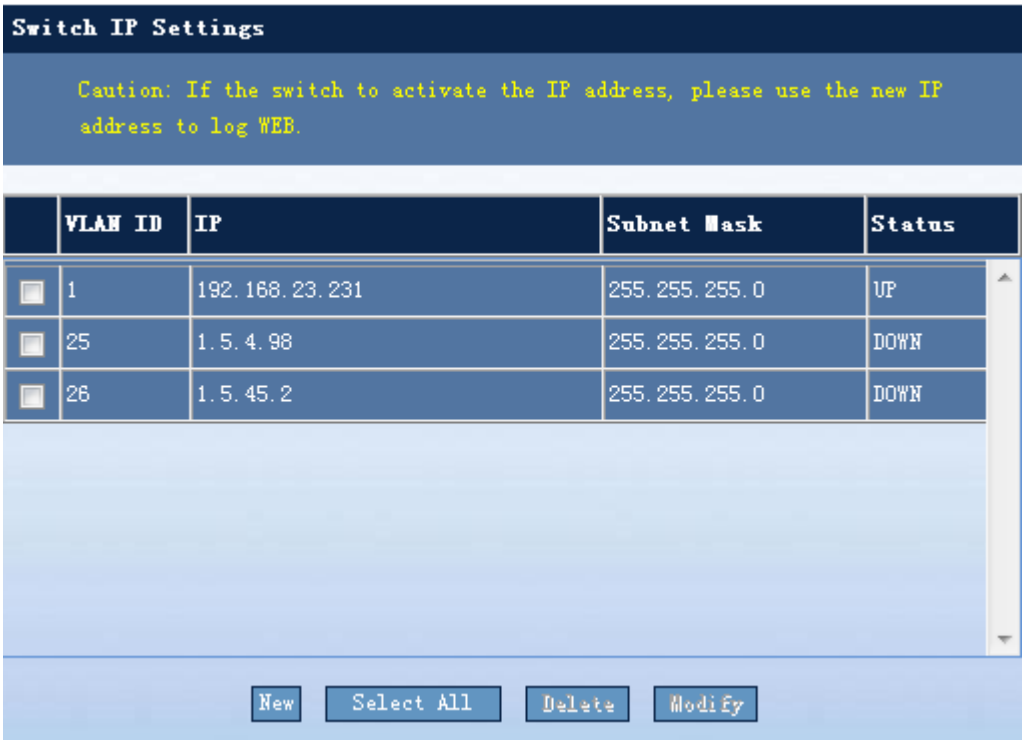
1.3.2 System Management

1.3.2.1 Switch IP address Configuration

Use the function through the menu “Switch IP Setting”.

The page of the “switch IP address setting”

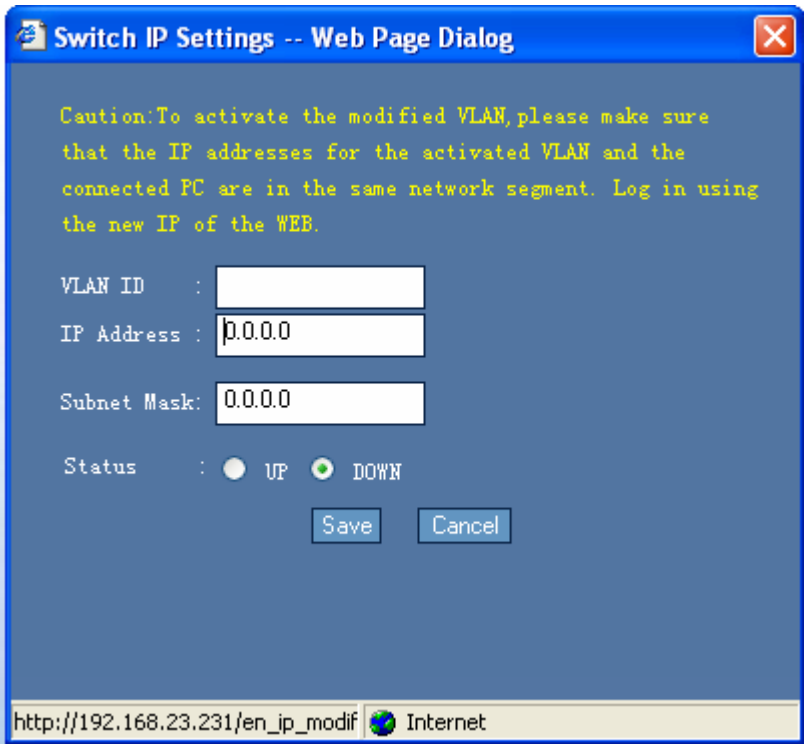
Figure 1-4 Switch IP address setting



Configuration Description:

Modification: If you want to modify the IP address of a switch, select the checkbox and click “Modify” to display the following configuration page.

Figure 1-5 Switch IP Address Modification



Users can modify the IP address and subnet mask. After modifying the corresponding parameters, click “Save” to validate the configuration.

1.3.2.2 VLAN Management

Use the function through the menu item “**VLAN Management**”.

1) VLAN management page

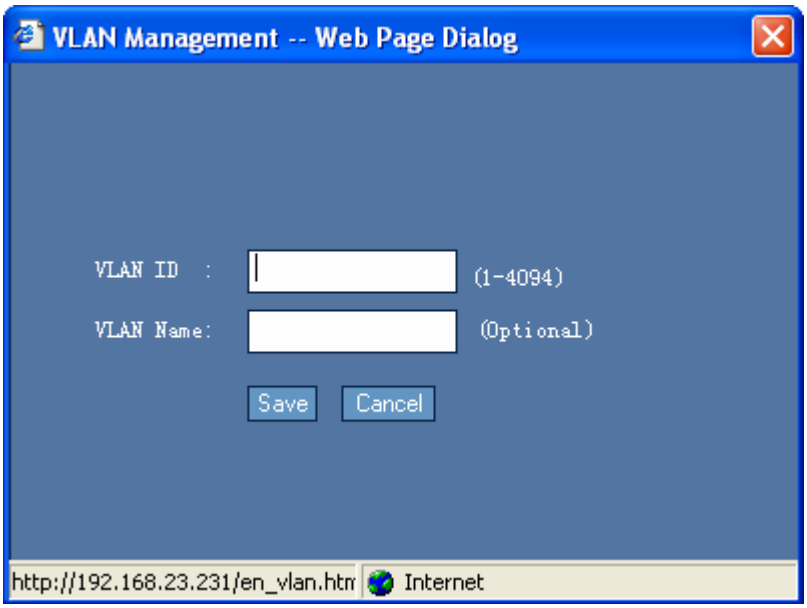
Figure 1-6 VLAN management

Configuration Description

Enter this page to display the VLAN information of the current system. Users can create, delete and modify the VLAN, but the default VLAN cannot be deleted.

Create: Click “**New**” to display the following configuration page.

Figure 1-7 Create VLAN

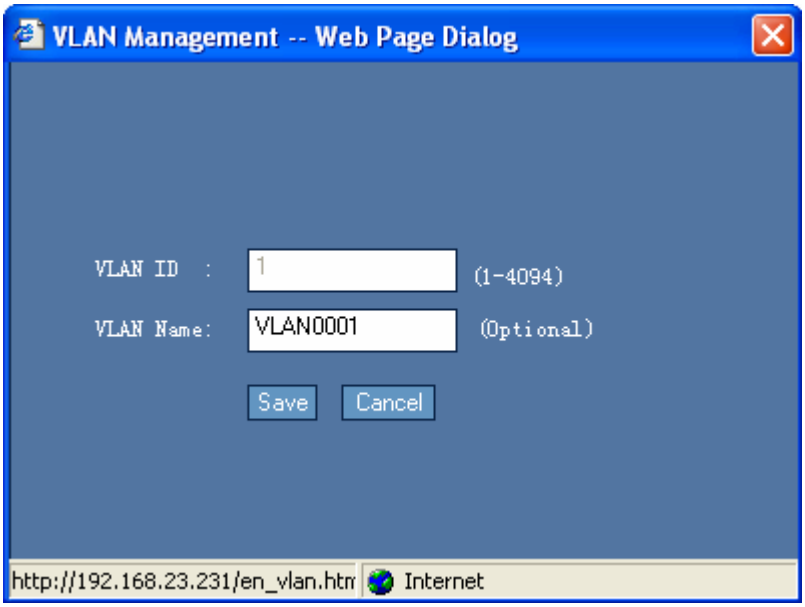


Enter the VLAN ID and VLAN Name (optional) and then click **Save** to validate the setting. After the succesful setting, the new VLAN is displayed on the **VLAN Management** page.

Delete: To delete the specified VLAN, select the corresponding checkbox and then click **Delete** to validate the configuration.

Modify: To modify the configured VLAN, select the corresponding checkbox and then click **Modify** to display the following configuration page.

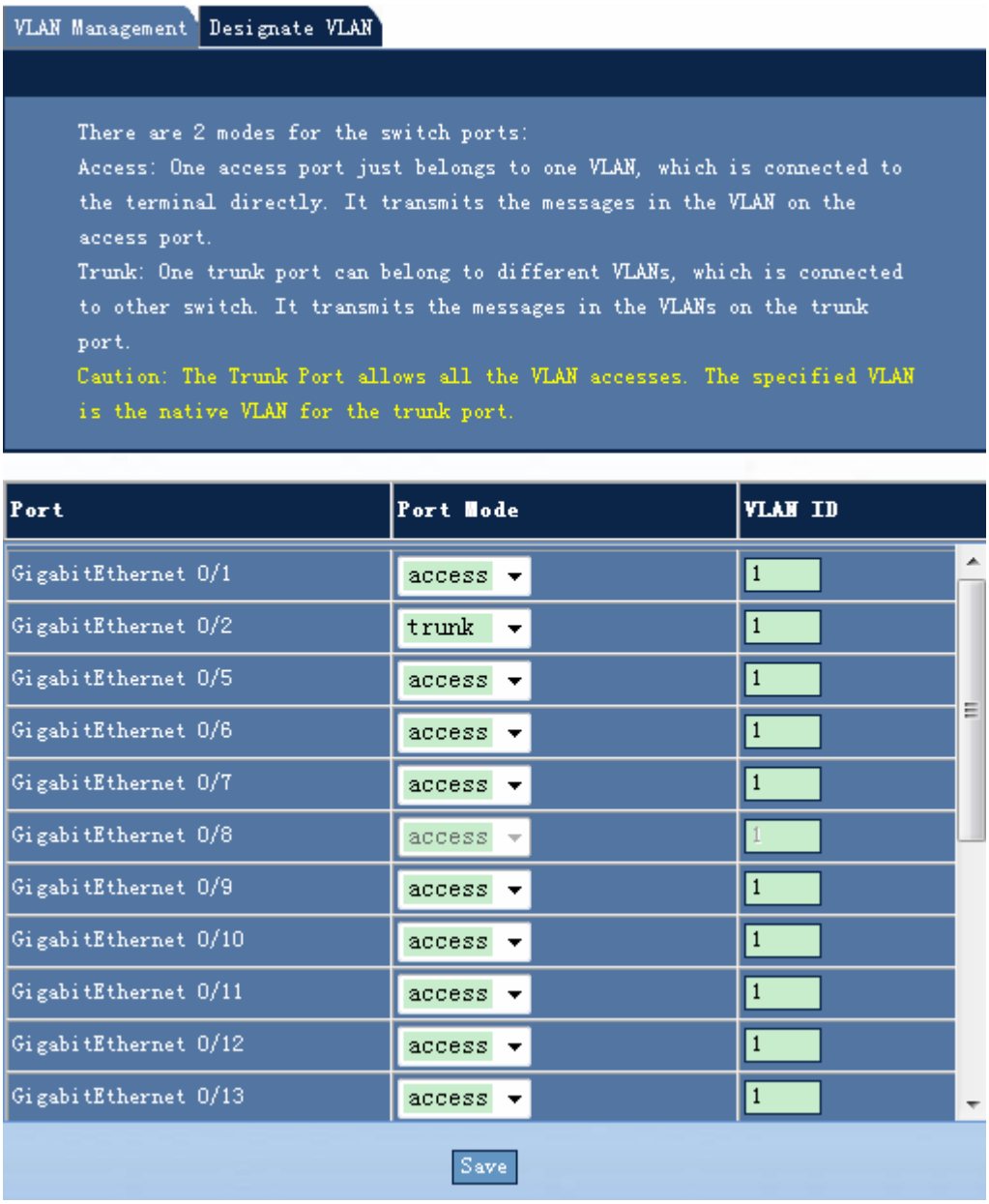
Figure 1-8 Modifying VLAN



The VLAN information to be modified is displayed in the textbook. After modifying the VLAN information, click **Save** to validate the configuration. The modified result is displayed in the VLAN management page.

2) Specify the VLAN page

Figure 1-9 Specify the VLAN



Configuration Description:

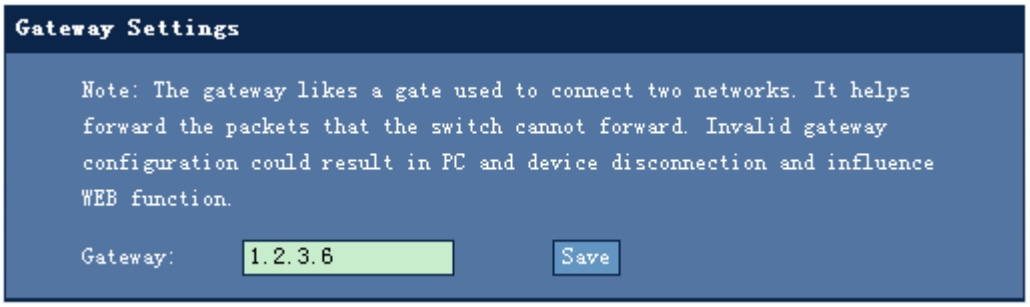
Specify the port mode and **VLAN ID** to be configured. After all the ports are set, click **Save** to validate the configuration.

1.3.2.3 Gateway Setting

Use the function through the menu item **Gateway Setting**.

Gateway setting page

Figure 1-10 Gateway setting



Configuration Description:

If the switch has already been configured with a gateway, when you open the page, the IP address of the configured gateway is displayed in the textbox. If you want to set a new gateway IP address, enter the new one in the textbox and then click **Save** to validate the configuration.

1.3.2.4 Port Mirroring

Use the function through the menu item **Port Mirroring**

Port mirroring setting page

Figure 1-11 Port mirroring setting

Configuration Description:

Select the monitoring ports and tick the checkbox in front of the ports to be monitored. Click **Save** to validate the configuration. The monitoring port and the port to be monitored should not be the same one.

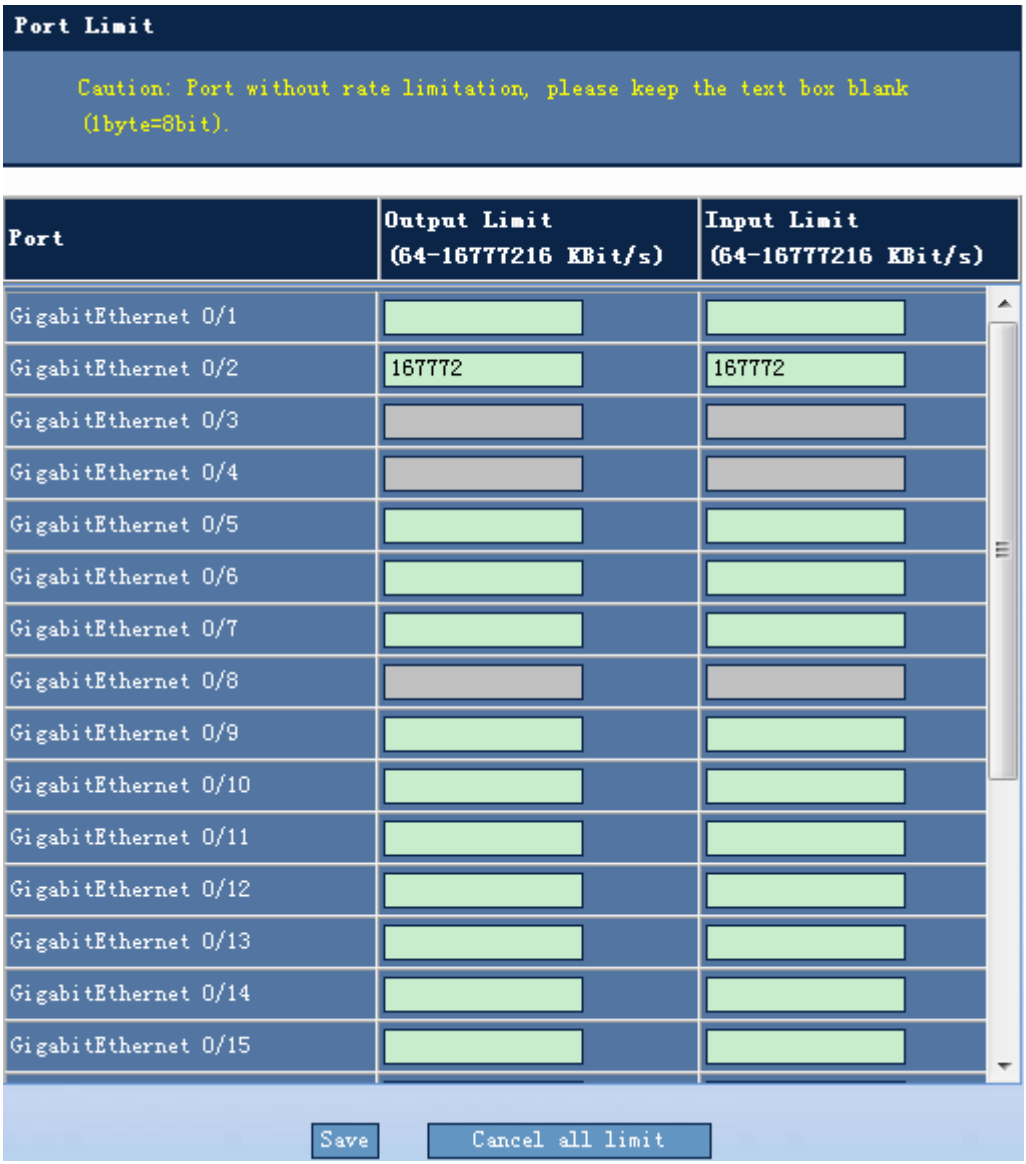
Click **Delete Port Monitor** to delete the configuration of port monitoring.

1.3.2.5 Rate Limiting on the Port

Use the function through the menu item **Rate Limiting on the Port**.

Main page of setting rate limiting on the port

Figure 1-12 Setting rate limiting on the port



Configuration Description:

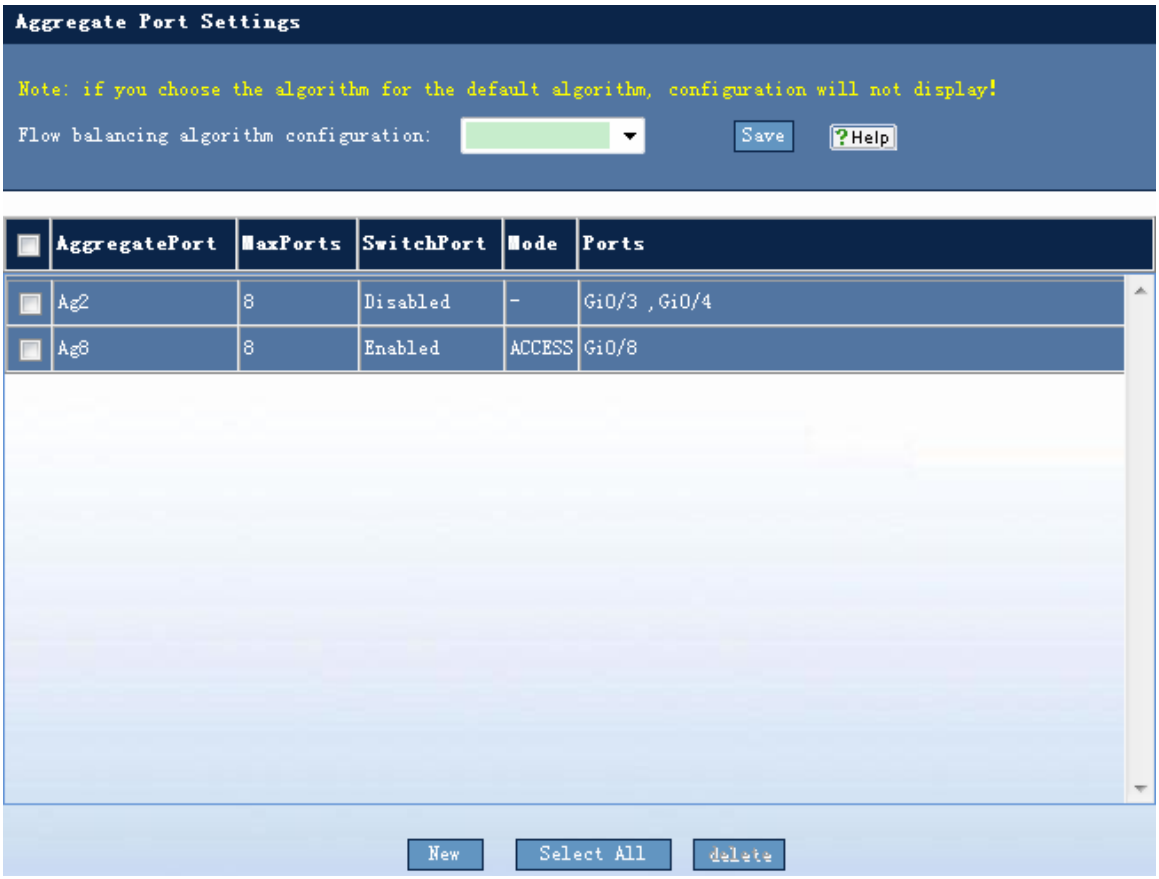
Enter the rate limiting value in the textbox on the port that limits the rate. You can set the values on multiple ports. After the rate limiting value is set, click **Save** to validate the setting. The textbox should be null for the port without limiting the rate. In order to cancel the rate limiting setting on all the ports, click **Cancel all Rate Limiting** to validate the setting.

1.3.2.6 Aggregation Port

Use the function through the menu item **Aggregation Port**.

Aggregation port setting page

Figure 1-13 Aggregation port setting



Configuration Description:

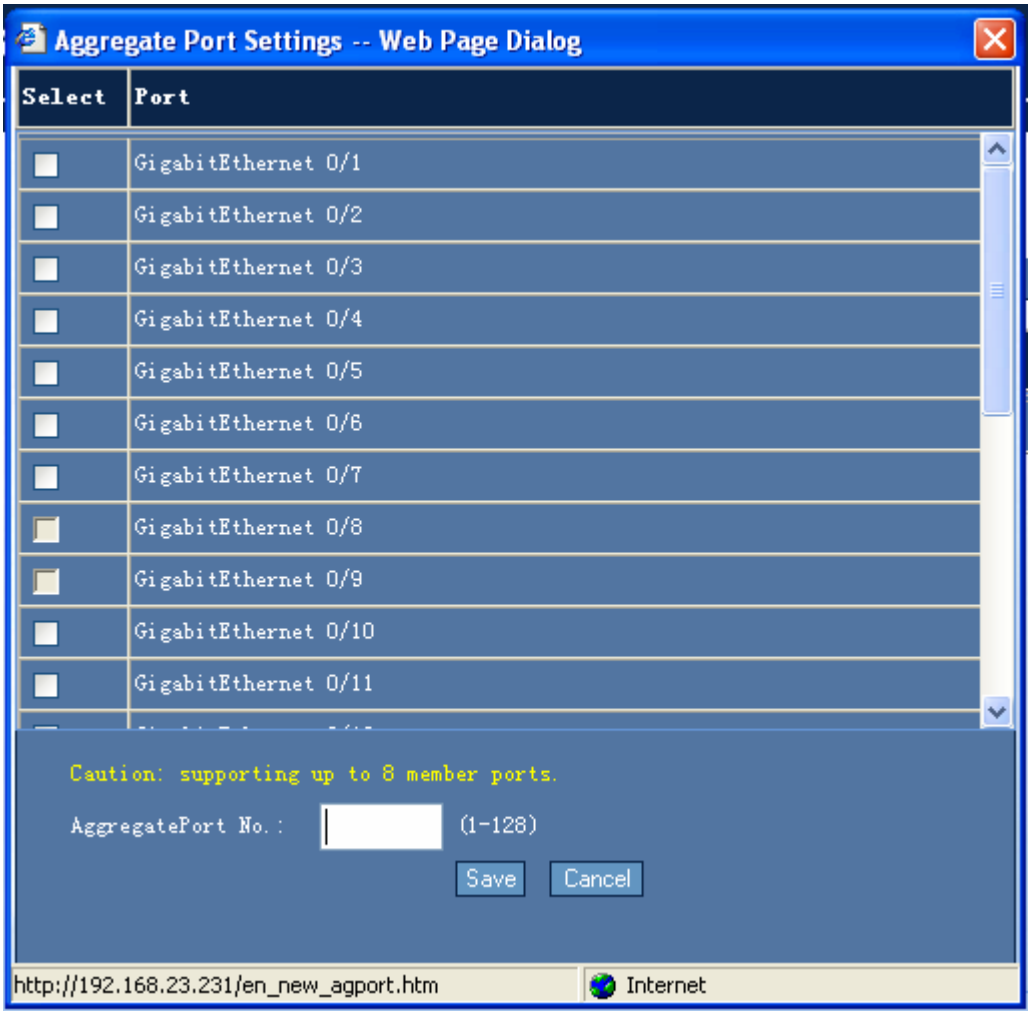
1) Configuring the traffic balancing algorithm

To configure the traffic balancing algorithm, select the corresponding algorithm item and click **Save** to validate the configuration.

2) Configuring the aggregation port

To create an aggregation port, click **New** to display the following interface.

Figure 1-14 Aggregation port creation



Select the member port and specify the aggregation port number, then click **Save** to validate the configuration. If a member port belongs to other aggregation port, then the check box in front of the member port can not be selected.

3) Deleting the Aggregation port

To delete an aggregation port, tick the check box in front of the corresponding aggregation port and click **Delete** to validate the configuration.

1.3.2.7 Port Setting

Use the function through the menu item **Port Setting**.

Port setting page

Figure 1-15 Port setting

Configuration Description:

Select the port to be configured and configure related parameters, then click **Save** to validate the configuration. If the selected parameter is not be supported by the device, the corresponding paramter setting does not take effect.

1.3.2.8 DHCP Relay

Use the function menu item through the **DHCP Relay**.

DHCP relay setting page

Figure 1-16 DHCP relay

1) Enabling/disabling DHCP relay

To enable or disable the DHCP relay function, select the related option button and click **Save** to validate the configuration.

2) Setting DHCP server

Set the IP address for the DHCP server and then click **Save** to validate the configuration. The configuration result is displayed in the following figure. To delete the DHCP server, tick the check box and click **Delete** to validate the configuration.

1.3.2.9 DHCP Snooping

Use the function through the menu item **DHCP Snooping** .

DHCP Snooping setting page

Figure 1-17 DHCP Snooping setting

Configuration Description:

1)DHCP Snooping setting

To enable the DHCP Snooping function or the source MAC address detection function of DHCP Snooping, select the related option button and then click **Save** to validate the configuration.

2) Setting the DHCP Snooping trust port

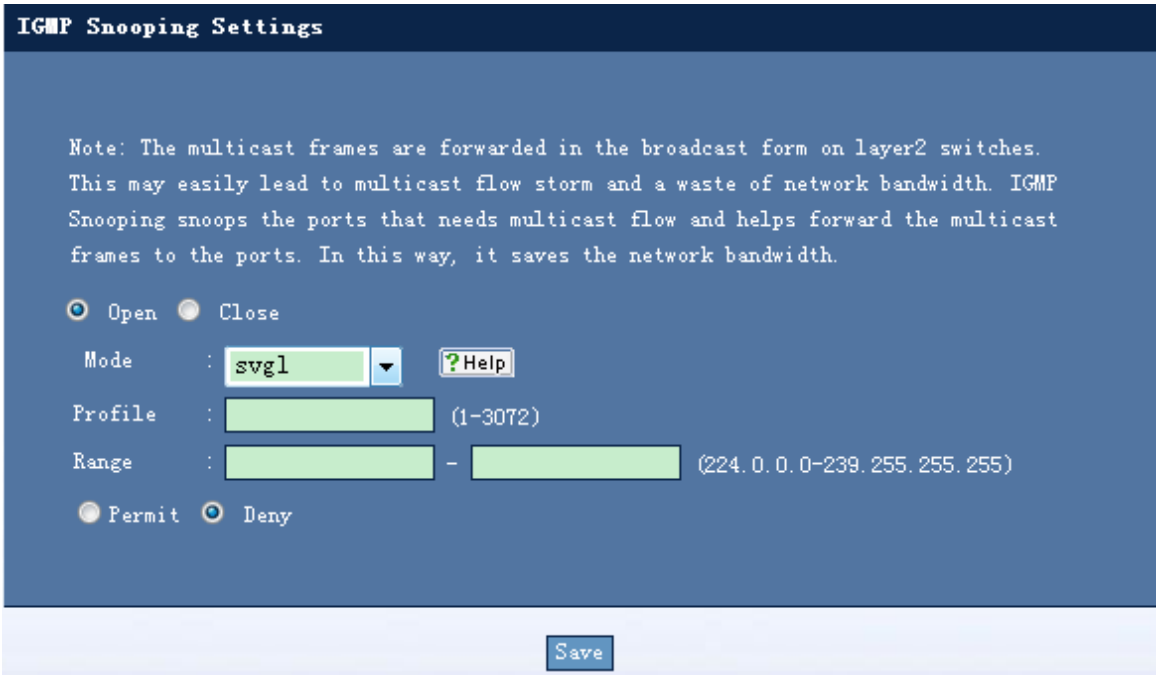
Select the trust port to be configured and click **Save** to validate the configuration. The configuration information is displayed in the following figure. To delete the trusted port, tick the check box and click **Delete** to validate the configuration.

1.3.2.10 IGMP Snooping

Use the function through the menu item IGMP Snooping .

IGMP Snooping setting page

Figure 1-18 IGMP Snooping setting



Configuration description:

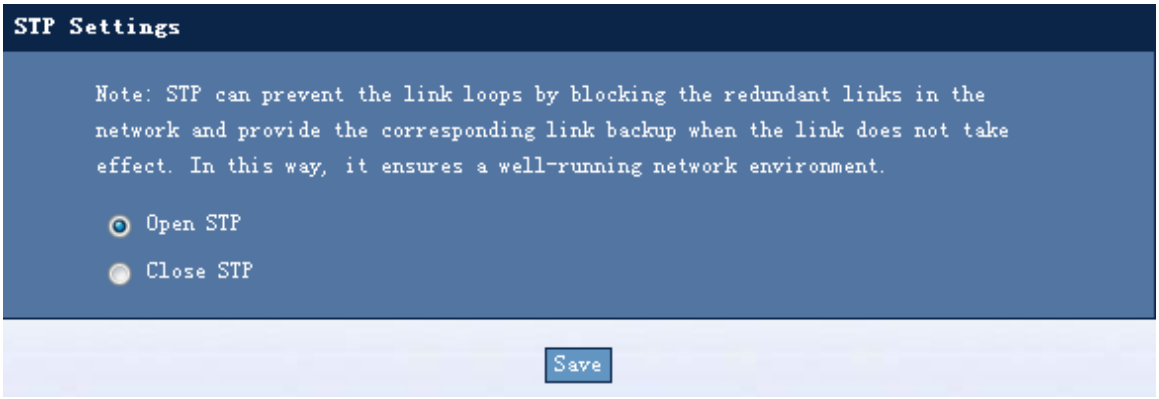
To enable the IGMP Snooping function, Click the **Enable** option button and then the **Mode** drop-down list changes to the selectable state. You can select three modes: ivgl, svgl, or ivgl-svgl from this list. If you select the mode svgl or ivgl-svgl, then you can set the parameters such as identification and the range of the IP addresses. After the parameters are configured, click **Save** to validate the configuration. To disable the IGMP Snooping function, Click the **Disable** option button and click **Save** to validate the configuration.

1.3.2.11 STP Setting

Use the function through the menu item **STP Setting** .

The following is the main page of STP Setting.

Figure 1-19 STP setting



Configuration Description:

Select the Enable STP functions option button or the Disable STP functions option button and click **Save** to validate the configuration.

1.3.2.12 SNMP Management

Use the function through the menu item **SNMP Management**.

SNMP management page

Figure 1-20 SNMP management setting

Configuration description:

To enable the SNMP management function, select the **Enable SNMP** option button and configure the parameters such as the group name, read-write attribute. Click **Save** to validate the configuration. To disable the SNMP management function, select the **Disable SNMP** option button and click **Save** to validate the configuration. To delete the configured group name, tick the check box of the entry to be deleted and click **Delete** to validate the configuration.

1.3.3 Security

1.3.3.1 Anti-Gateway ARP Spoofing

Use the **Anti-Gateway ARP Spoofing** menu item to enable the function.

Anti-Gateway ARP Spoofing page

Figure 1-21 Anti-gateway ARP spoofing

Configuration Description:

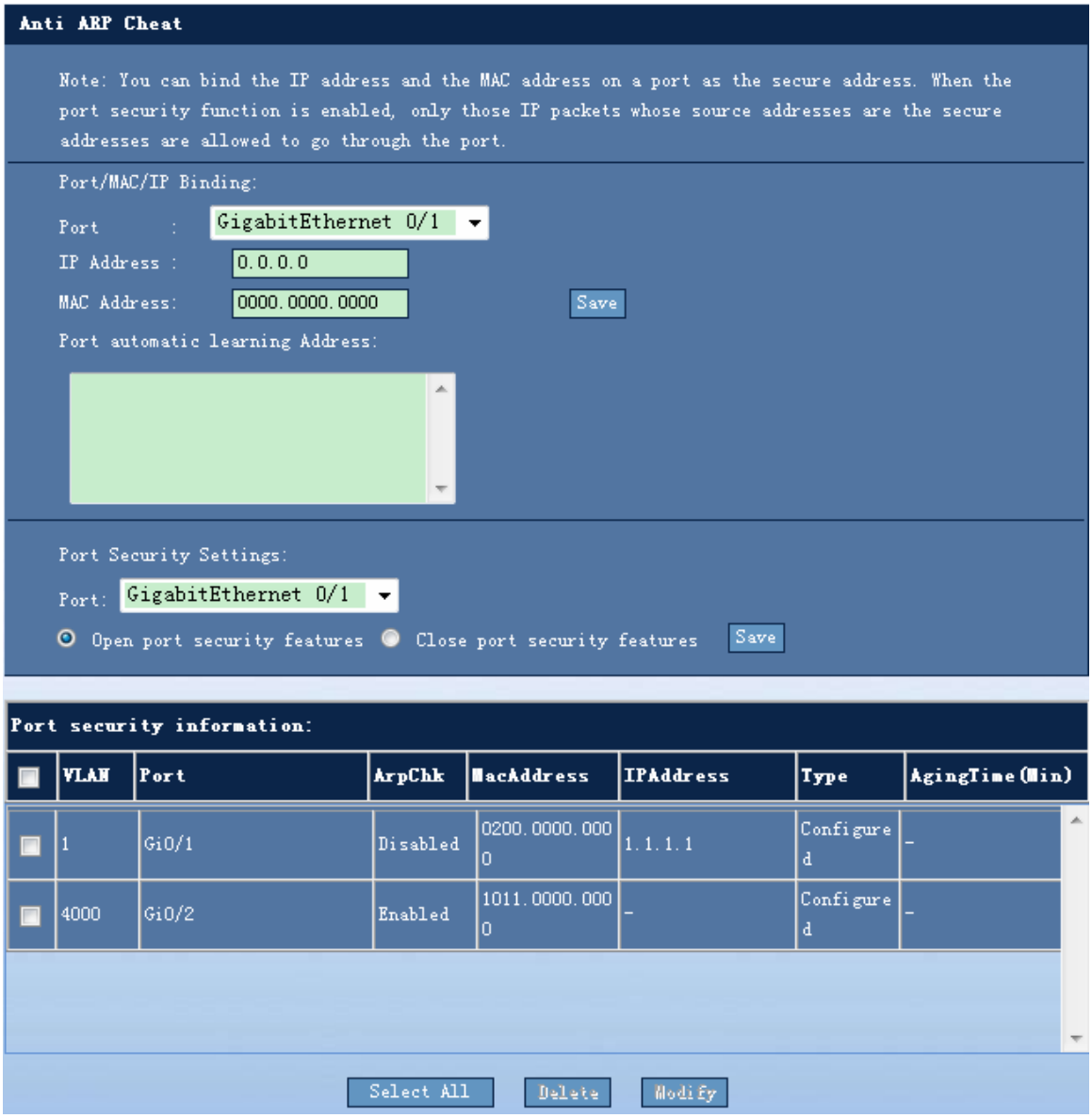
Select the port to be configured. Enter the IP address of the gateway and click **Save** to validate the configuration. A port can be configured with multiple IP addresses of the gateway. In order to delete the configured gateway, tick the check box of the IP address of the gateway to be deleted and click **Delete** to validate the configuration.

1.3.3.2 Anti-ARP-Spoofing

Use the **Anti-ARP-Spoofing** menu item to enable the function.

The anti-ARP-spoofing setting page

Figure 1-22 Anti-ARP-spoofing setting



Configuration Description:

1) Binding Port/MAC address/IP address

In order to configure port/MAC address/IP address binding, select the port to be configured and configure the IP address and MAC address. Click **Save** to validate the configuration. If the selected port learns MAC address automatically, the MAC address is displayed in the address textbox, as shown in the figure above. When you select the GigabitEthernet 0/15 port, the textbox lists the MAC address learned by the port.

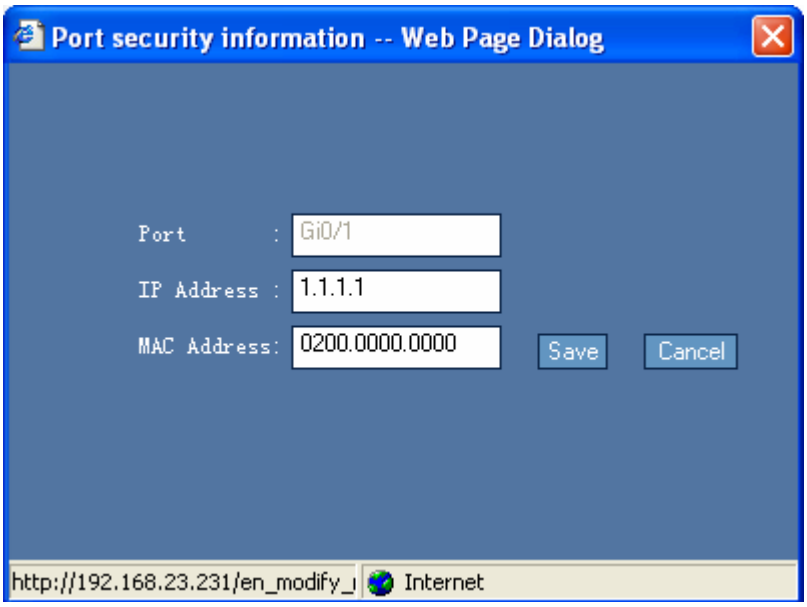
2) Setting the port security function

Select the port to be configured. If the port security function is enabled on the port, the **Enable port security** option button is selected. Otherwise the **Disable port security** option button is selected. If the port security function is enabled, the following figure shows the security port information.

3) Modifying the information of the security port

In order to modify the information of the security port, tick the check box of the port to be modified and click **Modify** to display the Modify security port page as shown below.

Figure 1-23 Security port modification



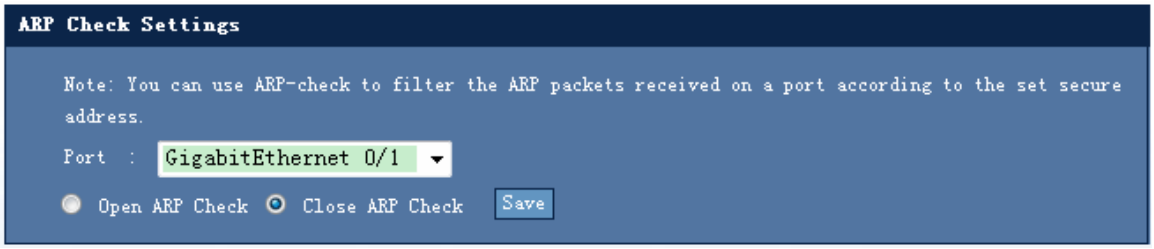
After modifying related parameters, click **Save** to validate the configuration. If the port type is dynamic, the type of the modified port changes to static.

1.3.3.3 ARP Detection Setting

Use the **ARP Detection Setting** menu item to enable the function.

ARP detection setting page

Figure 1-24 ARP detection setting



Configuration Description:

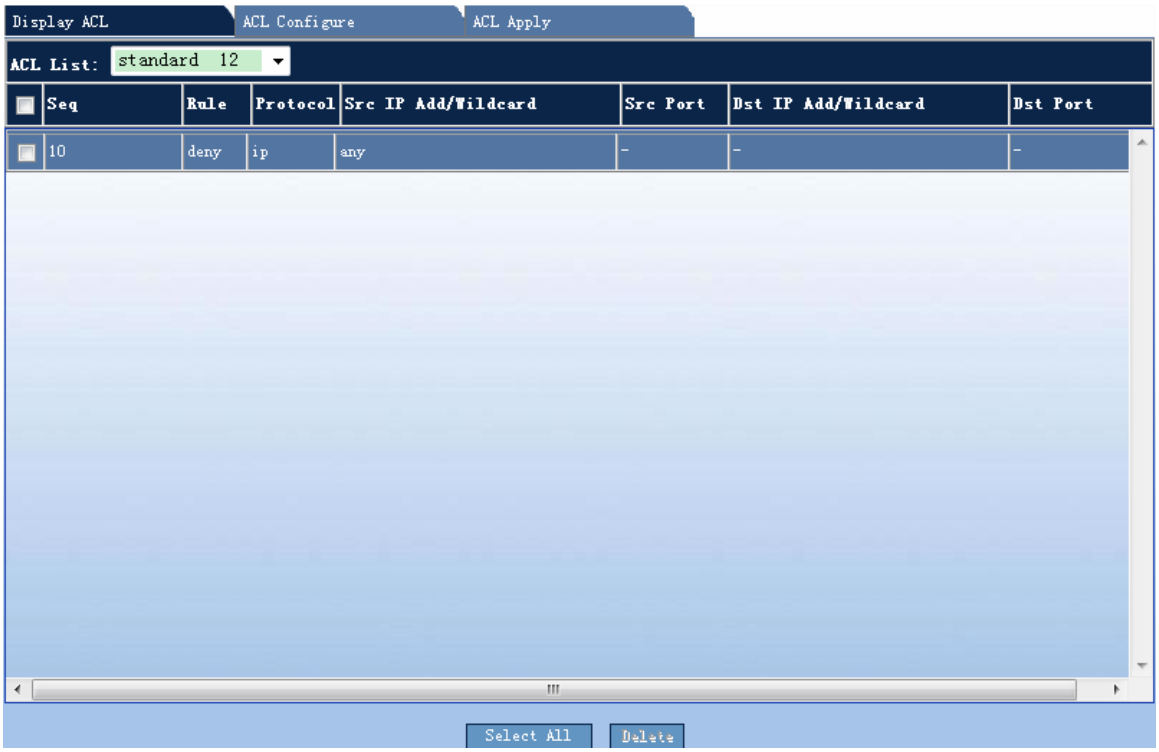
If the ARP detection function is already enabled on the selected port, the **Enable ARP detection function** option button is selected. Otherwise the **Disable ARP detection function** option button is selected by default.

1.3.3.4 ACL

Use the **ACL** menu item to enable the function.

ACL setting page

Figure 1-25 ACL setting



1) Displaying ACL Information

Configuration Description:

The **Display ACL information** interface is shown as the figure. In order to view the detailed information of the specified ACL, select the ACL from the ACL drop-down list to display all ACEs of the ACL. In order to delete an ACE, tick the check box and then click **Delete** to validate the configuration. In order to delete the whole ACL, click **Select All** to select all ACEs and click **Delete** to validate the configuration.

2) Configuring ACL

To configure the standard IP address access list, click **Configure standard IP address access list** option button. The following figure is the interface of configuring standard IP address access list.

Figure 1-26 Configuring standard IP address access list

Configuration description:

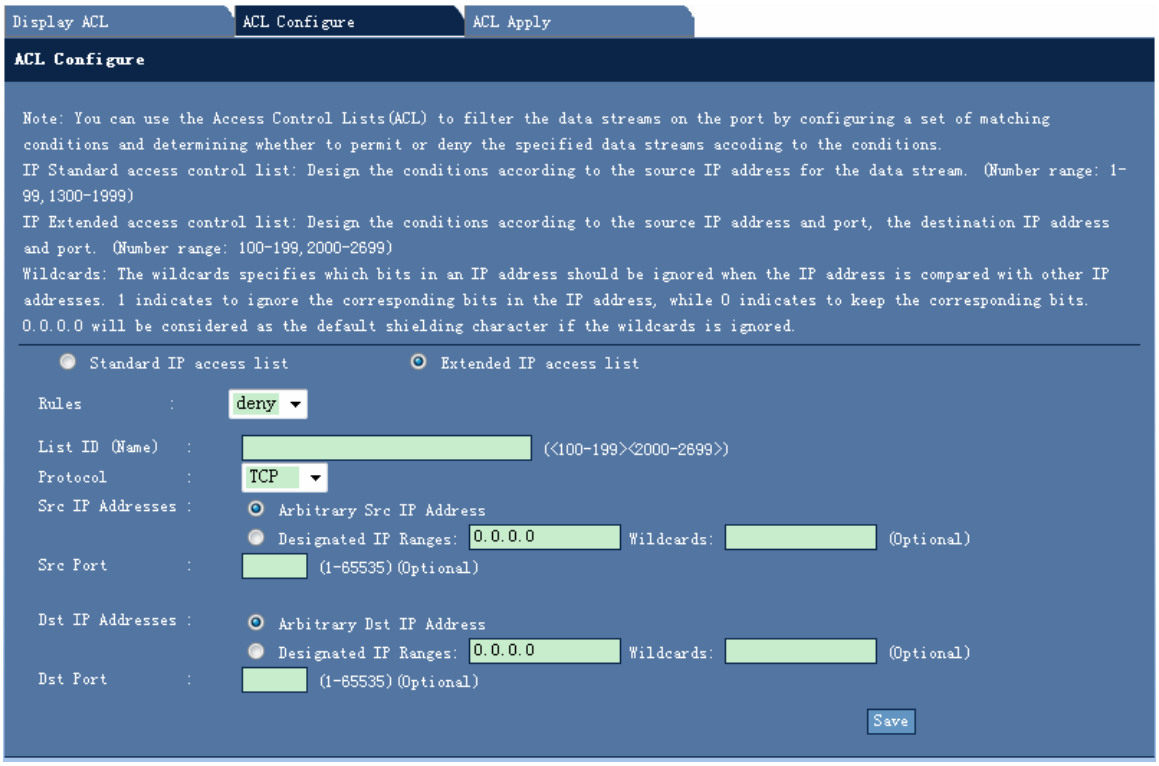
Rule: Select the filtering rule from the drop-down list. There are **Disable** and **Enable** filtering rules.

List ID (name): Enter the standard access list ID or name.

IP address: If you select the **Specify IP address range** option button, enter the correct IP address. The wildcard mask textbox is optional. After the configuration is complete, click **Save** to validate the configuration.

In order to configure the extended IP address access list, click **Configure extended IP address access list** option button. The following figure is the interface of configuring extended IP address access list.

Figure 1-27 Configuring extended IP address access list



Configuration Description:

Rule: Select the filtering rule from the drop-down list. There are **Disable** and **Enable** filtering rules.

List ID (name): Enter the extended access list ID or name.

Protocol: You can select the TCP, UDP, IP, or ICMP protocol.

Source IP address: You can select the **Any source IP address** or **Specify IP address range** option button. The wildcard is optional.

Source port: This parameter is optional.

Destination IP address: You can select the **Any source IP address** or **Specify IP address range** option button. The wildcard is optional.

Destination port: This parameter is optional.

After the parameters are configured, click **Save** to validate the configuration.

3) Applying ACL in the Port

Figure 1-28 Applying ACL on the port

Configuration Description:

Port: Select the port to be configured.

ACL list: Select the ACL applied on the port.

After the parameters are configured, click **Save** to validate the configuration.

In order to delete the configuration of the port, select the entry to be deleted and then click **Delete** to validate the configuration.

Note

To configure the port connecting to the PC, make sure that the ACL does not affect the interaction between the PC and device. If the configuration is incorrect, you cannot use WEB to manage the device.

1.3.4 QOS

1.3.4.1 Classification Setting

Use the **Classification Setting** menu item to enable the function. The following is the main page of classification setting.

Figure 1-29 Classification setting

Configuration description:

After setting the classification name and ACL, click **Save** to validate the configuration. The configuration information is displayed in the following figure. In order to delete the configured classification, tick the check box of the classification and click **Delete** to validate the configuration.

1.3.4.2 Policy Setting

Use the **Policy Setting** menu item to enable the function.

Policy setting page

Figure 1-30 Policy setting

Configuration description:

Policy name: Configure the policy name.

Classification list: This item lists the classification name that is already set. If the list is null, no classification is set. Go to the **classification setting** page to set the classification.

Bandwidth: Enter the bandwidth value in the specified range.

Burst traffic: Enter a value in the specified range depending on the prompt in the page.

When the bandwidth is beyond the specified range, if the DSCP priority is specified, enter a number in the specified range.

After the parameters are configured, click **Save** to validate the configuration.

In order to delete the policy that is already set, select the policy from the policy list to display the detailed information of the policy. Select the entry to be deleted and click **Delete** to

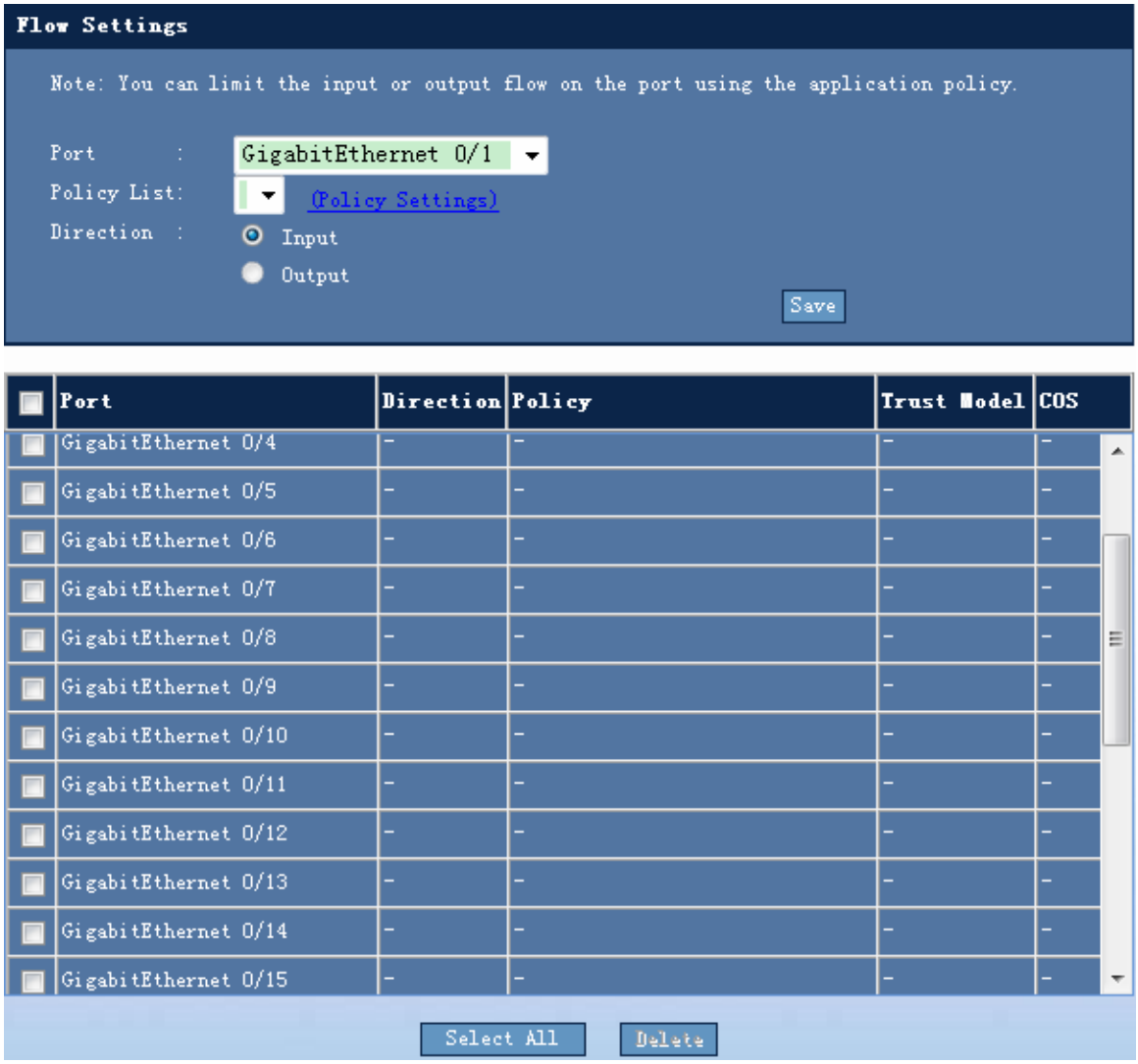
validate the configuration. In order to delete the policy name while deleting the policy, select all and click **Delete** to validate the configuration.

1.3.4.3 Traffic Setting

Use the **Traffic Setting** menu item to enable the function.

Traffic setting page

Figure 1-31 Traffic setting



Configuration description:

Port: Select the port to be configured.

Policy list: Select the policy applied in the port. If the list is null, set the policy.

Rate limiting direction: Select the rate limiting direction.

After the parameters are configured, click **Save** to validate the configuration. In order to delete the configuration of the port, tick the check box of the entry to be deleted and then click **Delete** to validate the configuration.

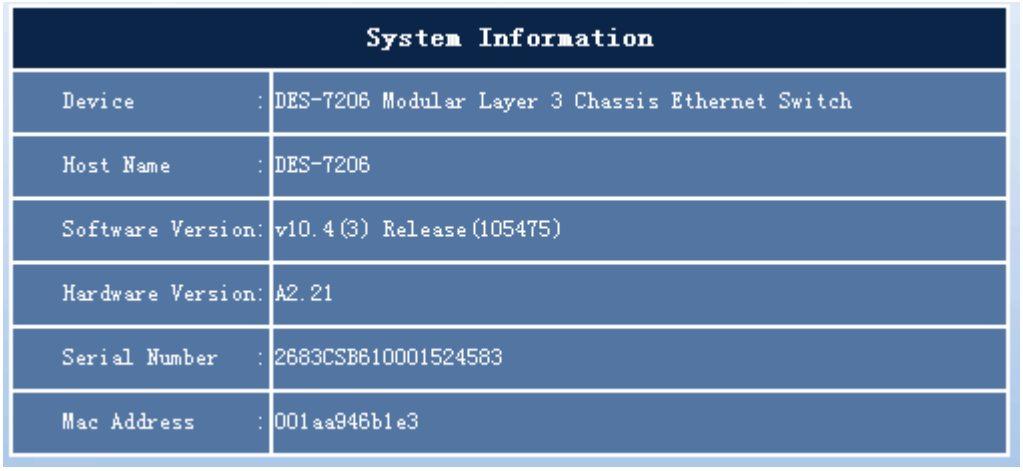
1.3.5 System Status

1.3.5.1 System Information

Use the System Information menu item to enable the function.

System information page

Figure 1-32 System information

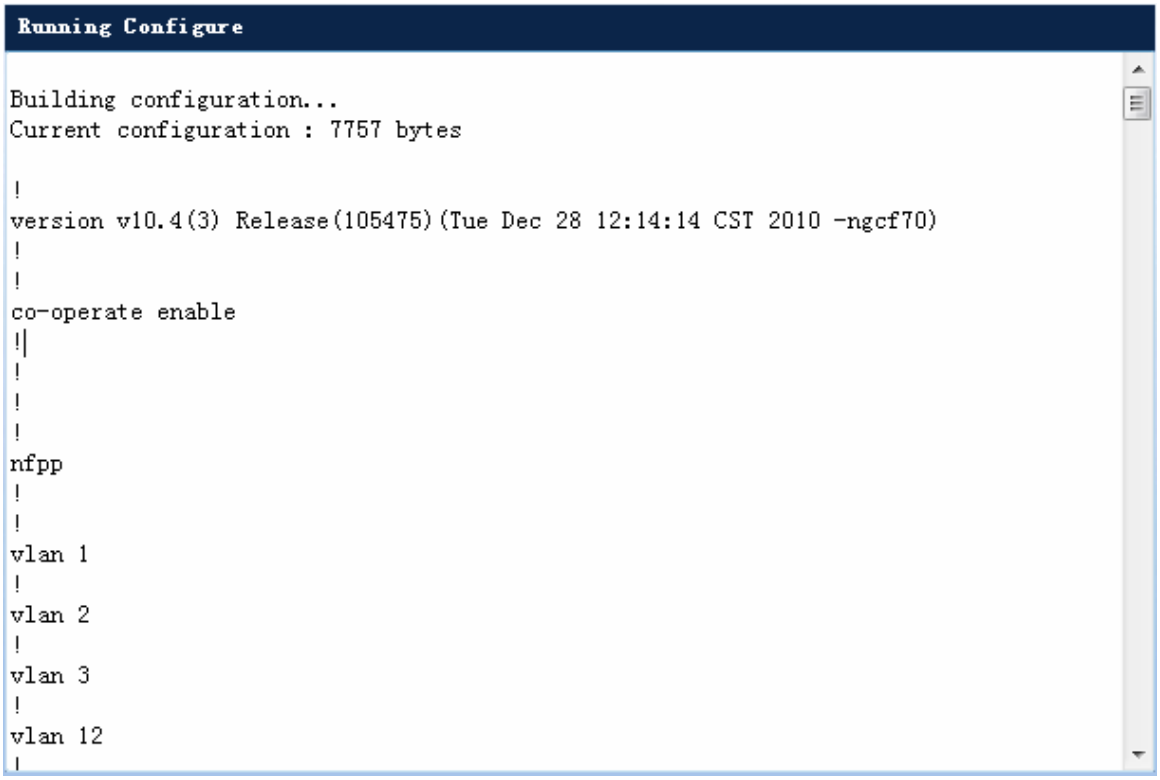


1.3.5.2 Current Configuration

Use the Current Configuration menu item to enable the function.

Current configuration page

Figure 1-33 Current configuration

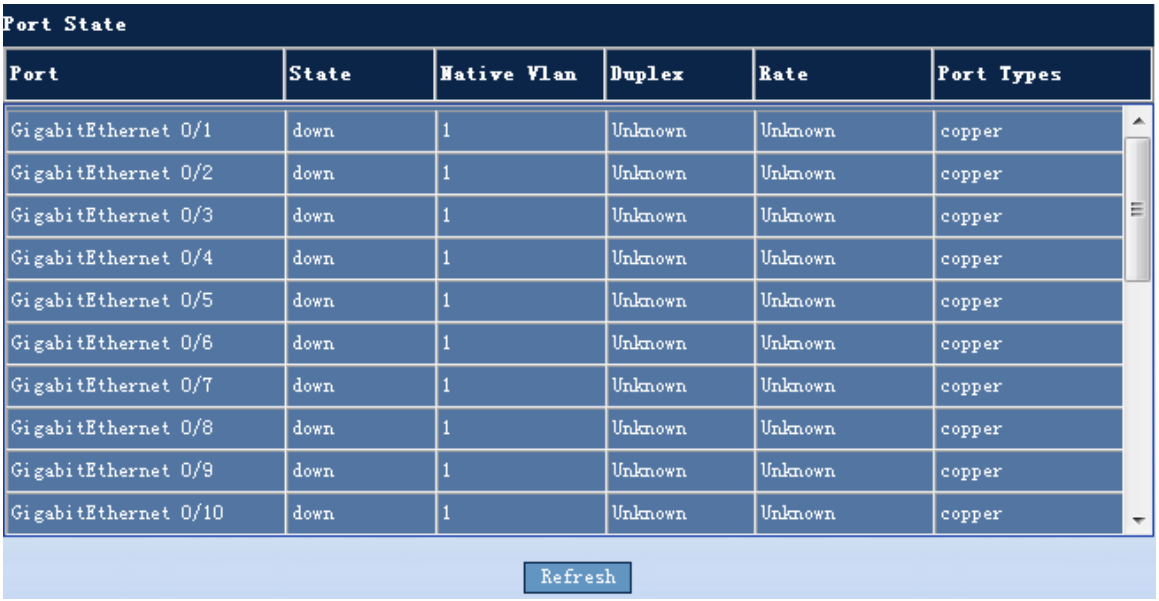


1.3.5.3 Port Status

Use the Port Status menu item to enable the function.

Port status page

Figure 1-34 Port status

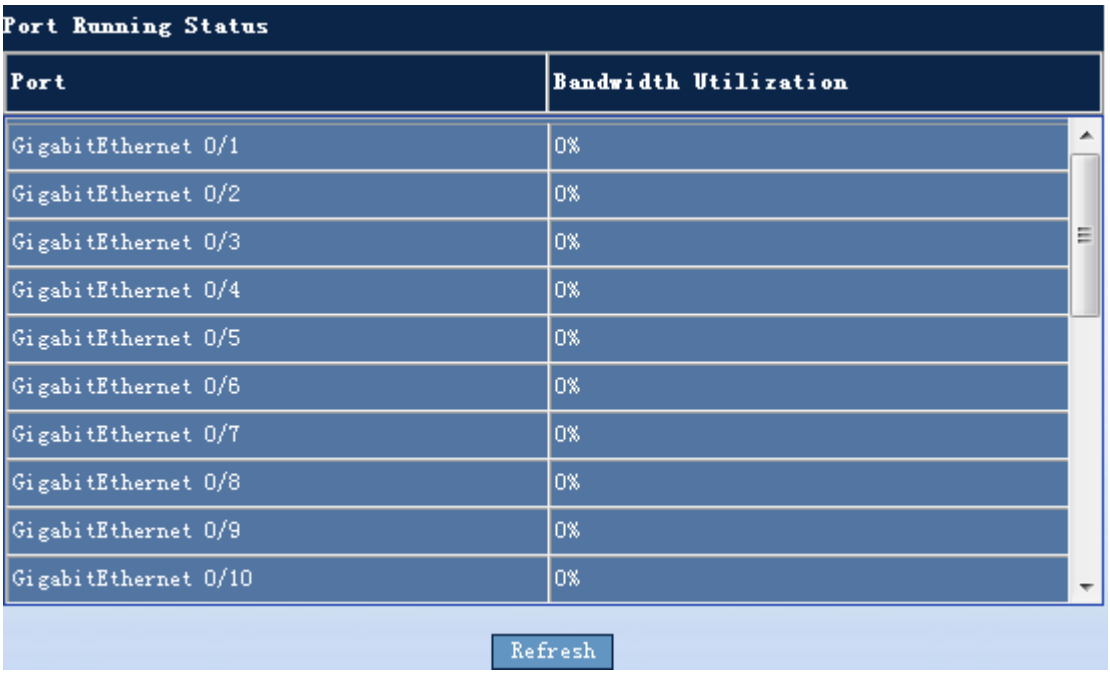


1.3.5.4 Port running status

Use the Port Running Status menu item to enable the function.

Port running status page

Figure 1-35 Figure 35 Port running status

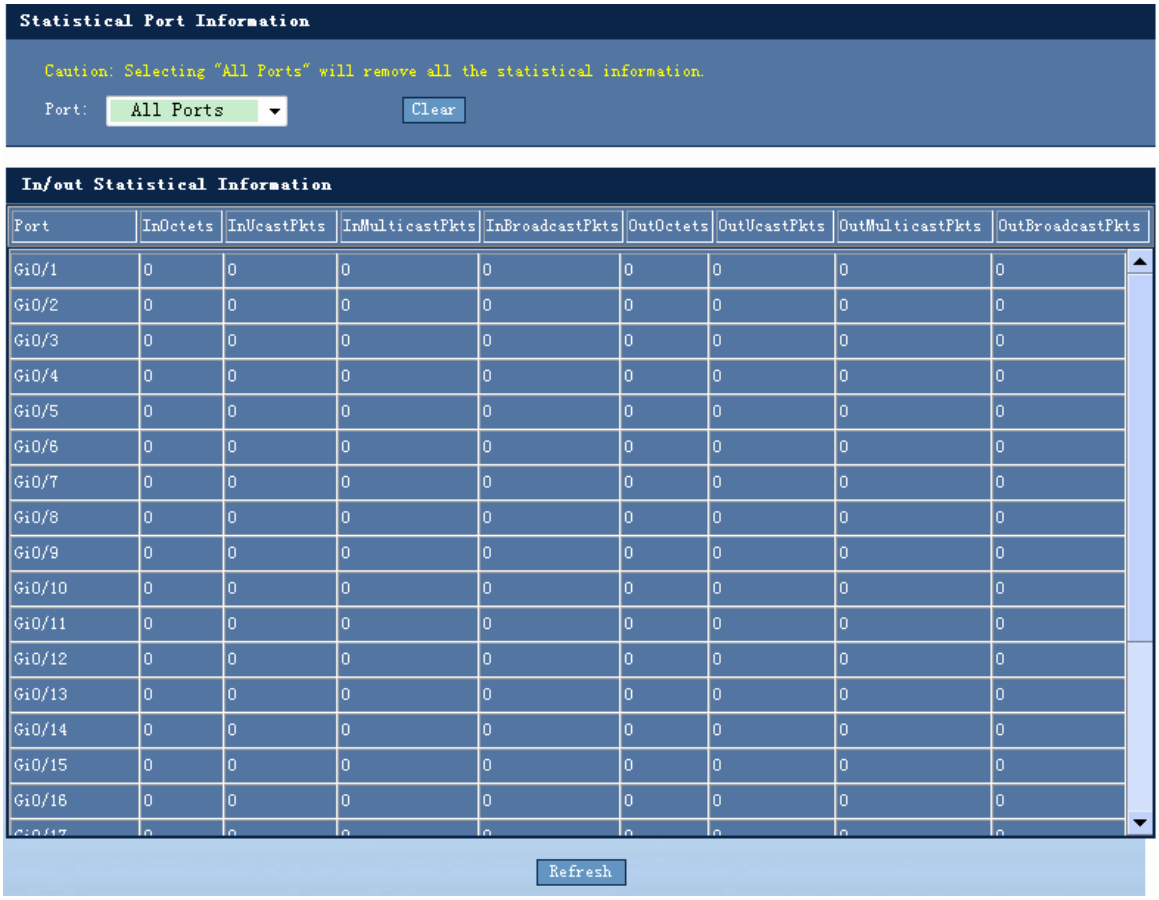


1.3.5.5 Port statistics information

Use the **Port Statistics** Information menu item to enable the function.

Port statistics information page

Figure 1-36 Port statistics information

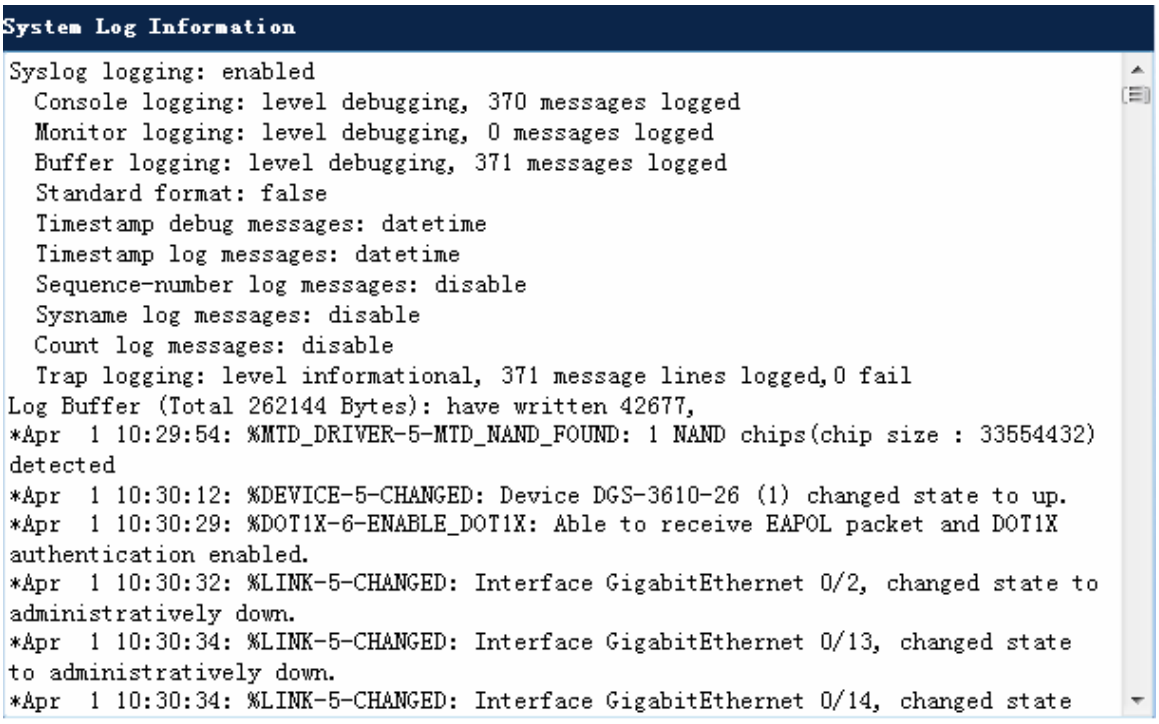


1.3.5.6 Showing the Log information

Use the Log Information menu item to enable the function.

System log information page

Figure 1-37 Showing system log information



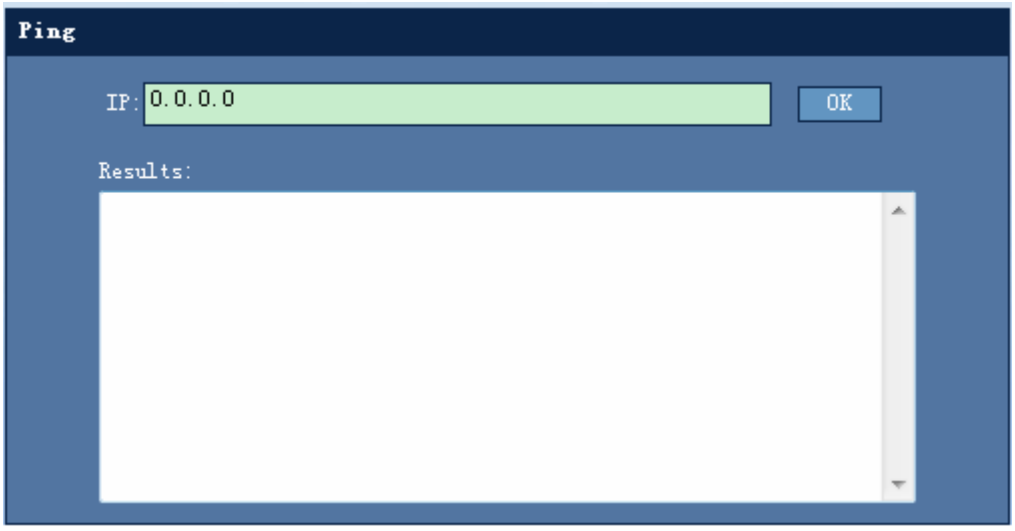
1.3.6 System maintenance

1.3.6.1 Ping

Use the Ping menu item to enable the function.

Ping page

Figure 1-38 Ping



Configuration description:

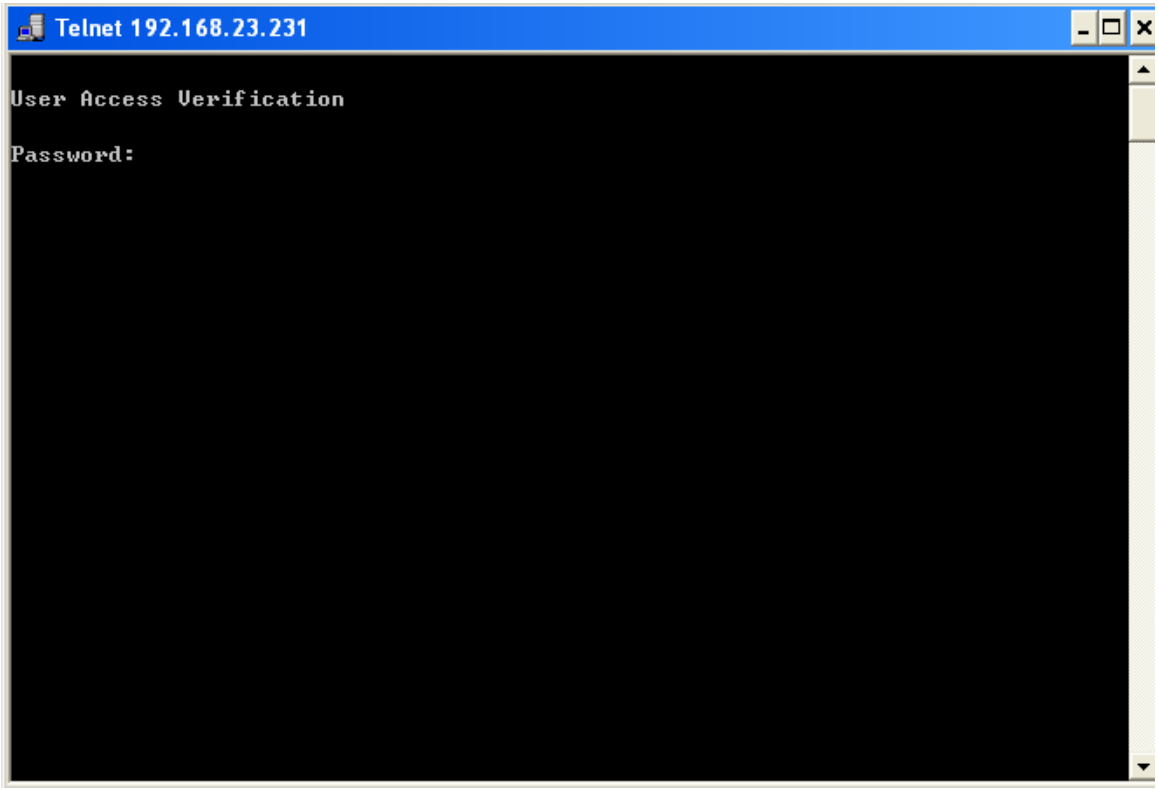
Enter the IP address in the textbox and click Start. If you cannot ping through the IP address, the page makes response after Ping times out.

1.3.6.2 Telnet

Use the Telnet menu item to enable the function.

Telnet page

Figure 1-39 Telnet



Configuration Description:

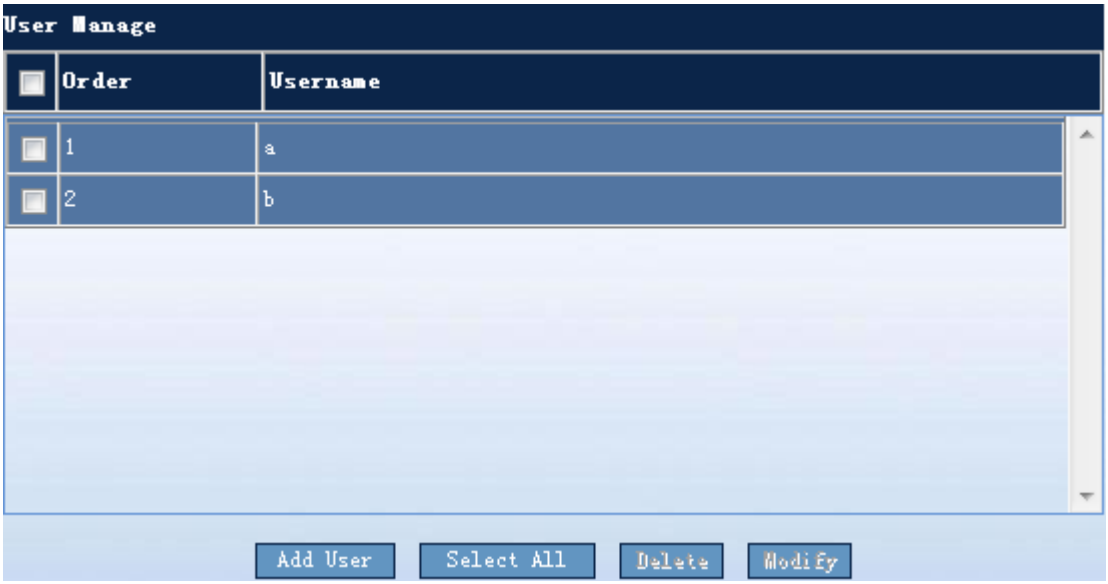
Click the Telnet menu item to enable the Telnet function directly. If the PC does not enable the Telnet service, enable it first.

1.3.6.3 User Management

Use the User Management menu item to enable the function.

User management page

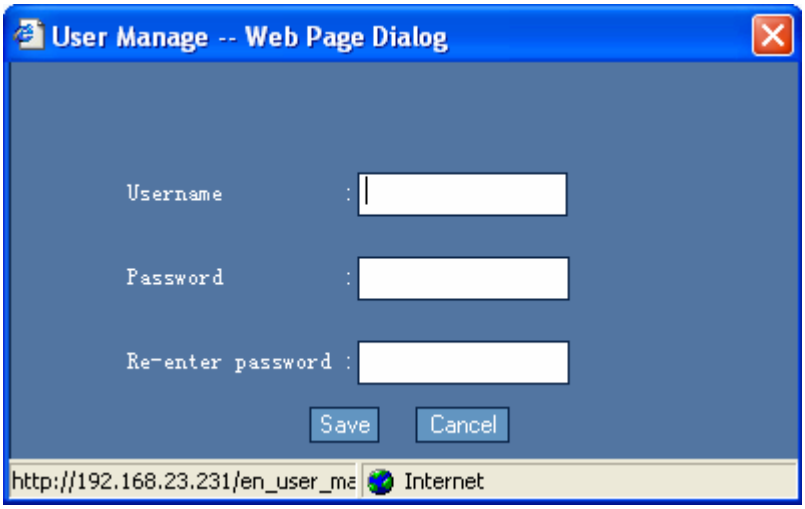
Figure 1-40 Users management



Configuration Description:

Add users: In order to add a new user, click Add users to display the following configuration page.

Figure 1-41 Adding the users

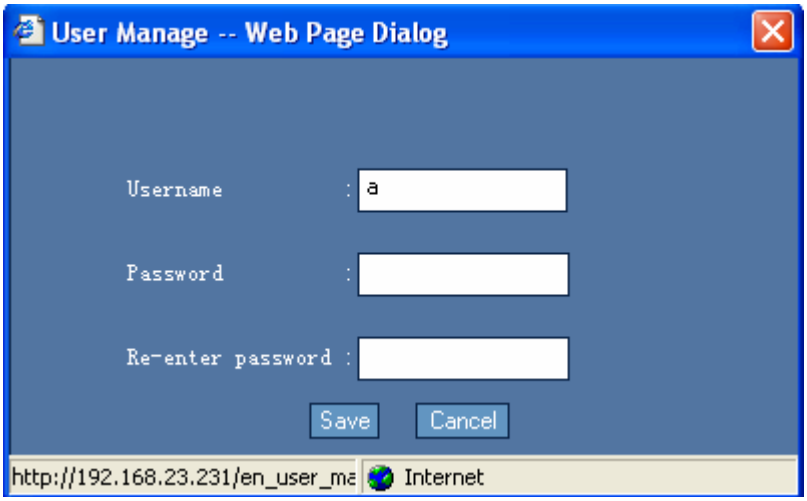


Enter the user name and password and then click **Save** to validate the configuration. After the configuration succeeds, the new user is displayed in the User management page.

Delete: Tick the check box of the user to be deleted and click **Delete**. The selected user is deleted.

Modify: Tick the check box of the user to be modified and click **Modify** to display the following configuration page.

Figure 1-42 Modifying the users



Enter the user name and password and then click **Save** to validate the configuration. After the configuration succeeds, the modified user is displayed in the **User management** page.

Note

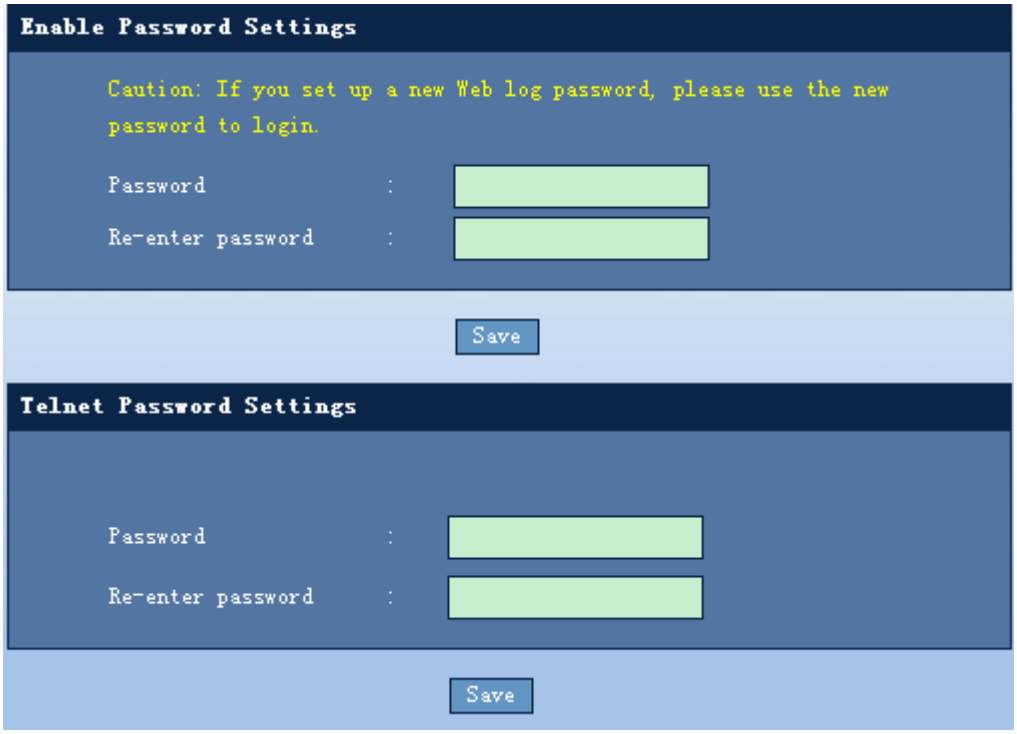
If the deleted or modified user name is the login user name, an authentication dialog box is displayed. Use other user name or the modified user name to re-authenticate. If the current system has only one user name, the user name cannot be deleted.

1.3.6.4 Password setting

Use the Password Setting menu item to enable the function.

Password setting page

Figure 1-43 Password setting

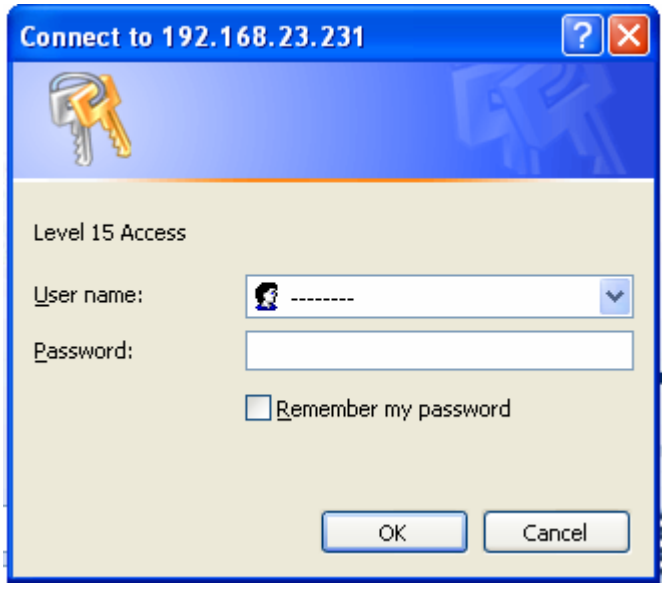


Configuration description:

1) Modifying the password of Enable.

In order to modify the password of Enable, enter the new password and then click **Save** to validate the configuration. The following dialog box is displayed.

Figure 1-44 Login authentication dialog box



Use the new password to log in.

2) Modifying the Telnet login password.

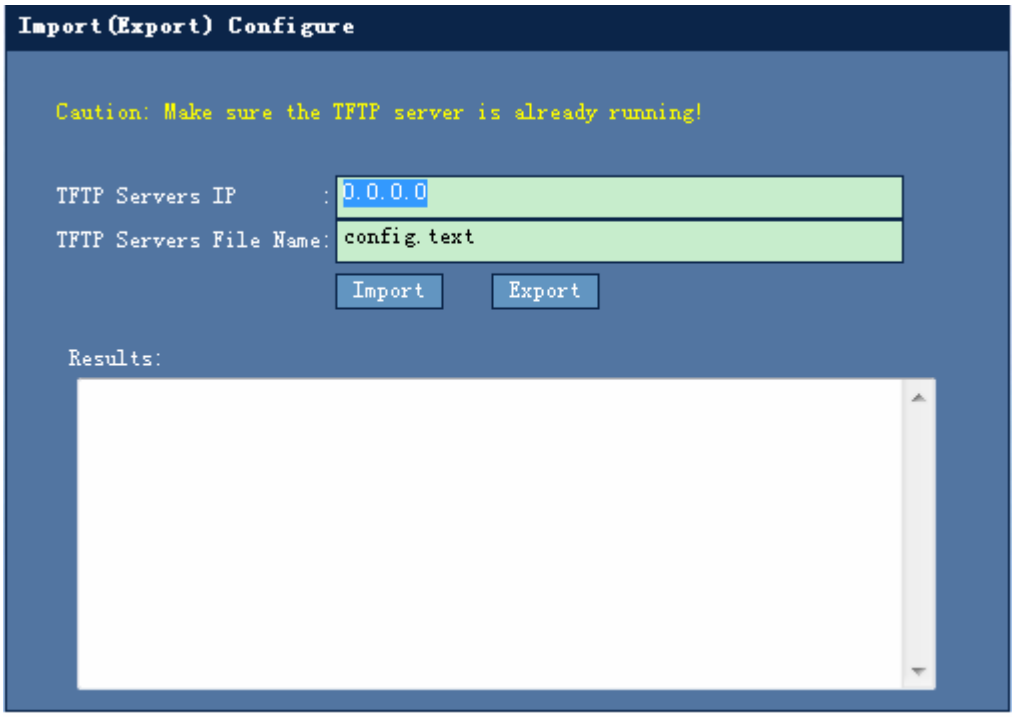
In order to modify the password of Telnet, enter the new password and then click **Save** to validate the configuration.

1.3.6.5 Import/Export Configuration

Use the **Import/Export Configuration** menu item to enable the function.

Import/Export configuration page

Figure 1-45 Import/Export configuration



Configuration description:

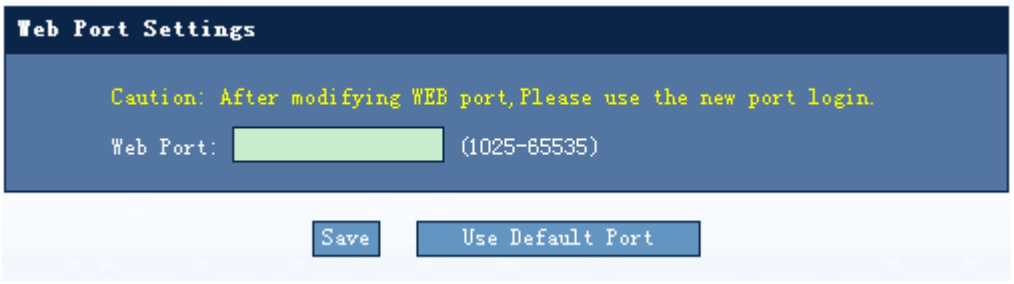
In order to import or export the config.text file in the switch, enter the IP address and file name of the TFTP server and click Save to validate the configuration.

1.3.6.6 Setting the WEB Port

Use the **WEB Port Setting** menu item to enable the function.

WEB port setting page

Figure 1-46 WEB Port setting



Configuration description:

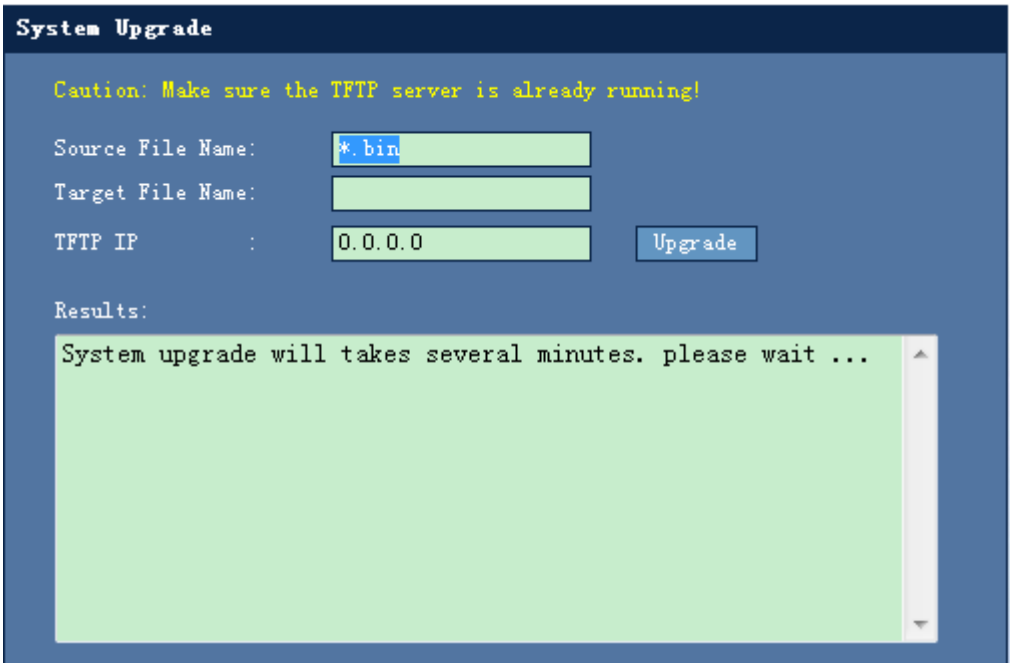
Enter the valid port number and click **Save** to validate the configuration. After the port number is set, log in to the device using the new port. For example, if the new port is 8080 and the IP address of the device is 192.168.1.1, log in to the device through http://192.168.1.1:8080. In order to recover the default port, click **Use the default port** and then re-log in through http://192.168.1.1.

1.3.6.7 System Upgrade

Use the **System Upgrade** menu item to enable the function.

System upgrade page

Figure 1-47 Upgrade system



Configuration description:

In order to upgrade the system, make sure that the TFTP server is enabled. The source file name is the name of the file to be upgraded on the TFTP server and the target file name is

the name of the file after the upgrade. Enter the IP address of the TFTP server and click **Upgrade** to validate the configuration.

1.3.6.8 Exiting the System

Use the **Exiting system** menu item to enable the function.

Configuration Description:

Click the **Exiting system** menu item to close the browser window.

1.3.7 Viewing the Configuration

None.

1.4 Typical Configuration Example for WEB Management

1.4.1 Configuration Keypoints

If the WEB service is enabled, the authentication for WEB management adopts the Enable mode by default.

1.4.2 Configuration steps

The login authentication for WEB management adopts the Local or Enable mode. Users can enter the WEB management page to perform WEB configuration only when the authentication succeeds.

1) Perform login authentication in the Local method.

The detailed configuration is shown as follows.

a. Enter the config mode.

```
DES-7200#configure
Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Enable the WEB service.

```
DES-7200(config)#enable service WEB-server
```

c. Configure the login authentication method for WEB management to Local.

```
DES-7200(config)#ip http authentication local
```

d. Configure the local user name (class 15 users) and password.

```
DES-7200(config)#user name admin password admin
DES-7200(config)#user name admin privilege 15
```

e. Configure the IP address for management.

```
DES-7200(config)#interface vlan 1
DES-7200(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
```

2) Perform login authentication in the Enable method.

The detailed configuration is shown as follows.

a. Enter the config mode.

```
DES-7200#configure

Enter configuration commands, one per line.  End with CNTL/Z.
```

b. Enable the WEB service.

```
DES-7200(config)#enable service WEB-server
```

c. Configure the login authentication method for WEB management to Enable (the command is not displayed after configured).

```
DES-7200(config)#ip http authentication enable
```

d. Configure the password of Enable.

```
DES-7200(config)#enable password admin
```

e. Configure the IP address for management.

```
DES-7200(config)#interface vlan 1

DES-7200(config-if-VLAN 1)#ip address 192.168.100.1 255.255.255.0
```

1.4.3 Authentication Display

1) Perform login authentication in the Local method.

```
DES-7200(config)#show running-config
Building configuration...
Current configuration : 2014 bytes
!
version 10.2(4), Release(55435)(Wed May 13 11:50:07 CST 2009 -ngcf32)
vlan 1
user name admin password admin
```

// User name and password of authentication for WEB management

```
user name admin privilege 15
```

//The WEB management users must be in class 15.

```
no service password-encryption
ip http authentication local
```

// The authentication for WEB management adopts Local.

```
!
enable service WEB-server
```

// Enable the WEB service.

```
!
…..
    ……
!
interface VLAN 1
 ip address 192.168.100.1 255.255.255.0
```

// IP address for management of the device

```
 no shutdown
!
!
line con 0
line vty 0 4
 login
!
!
end
```

2) Perform login authentication in the Enable method.

```
DES-7200(config)#show running-config

Building configuration...
Current configuration : 2014 bytes

!
version 10.2(4), Release(55435)(Wed May 13 11:50:07 CST 2009 -ngcf32)
vlan 1

no service password-encryption

!
```

enable password admin

// The password authentication for WEB management adopts Enable.

enable service WEB-server

// Enable the WEB service.

```
!
…..
```

```
    ……
!
interface VLAN 1

 ip address 192.168.100.1 255.255.255.0
```

// IP address for management of the device

```
no shutdown
!
!
line con 0
line vty 0 4
 login
!
!

end
```