



X S T A C K[®]

Web UI Reference Guide

Product Model: xStack[®] DGS-3400 Series

Layer 2 Managed Gigabit Ethernet Switch

Release 2.7



Information in this document is subject to change without notice.

© 2010 D-Link Corporation. All rights reserved.

Reproduction in any manner whatsoever without the written permission of D-Link Corporation is strictly forbidden.

Trademarks used in this text: D-Link and the D-LINK logo are trademarks of D-Link Corporation; Microsoft and Windows are registered trademarks of Microsoft Corporation.

Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. D-Link Corporation disclaims any proprietary interest in trademarks and trade names other than its own.

April 2010 P/N: 651GS34XX015G

Table of Contents

Intended Readers	ix
Typographical Conventions	ix
Notes, Notices, and Cautions	ix
Web-based Switch Configuration.....	1
Introduction.....	1
Logging in to the Web Manager	1
Web-based User Interface	2
Areas of the User Interface	2
Web Pages.....	3
Administration	4
Device Information	5
IPv6.....	7
Overview.....	7
Packet Format	9
IPv6 Header	9
Extension Headers	10
Packet Fragmentation	10
Address Format	10
Types	11
ICMPv6.....	12
Neighbor Discovery	12
Neighbor Unreachability Detection	12
Duplicate Address Detection (DAD)	13
Assigning IP Addresses	13
IP Interface Setup	13
IP Address.....	14
Interface Settings.....	16
IPv4 Interface Settings	16
IPv6 Interface Settings	18
Stacking.....	21
Stacking Mode Settings	23
Force Master Role Settings	24
Box Information.....	24
Port Configuration.....	25
Port Configuration	25
Port Error Disabled	26
Port Description	27
Port Auto Negotiation Information	28
Port Details	29
Port Media Type	30
Cable Diagnostics	31
User Accounts	32
Password Encryption.....	33
Mirror.....	34
Port Mirror Global Settings.....	34
Port Mirror Settings	34
System Log	36
System Log Host.....	36
System Log Save Mode Settings.....	38
System Log Source Interface Settings.....	39
System Severity Settings.....	39
Command Logging Settings.....	40
SNTP Settings	40
Time Settings	40
Time Zone and DST.....	41
MAC Notification Settings	44
TFTP Services.....	44
Global Settings	44
Port Settings.....	44
Multiple Image Services	46
Firmware Information.....	46
Config Firmware Image	47
RCP	48
RCP Server Settings.....	48
RCP Services	49

Ping Test	50
IPv4 Ping Test.....	50
IPv6 Ping Test.....	51
IPv6 Neighbor.....	52
IPv6 Neighbor Settings.....	52
Route Redistribution Settings.....	53
Static/Default Route Settings.....	54
IPv4 Static/Default Route Settings.....	54
IPv6 Static/Default Route Settings.....	56
Route Preference Settings.....	57
Gratuitous ARP Settings.....	58
Static ARP Settings.....	59
DHCP Auto Configuration Settings.....	60
DHCP/BOOTP Relay.....	60
DHCP / BOOTP Relay Global Settings.....	60
DHCP/BOOTP Relay Interface Settings.....	64
DHCP Relay Option 60 Default Settings.....	64
DHCP Relay Option 60 Settings.....	65
DHCP Relay Option 61 Default Settings.....	66
DHCP Relay Option 61 Settings.....	66
DHCP/BOOTP Local Relay Settings.....	67
DHCPv6 Relay.....	68
DHCPv6 Relay Global Settings.....	68
DHCPv6 Relay Interface Settings.....	68
DHCP Server.....	70
DHCP Server Global Settings.....	70
DHCP Server Exclude Address Settings.....	71
DHCP Server Pool Settings.....	71
DHCP Server Dynamic Binding.....	74
DHCP Server Manual Binding.....	75
DHCPv6 Server.....	76
DHCPv6 Server Global Settings.....	76
DHCPv6 Server Pool Settings.....	77
DHCPv6 Server Manual Binding Settings.....	78
DHCPv6 Server Dynamic Binding Settings.....	79
DHCPv6 Server Interface Settings.....	80
DHCPv6 Server Excluded Address Settings.....	81
Filter DHCP Server.....	82
Filter DHCP Server Global Settings.....	82
Filter DHCP Server Port Settings.....	83
Layer 2 Protocol Tunneling Settings.....	84
RSPAN.....	85
RSPAN State Settings.....	85
RSPAN Settings.....	86
DNS Relay.....	88
DNS Relay Global Settings.....	89
DNS Relay Static Settings.....	89
DNS Resolver.....	90
DNS Resolver Global Settings.....	90
DNS Resolver Static Name Server Settings.....	90
DNS Resolver Dynamic Name Server Table.....	91
DNS Resolver Static Host Name Settings.....	91
DNS Resolver Dynamic Host Name Table.....	92
SNMP Manager.....	93
SNMP Settings.....	93
SNMP Trap Settings.....	94
SNMP User Table.....	95
SNMP View Table.....	97
SNMP Group Table.....	98
SNMP Community Table.....	99
SNMP Host Table.....	100
SNMP Engine ID.....	102
Trap Source Interface Settings.....	102
PoE.....	103
PoE System Settings.....	103
PoE Port Settings.....	105
sFlow.....	107
sFlow Global Settings.....	108
sFlow Analyzer Settings.....	108

sFlow Sampler Settings.....	110
sFlow Poller Settings	112
IP Multicast VLAN Replication.....	114
IP Multicast VLAN Replication Global Settings	114
IP Multicast VLAN Replication Settings	115
Single IP Management (SIM) Overview.....	118
SIM Settings	120
Topology.....	121
Tool Tips	124
Menu Bar	128
Firmware Upgrade	129
Configuration Backup/Restore.....	129
Upload Log	130
RIP	130
RIP	131
RIP Global Settings	132
RIP Interface Settings	132
RIPng	133
RIPng Global Settings	133
RIPng Interface Settings	134
IP Tunnel Settings.....	135
L2 Features	137
VLANs.....	137
Static VLAN Entry.....	142
VLAN Trunk.....	144
GVRP Settings.....	146
Double VLANs	147
Double VLAN Settings.....	149
PVID Auto Assign	151
MAC-based VLAN Settings	152
Protocol VLAN	152
Protocol VLAN Group Settings.....	153
Protocol VLAN Port Settings	154
Subnet VLAN	155
Subnet VLAN Settings	156
VLAN Precedence Settings	156
Trunking.....	158
Link Aggregation	159
LACP Port Settings.....	162
IGMP Snooping	164
IGMP Snooping Settings.....	164
Router Port Settings	166
IGMP Snooping Static Group Settings	168
ISM VLAN Settings.....	169
Limited IP Multicast Address Range Settings.....	172
MLD Snooping	174
MLD Snooping Settings.....	174
MLD Router Port Settings	177
Loop-back Detection Global Settings	179
Spanning Tree	181
STP Bridge Global Settings	183
MST Configuration Identification.....	185
MSTP Port Information	188
STP Instance Settings.....	190
STP Port Settings	191
Forwarding & Filtering	193
Unicast Forwarding.....	193
Multicast Forwarding.....	193
Multicast Filtering Mode.....	194
LLDP.....	195
LLDP Global Settings.....	196
Basic LLDP Port Settings	197
802.1 Extension LLDP Port Settings	198
802.3 Extension LLDP Port Settings	200
LLDP Management Address Settings.....	202
LLDP Statistics	204
LLDP Management Address Table.....	205
LLDP Local Port Table.....	205
LLDP Remote Port Table.....	208
Q-in-Q.....	210

Q-in-Q Settings	210
VLAN Translation Settings.....	211
ERPS	212
ERPS Global Settings	212
ERPS RAPS VLAN Settings	213
DULD Settings.....	216
NLB Multicast FDB Settings	218
QoS	220
QoS	220
The Advantages of QoS	220
Understanding IEEE 802.1p Priority.....	223
802.1p Settings.....	223
802.1p Default Priority Settings.....	224
802.1p User Priority Settings	225
Bandwidth Control	226
Bandwidth Control Settings	226
Per Queue Bandwidth Control Settings.....	228
HOL Prevention Settings	230
Schedule Settings	230
QoS Output Scheduling Settings.....	230
QoS Scheduling Mechanism Settings	232
ACL (Access Control List)	235
Time Range	235
Access Profile Table	236
ACL Flow Meter	254
CPU Interface Filtering	258
Security	275
Authorization Attributes State Settings	275
Traffic Control	276
Port Security	278
Port Security Settings	278
Port Security Entries	279
IP-MAC-Port Binding	280
IMPB Global Settings	282
IMPB Port Settings	283
IMPB Entry Settings	285
DHCP Snoop Entries	286
MAC Block List.....	287
ND Snoop Entries	287
802.1X.....	288
802.1X Port Settings	293
Guest VLAN Settings	296
Authentication RADIUS Server Settings	297
802.1X User Settings	298
Initialize Port(s)	299
Reauthenticate Port(s).....	300
Web-based Access Control (WAC)	302
WAC Global Settings.....	303
WAC Port Settings.....	304
WAC User Account	306
WAC Authentication State.....	307
Trust Host.....	308
BPDU Attack Protection Settings	310
ARP Spoofing Prevention Settings	311
Access Authentication Control.....	312
Authentication Policy and Parameter Settings	314
Application's Authentication Settings	314
Authentication Server Group	315
Authentication Server Host	316
Login Method Lists	318
Enable Method Lists	319
Configure Local Enable Password	321
Enable Admin	322
RADIUS Accounting Settings	323
MAC-based Access Control (MAC)	325
MAC-based Access Control Global Settings	325
MAC-based Access Control Local MAC Settings	328
Safeguard Engine	329

Safeguard Engine Settings	330
Traffic Segmentation.....	331
Secure Socket Layer (SSL)	332
SSL.....	333
Secure Shell (SSH).....	334
SSH Server Configuration.....	335
SSH Authentication Mode and Algorithm Settings	336
SSH User Authentication Mode.....	338
Compound Authentication	339
Compound Authentication Global Settings.....	340
Compound Authentication Settings	341
Authentication Guest VLAN Settings.....	343
Japanese Web-based Access Control (JWAC).....	344
JWAC Global Settings.....	344
JWAC Port Settings	347
JWAC User Account.....	350
JWAC Authentication State.....	351
JWAC Customize Page Language Settings.....	352
JWAC Customize Page.....	353
Monitoring.....	354
Device Status.....	354
Stacking Information.....	355
Stacking Device	356
Module Information	356
DRAM & Flash Utilization.....	357
CPU Utilization.....	358
Port Utilization.....	359
Packets	360
Received (RX)	360
UMB Cast (RX).....	362
Transmitted (TX)	364
Errors.....	366
Received (RX)	366
Transmitted (TX).....	368
Packet Size	370
Browse Router Port.....	372
Browse MLD Router Port	373
VLAN Status.....	373
VLAN Status Port	374
Port Access Control.....	374
Authenticator State.....	374
Authenticator Statistics	375
Authenticator Session Statistics	375
Authenticator Diagnostics.....	376
RADIUS Authentication.....	376
RADIUS Account Client.....	376
MAC Address Table	378
IGMP Snooping Group	379
IGMP Snooping Data Driven Group.....	379
MLD Snooping Group	380
MLD Snooping Data Driven Group.....	380
Trace Route	381
Trace IPv4 Route	381
Trace IPv6 Route	382
Switch Logs.....	383
Browse ARP Table.....	384
Session Table	384
IP Forwarding Table	385
Routing Table.....	385
Browse Routing Table	385
Browse IPv6 Routing Table.....	386
MAC-based Access Control Authentication Status	386
Save, Reset and Reboot.....	387
Reset.....	387
Reboot System	387
Save Services	388
Save Changes.....	388

Configuration Information	389
Current Configuration Settings	390
Appendix A	391
Mitigating ARP Spoofing Attacks Using Packet Content ACL	391
Appendix B	398
Switch Log Entries.....	398
Appendix C	409
Trap Logs	409
Glossary	414

Intended Readers

The *xStack® DGS-3400 Series User Manual* contains information for setup and management of the Switch. This manual is intended for network managers familiar with network management concepts and terminology.

Typographical Conventions

Convention	Description
[]	In a command line, square brackets indicate an optional entry. For example: [copy filename] means that optionally you can type copy followed by the name of the file. Do not type the brackets.
Bold font	Indicates a button, a toolbar icon, menu, or menu item. For example: Open the File menu and choose Cancel . Used for emphasis. May also indicate system messages or prompts appearing on screen. For example: You have mail . Bold font is also used to represent filenames, program names and commands. For example: use the copy command .
Boldface Typewriter Font	Indicates commands and responses to prompts that must be typed exactly as printed in the manual.
Initial capital letter	Indicates a window name. Names of keys on the keyboard have initial capitals. For example: Click Enter.
<i>Italics</i>	Indicates a window name or a field. Also can indicate a variables or parameter that is replaced with an appropriate word or string. For example: type <i>filename</i> means that the actual filename should be typed instead of the word shown in italic.
Menu Name > Menu Option	Menu Name > Menu Option Indicates the menu structure. Device > Port > Port Properties means the Port Properties menu option under the Port menu option that is located under the Device menu.

Notes, Notices, and Cautions



A **NOTE** indicates important information that helps make better use of the device.



A **NOTICE** indicates either potential damage to hardware or loss of data and tells how to avoid the problem.



A **CAUTION** indicates a potential for property damage, personal injury, or death.

Section 1

Web-based Switch Configuration

Introduction

Logging in to the Web Manager

Web-based User Interface

Web Pages

Introduction

All software functions of the xStack® DGS-3400 switch series can be managed, configured and monitored via the embedded web-based (HTML) interface. Manage the Switch from remote stations anywhere on the network through a standard browser. The browser acts as a universal access tool and can communicate directly with the Switch using the HTTP protocol.

The Web-based management module and the Console program (and Telnet) are different ways to access the same internal switching software and configure it. Thus, all settings encountered in web-based management are the same as those found in the console program.

Logging in to the Web Manager

To begin managing the Switch, simply run the browser installed on your computer and point it to the IP address you have defined for the device. The URL in the address bar should read something like: `http://123.123.123.123`, where the numbers 123 represent the IP address of the Switch.



NOTE: The factory default IP address is 10.90.90.90.

This opens the management module's user authentication dialog box, as seen below.

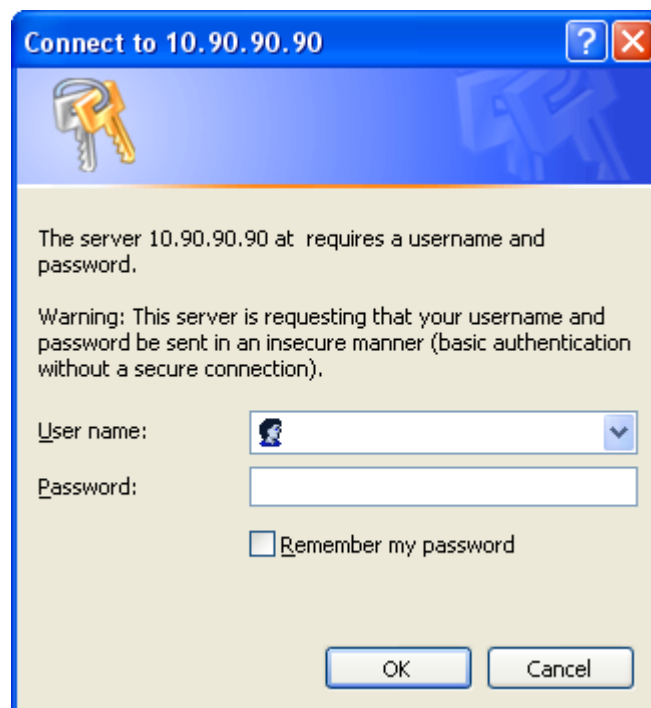


Figure 1 - 1 Enter Network Password dialog box

Leave both the User Name field and the Password field blank and click **OK**. This will open the Web-based user interface. The Switch management features available in the Web-based manager are explained below.

Web-based User Interface

The user interface provides access to various Switch configuration and management windows, allows the user to view performance statistics, and permits graphical monitoring of the system status.

Areas of the User Interface

The figure below shows the user interface. Three distinct areas divide the user interface, as described in the table.

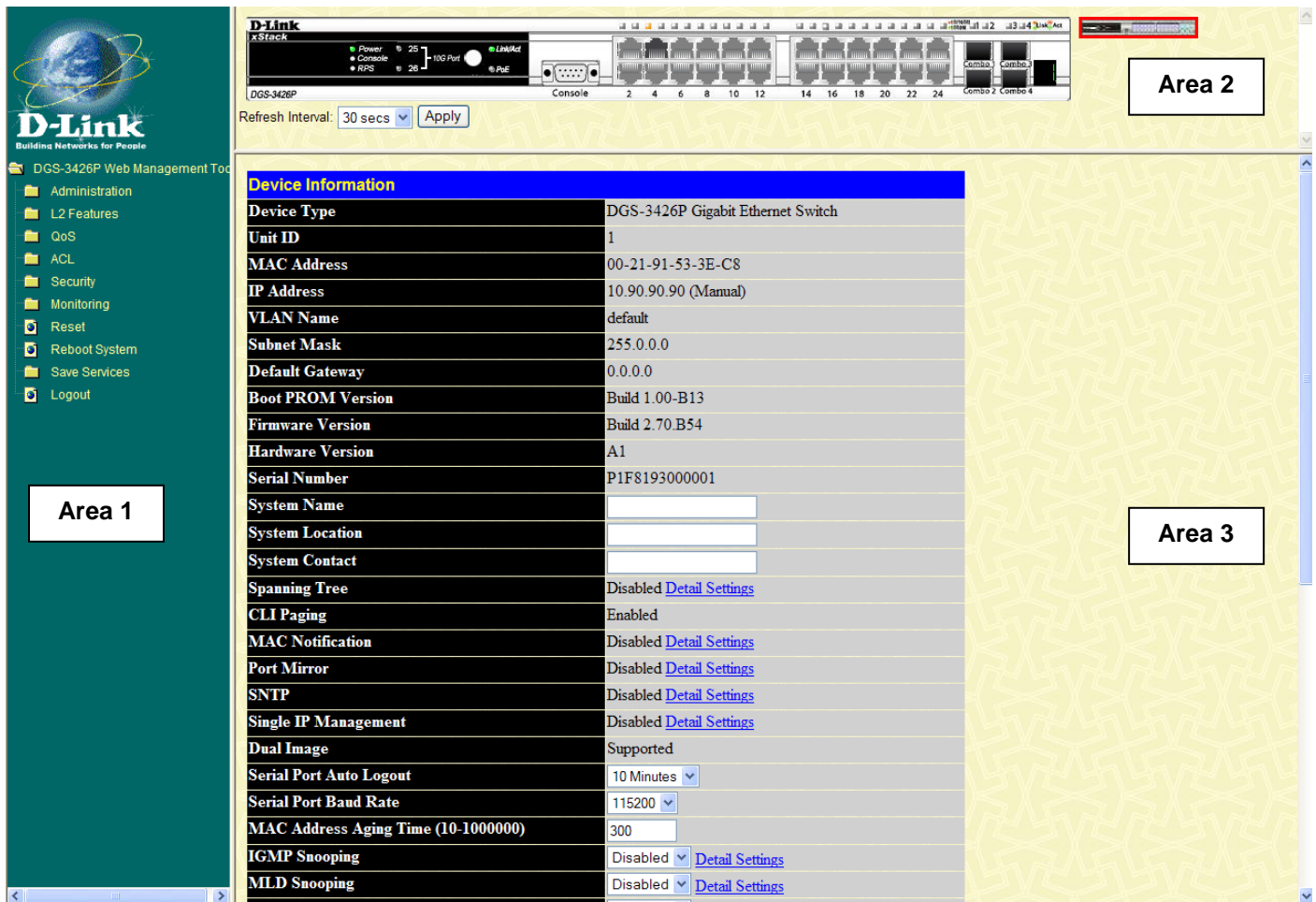


Figure 1- 2 Main Web-Manager window

Area	Function
Area 1	Select the menu or window to display. Open folders and click the hyperlinked menu buttons and subfolders contained within them to display menus. Click the D-Link logo to go to the D-Link website.
Area 2	Presents a graphical near real-time image of the front panel of the Switch. This area displays the Switch's ports and expansion modules, showing port activity, duplex mode, or flow control, depending on the specified mode. Some management functions, including port configuration are accessible here.
Area 3	Presents Switch information based on user selection and the entry of configuration data.

Web Pages

When connecting to the management mode of the Switch with a Web browser, a login screen is displayed. Enter a user name and password to access the Switch's management mode.

Below is a list of the main folders available in the Web interface:

Administration – Contains the following menu pages and sub-directories: IP Address, Interface Settings, Stacking, Port Configuration, User Accounts, Password Encryption, Mirror, System Log, System Severity Settings, Command Logging Settings, SNMP Settings, MAC Notification Settings, TFTP Services, Multiple Image Services, RCP, Ping Test, IPv6 Neighbor, Route Redistribution Settings, Static/Default Route Settings, Route Preference Settings, Gratuitous ARP Settings, Static ARP Settings, DHCP Auto Configuration Settings, DHCP/BOOTP Relay, DHCP/BOOTP Local Relay Settings, DHCPv6 Relay, DHCP Server, DHCPv6 Server, Filter DHCP Server, Layer 2 Protocol Tunneling Settings, RSPAN, DNS Relay, DNS Resolver, SNMP Manager, Trap Source Interface Settings, PoE (DGS-3426P only), sFlow, IP Multicast VLAN Replication, Single IP Management Settings, RIP, and IP Tunnel Settings.

L2 Features – Contains the following menu pages and sub-directories: VLAN, Trunking, IGMP Snooping, MLD Snooping, Loopback Detection Global Settings, Spanning Tree, Forwarding & Filtering, LLDP, Q-in-Q, ERPS, DULD Settings, and NLB Multicast FDB Settings.

QoS – Contains the following menu pages and sub-directories: 802.1p Settings, Bandwidth Control, HOL Prevention Settings, and Schedule Settings.

ACL – Contains the following menu pages and sub-directories: Time Range, Access Profile Table, ACL Flow Meter and CPU Interface Filtering.

Security – Contains the following menu pages and sub-directories: Authorization Network State Settings, Traffic Control, Port Security, IP-MAC-Port Binding, 802.1X, Web-based Access Control (WAC), Trust Host, BPDU Attack Protection Settings, ARP Spoofing Prevention Settings, Access Authentication Control, MAC-based Access Control, Safeguard Engine, Traffic Segmentation, SSL, SSH, Compound Authentication, and Japanese Web-based Access Control (JWAC).

Monitoring – Contains the following menu pages and sub-directories: Device Status, Stacking Information (only when stacking mode is enabled), Stacking Device (only when stacking mode is enabled), Module Information, DRAM & FLASH Utilization, CPU Utilization, Port Utilization, Packets, Errors, Packet Size, Browse Router Port, Browse MLD Router Port, VLAN Status, VLAN Status Port, Port Access Control, MAC Address Table, IGMP Snooping Group, IGMP Snooping Data Driven Group, MLD Snooping Group, MLD Snooping Data Driven Group, Trace Route, Switch Logs, Browse ARP Table, Session Table, IP Forwarding Table, Routing Table, and MAC-based Access Control Authentication Status.

Save Services – Contains the following menu pages and sub-directories: Save Changes, Configure Information, and Current Configuration Settings.

Reset, Reboot System and **Logout** menu links are displayed in the main directory.



NOTE: Be sure to configure the user name and password in the User Accounts window before connecting the Switch to the greater network.

Administration

DGS-3400 Web Management Tool

IP Address

Interface Settings

Stacking

Port Configuration

User Accounts

Password Encryption

Mirror

System Log

System Severity Settings

Command Logging Settings

SNTP Settings

MAC Notification Settings

TFTP Services

Multiple Image Services

RCP

Ping Test

IPv6 Neighbor

Route Redistribution Settings

Static/Default Route Settings

Route Preference Settings

Gratuitous ARP Settings

Static ARP Settings

DHCP Auto Configuration Settings

DHCP/BOOTP Relay

DHCP/BOOTP Local Relay Settings

DHCPv6 Relay

DHCP Server

DHCPv6 Server

Filter DHCP Server

Layer 2 Protocol Tunneling Settings

RSPAN

DNS Relay

DNS Resolver

SNMP Manager

Trap Source Interface Settings

PoE

sFlow

IP Multicast VLAN Replication

Single IP Management (SIM) Overview

RIP

IP Tunnel Settings

Device Information

The **Device Information** window contains the main settings for all major functions for the Switch. It appears automatically when you log on to the Switch. To return to the **Device Information** window after viewing other windows, click the **DGS-3400 Web Management Tool** folder. The **Device Information** window shows the Switch's MAC Address (assigned by the factory and unchangeable), IP Address, VLAN Name, Subnet Mask, Default Gateway, Boot PROM, Firmware Version, Hardware Version and Serial Number. This information is helpful to keep track of PROM and firmware updates and to obtain the Switch's MAC address for entry into another network device's address table, if necessary. The user may also enter a System Name, System Location and System Contact to aid in defining the Switch, to the user's preference. In addition, this window displays the status of functions on the Switch to quickly assess their current global status. Some Functions are hyper-linked for easy access from the **Device Information** window.

Many miscellaneous functions are enabled and disabled in the **Device Information** window.

Device Information	
Device Type	DGS-3426P Gigabit Ethernet Switch
Unit ID	1
MAC Address	00-21-91-53-3E-C8
IP Address	10.90.90.90 (Manual)
VLAN Name	default
Subnet Mask	255.0.0.0
Default Gateway	0.0.0.0
Boot PROM Version	Build 1.00-B13
Firmware Version	Build 2.70.B54
Hardware Version	A1
Serial Number	P1F8193000001
System Name	<input type="text"/>
System Location	<input type="text"/>
System Contact	<input type="text"/>
Spanning Tree	Disabled Detail Settings
CLI Paging	Enabled
MAC Notification	Disabled Detail Settings
Port Mirror	Disabled Detail Settings
SNTP	Disabled Detail Settings
Single IP Management	Disabled Detail Settings
Dual Image	Supported
Serial Port Auto Logout	10 Minutes <input type="text"/>
Serial Port Baud Rate	115200 <input type="text"/>
MAC Address Aging Time (10-1000000)	300 <input type="text"/>
IGMP Snooping	Disabled <input type="text"/> Detail Settings
MLD Snooping	Disabled <input type="text"/> Detail Settings
GVRP Status	Disabled <input type="text"/>
Telnet Status	Enabled <input type="text"/>
Telnet TCP Port Number (1-65535)	23 <input type="text"/>
Web Status	Enabled <input type="text"/>
Web TCP Port Number (1-65535)	80 <input type="text"/>
SNMP Status	Disabled <input type="text"/>
RMON Status	Disabled <input type="text"/>
Link Aggregation Algorithm	MAC Source <input type="text"/>
Switch 802.1X	Disabled <input type="text"/>
Auth Protocol	RADIUS EAP <input type="text"/>
802.1X Authen Network RADIUS	Enabled <input type="text"/>
Forward EAPOL PDU	Disabled <input type="text"/>
HOL Prevention	Enabled <input type="text"/>
Jumbo Frame	Disabled <input type="text"/> Maximum Frame Size: 1536 bytes
Syslog State	Disabled <input type="text"/>
Broadcast Ping Reply State	Enabled <input type="text"/>
ARP Aging Time (0-65535)	20 <input type="text"/> min
RIP State	Disabled Detail Settings
RIPng State	Disabled Detail Settings

Figure 2 - 1 Device Information window

Device Information window configurable parameters include those described in the table below.

Parameter	Description
System Name	Enter a system name for the Switch, if so desired. This name will identify it in the Switch network.
System Location	Enter the location of the Switch, if so desired.
System Contact	Enter a contact name for the Switch, if so desired.
Serial Port Auto Logout Time	Select the logout time used for the console interface. This automatically logs the user out after an idle period of time, as defined. Choose from the following options: <i>2 Minutes</i> , <i>5 Minutes</i> , <i>10 Minutes</i> , <i>15 Minutes</i> or <i>Never</i> . The default setting is <i>10 minutes</i> .
Serial Port Baud Rate	This field specifies the baud rate for the serial port on the Switch. The default setting is 115200.
MAC Address Aging Time (10-1000000)	This field specifies the length of time a learned MAC Address will remain in the forwarding table without being accessed (that is, how long a learned MAC Address is allowed to remain idle). To change this, type in a different value representing the MAC address age-out time in seconds. The MAC Address Aging Time can be set to any value between <i>10</i> and <i>1,000,000</i> seconds. The default setting is <i>300</i> seconds.
IGMP Snooping	To enable system-wide IGMP Snooping capability, select <i>Enabled</i> . IGMP snooping is <i>Disabled</i> by default. Enabling IGMP snooping allows the user to specify use of a multicast router only (see below). To configure IGMP Snooping for individual VLANs, use the IGMP Snooping window under the IGMP Snooping folder.
MLD Snooping	To enable system-wide MLD Snooping capability, select <i>Enabled</i> . MLD snooping is <i>Disabled</i> by default. Enabling MLD snooping allows you to specify use of a multicast router only (see below). To configure MLD Snooping for individual VLANs, use the MLD Snooping window under the MLD Snooping folder.
GVRP Status	Use this pull-down menu to enable or disable GVRP on the Switch.
Telnet Status	Telnet configuration is <i>Enabled</i> by default. If you do not want to allow configuration of the system through Telnet choose <i>Disabled</i> .
Telnet TCP Port Number (1-65535)	The TCP port number used for Telnet management of the Switch. The “well-known” TCP port for the Telnet protocol is 23.
Web Status	Web-based management is <i>Enabled</i> by default. If you choose to disable this by selecting <i>Disabled</i> , you will lose the ability to configure the system through the Web interface as soon as these settings are applied.
Web TCP Port Number (1-65535)	The TCP port number used for Web-based management of the Switch. The “well-known” TCP port for the Telnet protocol is 80.
SNMP Status	Simple Network Management Protocol (SNMP) of the Switch is <i>Enabled</i> or <i>Disabled</i> here.
RMON Status	Remote monitoring (RMON) of the Switch is <i>Enabled</i> or <i>Disabled</i> here.
Link Aggregation Algorithm	The algorithm that the Switch uses to balance the load across the ports that make up the port trunk group is defined by this definition. Choose <i>MAC Source</i> , <i>MAC Destination</i> , <i>MAC Src & Dest</i> , <i>IP Source</i> , <i>IP Destination</i> or <i>IP Src & Dest</i> (See the Link Aggregation section of this manual).
Switch 802.1X	MAC Address may enable by port or the Switch’s 802.1X function; the default is <i>Disabled</i> . This field must be enabled to view and configure certain windows for 802.1X. More information regarding 802.1X, its functions and implementation can be found later in this section, under the Port Access Entity folder. Port-based 802.1X specifies that ports configured for 802.1X are initialized based on the port number only and are subject to any authorization parameters configured. MAC-based Authorization specifies that ports configured for 802.1X are initialized based on the port number and the MAC address of the computer being authorized and are then subject to any authorization parameters configured.
Auth Protocol	The user may use the pull-down menu to choose between <i>RADIUS EAP</i> and <i>Local</i> for the 802.1X authentication protocol on the Switch. The default setting is <i>RADIUS EAP</i> .
802.1X Authen	The user may use the pull-down menu to <i>Enable</i> or <i>Disable</i> the 802.1X Authen Network

Network RADIUS	RADIUS on the Switch. The default setting is <i>Enabled</i> .
Forward EAPOL PDU	The user may use the pull-down menu to <i>Enable</i> or <i>Disable</i> the Forward EAPOL PDU on the Switch. The default setting is <i>Disabled</i> .
HOL Prevention	If this option is enabled it prevents the forwarding of data to a port that is blocked. Traffic that would normally be sent to the buffer memory of the Switch's TX queue is dropped so that memory usage is conserved and performance across all ports remains high.
Jumbo Frame	This field will enable or disable the Jumbo Frame function on the Switch. The default is <i>Disabled</i> . Max. Jumbo frame size = 9216 bytes if this is enabled.
Syslog State	The user may globally enable or disable the Syslog function here by using the pull-down menu. The default is <i>Disabled</i> .
Broadcast Ping Replay State	The user may use the pull-down menu to <i>Enable</i> or <i>Disable</i> the broadcast ping relay.
ARP Aging time (0-65535)	The user may set the ARP Aging Time here by entering a time between 0 and 65535 minutes. The default setting is 20 minutes.

Click **Apply** to implement changes made.

IPv6

The xStack® DGS-3400 has the capability to support the following:

- IPv6 unicast, multicast and anycast addresses
- Allow for IPv6 packet forwarding
- IPv6 fragmentation and re-assembly
- Processing of IPv6 packet and extension headers
- Static IPv6 route configuration
- IPv6 Neighbor Discovery
- Link-Layer Address resolution, Neighbor Unreachability Detection, and Duplicate Address Detection over broadcast mediums (ex: Ethernet)
- Send Router Advertisement
- ICMPv6 functionality

The following sections will briefly explain IPv6, its functionality and how IPv6 is implemented on this Switch.

Overview

IP version 6 is the logical successor to IP version 4. It was known that IPv4 could not support the amount of addresses that would eventually be needed for not only each person, but each device that would require an IP address, and therefore a system with a larger pool of IP addresses was required. IPv6 has addressed that issue, along with other issues that enhance routing over the network, provide better security and improve Quality of Service for Internet users. Some of the improvements made were:

Expanding the Capabilities for IP Addressing – IPv6 has increased the size of the IP address from 32 bits to 128 bits. As a result, the addressing hierarchy has been greatly expanded, more nodes now have the capability of having a unique IP address and the method of assigning an IP address to an interface has become cleaner and quicker. Unicast and multicast addresses still exist but in a purer form and multicast addresses now have a scope field which increases the scalability of multicast routing. Also, an anycast address has been added, which will send packets to the closest node which is a part of a group of nodes, thereby eliminating a specified device for a particular group.

Simplifying the Packet Header – The IPv6 packet header has been simplified from IPv4 as some headers have been modified or dropped altogether, which improves processing speed and cost. The IPv6 header now has a fixed length of 40 bytes consisting of an 8-byte header and two 16-byte IP addresses (source and destination).

Extensions and Options Enhancement – Packet header option fields encoding has been enhanced to allow for proficient forwarding of packets due to lesser restrictions on packet option length and encoding method. This enhancement will also allow

new option fields to be integrated into the IPv6 system without hassles and limitations. These optional headers are placed between the header and the payload of a packet, if they are necessary at all.

Authentication and Privacy Extension Support – New authentication capabilities use extensions for data integrity and data confidentiality for IPv6.

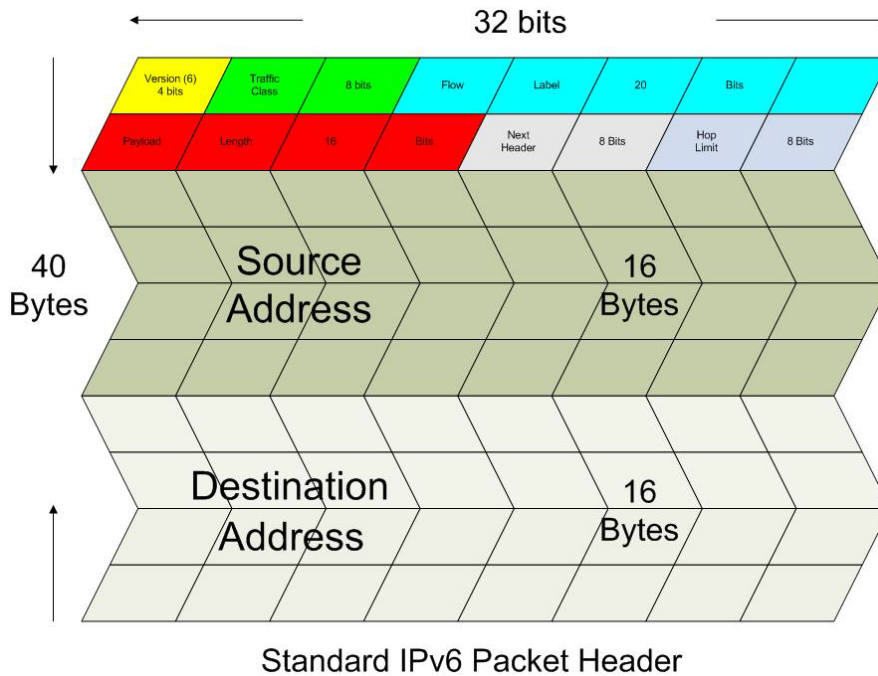
Flow Labeling – This new capability allows packets to be streamlined into certain traffic “flows” if labeled by the sender. In this way, services such as “real time services or non-default quality of service can receive special attention for improved flow quality.

Packet Format

As in IPv4, the IPv6 packet consists of the packet header and the payload, but the difference occurs in the packet header which has been amended and improved for better packet flow and processing. The following will outline and detail the IPv6 enhancements and parts of the IPv6 packet, with special attention to the packet header.

IPv6 Header

The IPv6 packet header has been modified and simplified from IPv4. The header length, identification, flags, fragment offset and header checksum have all been removed in the IPv6 header due to lack of necessity or improvement to a better function of the header. The minimum header length is now 40 bytes. The following picture is an example of an IPv6 packet header.



Standard IPv6 Packet Header

Eight fields make up the basic IPv6 packet header:

Version – This 4-bit field defines the packet version, which is IPv6 and is defined as the number 6.

Traffic Class – This 1-byte field replaces the Type of Service field used in IPv4 and is used to process real-time data and other data requiring special packet management. This field defines the Class of Service priority of an IPv6 packet.

Flow Label – This 20-bit field is used to facilitate the handling of real-time traffic. Hosts sending data can place a flow label into this field to identify a sequence of packets that have an identical set of options. In this way, router can process these packets more efficiently once the flow class has been identified and the rest of the packet header no longer needs to be fully processed, just the flow label and the source address. All flow label packets must have identical source and destination addresses.

Payload Length – Known as the datagram length in IPv4, this 16-bit field specifies the length of the IPv6 data carried after the header of the packet. Extension headers are considered part of the payload and are included in the length specified here.

Next Header – This 8-bit field is used to identify the header immediately following the IPv6 header. When this field is set after the hop by-hop header, it defines the extension header that will appear after the destination address. Each extension header must be preceded by a Next Header field. Integers used to define extension headers in the next Header field use the same values as IPv4 (ex: 6=TCP, 17=UDP, etc.).

Hop Limit - Similar to the TTL field in IPv4, this 8-bit field defines the number of hops remaining after the packet has been processed by a node, instead of the number of seconds left to live as on an IPv4 network. This field will decrement by one after every node it passes and the packet will be discarded once this field reaches zero.

Source Address – This 16-byte field defines the IPv6 address of the source node sending the packet.

Destination Address – This 16-byte field defines the IPv6 address of the destination node receiving the packet. This may or may not be the final destination node of this packet, depending on the routing header, if present.

Extension Headers

Extension headers are used to identify optional parameters regarding IPv6 packets such as routing, fragmentation of packets or authentication parameters. The types of extension headers supported are Hop-by-Hop, Routing, Fragment, Destination Options, Authentication and Encapsulating Security Payload. These extension headers are placed between the IPv6 packet header and the payload and are linked together by the aforementioned Next Header, as shown below.

IPv6 header Next Header = TCP	TCP header + data
--	--------------------------

IPv6 header Next Header = Routing	Routing Header Next Header = TCP	TCP header + data
--	---	--------------------------

IPv6 header Next Header = Destination Options	Destination Options Header Next Header = Routing	Routing Header Next Header = TCP	TCP header + data
--	---	---	--------------------------

Each header has a specific place in the header chain and must follow the following order:

- IPv6 Header
- Hop-By-Hop Header (Must follow the IPv6 header)
- Destination Options
- Routing Header
- Fragment Header
- Authentication Header
- Encapsulating Security Payload Header
- Destination Options Header
- Upper Layer Header

There may be zero, one or more extension headers in the IPv6 header, they must be processed in order and they are to be in increments of 8 octets in the IPv6 packet. Nodes that do not recognize the field of the extension header will discard the packet and send a relevant ICMPv6 message back to the source.

Packet Fragmentation

At times, packets are sent out to a destination that exceed the size of the Path MTU, so the source node is required to split these packets into fragments in individual packets which will be rebuilt when it reaches its final destination. Each of the packets that will be fragmented is given an Identification value, by the source node. It is essential that each of these Identification values is different than any other fragmented packet recently sent that include the same source and destination address. The original packet is divided into two parts, a fragmentable part and an unfragmentable part. The unfragmentable part of the packet consists of the IPv6 header and any extension headers present, up to the routing extension header. The fragmentable part has the payload plus any extension headers that must be processed by the final destination node. This part will be divided into multiple packets that are of a size that can be accepted by the Path MTU. The IPv6 header is then included with this fragmented part and sent to its destination. Once all parts of the fragmented packet reach its destination, they are reassembled using the Fragment Identification value, provided that the source and destination addresses are identical.

Address Format

To address the problem of finding a larger pool of IP addresses for IPv6, the size and format of the IPv4 format needed to be changed. Quadrupling the size of the address, from 32 bits to 128 bits, and encoding addresses using the hexadecimal form were used to solve the problem. In IPv4, the format of the address looked like xxx.xxx.xxx.xxx, where the x's represent integers from 0-9 (ex. 136.145.225.121). Now in IPv6, the format of the address resembles xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx where a

set of xxxx represents a 16-bit hexadecimal value (ex. 2D83:0C76:3140:0000:0000:020C:417A:3214). Although this address looks long and cumbersome, there are some compression rules that will shorten the format of the IPv6 address to make it more compatible to the user.

One such compression rule that is used is to remove leading zeros from any 16-bit hexadecimal value. This is only for zeros that begin the value, not for zeros within the value or ones that are ending the value. Therefore, if we take the previous example IPv6 address and use the compression rules, our IPv6 address would look like this:

2D83:0C76:3140:0000:0000:020C:417A:3214 → 2D83:C76:3140:0:0:20C:417A:3214

The second compression method is to change a string of zero bits into two colons. At times, there may be strings of empty values in the IPv6 address that are unused for this address, but they are necessary for the format of other IPv6 addresses with alternate purposes. To compress these zero strings, the format “::” is used to represent multiple zero fields in the address. This double colon can only be used once in the IPv6 address because when a computer finds a colon, it will expand this field with as many zeros as is necessary to reach the 128-bit address size. If two strings of zeros are present, separated by another non-zero field, a zero must be used to represent one of the two zero fields. So, if we reduce our example using this compression, it would look like this:

2D83:0C76:3140:0000:0000:020C:417A:3214 → 2D83:C76:3140:0:0:20C:417A:3214 → 2D83:C76:3140::20C:417A:3214

When IPv4 and IPv6 nodes are mixed in a network, the IPv6 notation overcomes the difficulty of using an IPv4 address by converting it to the IPv6 format using zeros at the beginning of the IPv4 address. For example, an IP address of 192.168.1.1 is represented in IPv6 format x:x:x:x:d.d.d.d where the x’s are a string of zeros and the d’s represent the normal IPv4 address. (ex. 0:0:0:0:192.168.1.1 or condensed ::192.168.1.1 or hex form ::C0A8:1:1).

Types

IPv6 addresses are classified into three main categories, unicast, multicast and anycast.

Unicast – This address represents a single interface on an IPv6 node. Any packet with a unicast address as its destination address will only be sent to that specific node. Two types of unicast addresses are mainly used for IPv6.

- *Link-Local* – Defined by the IPv6 address prefix FE80::/10, link-local addresses allow for communication to occur between devices on a local link. These addresses are used in neighbor discovery and stateless autoconfiguration.
- *Global Aggregateable* - Defined using a global routing prefix in the range of 2000::/3 to E000::/3, global addresses are aggregated using these routing prefixes to produce unique IPv6 addresses, which will limit global routing table entries. The MAC address of the device is used to produce this address in this form:

Global Routing Prefix + Site Level Aggregator + MAC address (first 3 bits) + FFFE + MAC Address (last 3 bits)

So if your MAC address looks like 00-0C-6E-6B-EB-0C, your IPv6 address may resemble 2000::C:6E:6B:FF:FE:EB:0C/64.

Multicast – Like IPv4, multicast addresses are used to send packets to multiple destinations on a network. These interfaces must be a part of the multicast group. IPv6 multicast prefixes begin with the prefix FF00::/8. FF represents the binary 1111 1111 which identifies a multicast address. The first zero, which is a 4-bit integer, represents the lifetime of the packet. An entry of zero in this field represents a permanent multicast address and an entry of one represents a temporary multicast address. The second zero, which is also a 4-bit integer, defines the scope of the multicast address. This scope defines to what places the multicast address is valid. For example, a value of 1 defines the node, 2 defines the link, 5 defines a site, 8 defines a organization and so on. Not all integers are in use for the scope field. An example of this would be FF02 where the 2 represents a multicast packet going to all the nodes on a local link.

Anycast – The anycast address will send messages to the nearest node of a particular group. This address is assigned to multiple interfaces in the group but only the node with the closest proximity will receive the message. These anycast addresses are allocated from the unicast address space and therefore have no real defined prefix to distinguish it from other IPv6 addresses. The main purpose of the anycast address is to identify a set of routers owned by an organization providing Internet service. It could also be used to identify a set of routers connected to a particular subnet or permitting entrance to a specific routing domain.

Two other special types of addresses exist in IPv6. The **unspecified address** has a value of 0:0:0:0:0:0:0:0 which is comparable to the 0.0.0.0 address in IPv4. This address is used to indicate the lack of a valid IP address on a node and may be used by a device when booting and requesting address configuration notification. In its IPv6 condensed form, it appears as “::” and should not be statically or dynamically assigned to an interface, nor should it be the destination address of an IPv6 packet, or located within the routing header.

The second type of special address is the **loopback address** which is represented by 0:0:0:0:0:0:0:1, or ::1 in its compressed form. It is akin to the 127.0.0.1 address in IPv4 and is used in troubleshooting and testing IP stacks. This address, like the unspecified address, and should not be statically or dynamically assigned to an interface.

ICMPv6

Network professionals are already very familiar with ICMP for IPv4, which is an essential tool in the IPv4 network, relaying messages about network problems and the general condition of the network. ICMPv6 is the successor to the IPv4 version and performs many of the same basic functions as its precursor, yet is not compatible with ICMPv4. ICMPv6 has made improvements over its forerunner, with such enhancements as managing multicast group memberships and allowing for neighbor discovery by resolving link-layer addresses attached to the same link and identifying changes in those addresses. ICMP can also discover routers, determine which neighbors can be reached and map IP addresses to MAC addresses within the network. ICMPv6 is a vital part of the IPv6 network and must be implemented on every IPv6 node for operations to function normally.

Two kinds of ICMP messages are apparent on the IPv6 network:

Error Messages – ICMP error messages are sent out on the network when packet sizes exceed the path MTU (Maximum Transfer Unit), when the hop count of the IPv6 packet has been surpassed, when messages cannot reach their intended destination and when there are parameter problems within the IPv6 packet.

Informational Messages – ICMP informational messages send out packets describing current network information valuable to devices on the network. A common and useful ICMPv6 informational message is the ping program use to discover the availability a device, by using a ping request and reply format. Other informational messages include Path MTU discovery, which is used to determine the maximum size of data packets that can be allowed to be transferred, and Neighbor Discovery messages, which discover routers that can forward packets on the network. Neighbor discovery will be discussed further in the next section.

Neighbor Discovery

Neighbor discovery is a new feature incorporated in IPv6. In IPv4, no means were available to tell if a neighbor could be reached. Now, combining ICMP messages and ARP, neighbors can be detected and their layer 2 addresses (MAC Address) can be identified. This feature can also discover neighboring routers that can forward packets and keep track of the reachability of routers, as well as if changes occur within link-layer addresses of nodes on the network or identical unicast addresses are present on the local link.

The functionality of the Neighbor Discovery feature is based on ICMPv6 packets, Neighbor Solicitation and Router Advertisement messages circulating on the network. When a node wishes to determine link layer addresses of other nodes on the same link, it produces a Neighbor Solicitation message to be circulated on the local link. When received by a neighbor, this neighbor will produce Router Advertisements immediately to be returned. These Router Advertisements will contain a multicast address as the destination address and have an ICMP type of 134 (the specified number for Router Advertisements), as well as having the link-layer address of the node sending the advertisement. Router Advertisement messages may be periodic, specified in the advertisement by having the all-nodes multicast address FF02::1, or sent out as a result of receiving a Neighbor Solicitation message, specified in the advertisement by having the address of the interface that first sent the solicitation message. Once confirmation of the Neighbor has been reached, packets can now be exchanged on the link.

Neighbor Unreachability Detection

At times on the network, problems occur in reaching the Neighbor node or getting a response from the Neighbor. A neighbor is considered reachable when it has received and processed packets sent to it, and in return sends a packet back notifying a affirmative response. This response may come in the form of an indication from an upper-layer protocol, like TCP, noting that progress is being made, or in response from a Neighbor Solicitation message in the form of a Router Advertisement message. If responses are not received from the node, it is considered unreachable and a Destination Unreachable message is received in the form of an ICMP packet. This Destination Unreachable ICMP packet will contain the reason for the fault, located in the code field of the ICMP header. Five possible reasons for the failure can be stated:

1. There is no route or destination (Code 0).
2. Communication has been administratively prohibited, such as a firewall or filter (Code 1)
3. Beyond the scope of the source address, when the multicast scope of the source address is smaller than the scope of the destination address (Code 2)
4. The address is unreachable (Code 3)
5. The port is unreachable (Code 4)

Duplicate Address Detection (DAD)

DAD messages are used to specify that there is more than one node on a local link possessing the same IP address. IPv6 addresses are only leased for a defined period of time. When that time expires, the address will become invalid and another address must be addressed to the node. To ensure that this new address is unique on the local link, a node runs a DAD process to determine the uniqueness of the new address. This is done through the use of a Neighbor Solicitation message containing a Tentative address. This message will detect if another node on the local link has this Tentative address. If the Tentative address is found on another node, that node will send out a Neighbor Advertisement message, the process will be terminated, and manual configuration will be necessary. If no answer is forthcoming regarding this Neighbor Solicitation message containing the tentative address, the address is allotted to the node and connectivity is established.

Assigning IP Addresses

For IPv4 addresses, users may only assign one address per interface and only one address may be used on a particular VLAN. Yet, IPv6 addresses are different. All IPv6 interfaces on the switch must have at least one IPv6 link-local unicast address, if the user is employing the IPv6 addressing scheme. Multiple IPv6 addresses may be configured for IPv6 interfaces, regardless of type, whether it is unicast, multicast or anycast. The scope of the address has some bearing on the assigning multiple addresses to a single interface as well. If multiple physical interfaces are considered as one interface on the Internet layer, multiple unicast addresses may be allotted to multiple physical interfaces, which would be beneficial for load sharing on these interfaces. This is dependent on these unicast addresses having a scope smaller than the link-local address, if these unicast addresses are not the source or destination address for IPv6 packets to or from address that are not IPv6 neighbors of the interface in question.

IP Interface Setup

Each VLAN must be configured prior to setting up the VLAN's corresponding IP interface.

An example is presented below:

VLAN Name	VID	Switch Ports
System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineer	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4
Backbone	6	25, 26

Table 2- 1 VLAN Example - Assigned Ports

In this case, six IP interfaces are required, so a CIDR notation of 10.32.0.0/11 (or a 11-bit) addressing scheme will work. This addressing scheme will give a subnet mask of 11111111.11100000.00000000.00000000 (binary) or 255.224.0.0 (decimal).

Using a 10.xxx.xxx.xxx IP address notation, the above example would give six network addresses and six subnets.

Any IP address from the allowed range of IP addresses for each subnet can be chosen as an IP address for an IP interface on the switch.

For this example, we have chosen the next IP address above the network address for the IP interface's IP Address:

VLAN Name	VID	Network Number	IP Address
System (default)	1	10.32.0.0	10.32.0.1
Engineer	2	10.64.0.0	10.64.0.1
Marketing	3	10.96.0.0	10.96.0.1
Finance	4	10.128.0.0	10.128.0.1
Sales	5	10.160.0.0	10.160.0.1
Backbone	6	10.192.0.0	10.192.0.1

Table 2- 2 VLAN Example – Assigned IP Interfaces

The six IP interfaces, each with an IP address (listed in the table above), and a subnet mask of 255.224.0.0 can be entered into the **Setup IP Interface** window.

IP Address

The IP Address may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the introduction of the *xStack® DGS-3400 Series CLI Manual*. To change IP settings using the web manager you must access the IP Address menu located in the Administration folder.

To configure the Switch's IPv4 address:

To view this window, click **Administration > IP Address**, as shown below.

IP Address	
Get IP From	Manual <input type="button" value="v"/>
IP Address	<input type="text" value="10.90.90.90"/>
Subnet Mask	<input type="text" value="255.0.0.0"/>
Default Gateway	<input type="text" value="0.0.0.0"/>
VLAN Name	<input type="checkbox"/> <input type="text" value="default"/>
<input type="button" value="Apply"/>	
IPv6 Address Settings	
Link-Local Address	
Global Unicast Address	

Figure 2 - 2 IP Address Settings window

To manually assign the Switch's IP address, subnet mask, and default gateway address:

1. Select *Manual* from the Get IP From drop-down menu.
2. Enter the appropriate IP Address and Subnet Mask.
3. If accessing the Switch from a different subnet from the one it is installed on, enter the IP address of the Default Gateway. If managing the Switch from the subnet on which it is installed, the user may leave the default address (0.0.0.0) in this field.
4. If the Switch has no previously configured VLANs, the user can use the default VLAN Name. The default *VLAN* contains all of the Switch ports as members. If the Switch has previously configured VLANs, the user will need to enter the *VLAN Name* of the VLAN that contains the port connected to the management station that will access the Switch. The Switch will allow management access from stations with the same VID listed here.



NOTE: The Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

To use the BOOTP or DHCP protocols to assign the Switch an IP address, subnet mask, and default gateway address:

Use the Get IP From: pull-down menu to choose from *BOOTP* or *DHCP*. This selects the method the Switch assigns an IP address on the next reboot.

The following fields can be set or modified:

Parameter	Description
BOOTP	The Switch will send out a BOOTP broadcast request when it is powered up. The BOOTP protocol allows IP addresses, network masks, and default gateways to be assigned by a central BOOTP server. If this option is set, the Switch will first look for a BOOTP server to provide it with this information before using the default or previously entered settings.
DHCP	The Switch will send out a DHCP broadcast request when it is powered up. The DHCP protocol allows IP addresses, network masks, and default gateways to be assigned by a DHCP server. If this option is set, the Switch will first look for a DHCP server to provide it with this information before using the default or previously entered settings.
Manual	Allows the entry of an IP address, Subnet Mask, and a Default Gateway for the Switch. These fields should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255.
IP Address	This address should be a unique address on the network assigned for use by the network administrator. The form should be xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal form) between 0 and 255.
Subnet Mask	A Bitmask that determines the extent of the subnet that the Switch is on. Should be of the form xxx.xxx.xxx.xxx, where each xxx is a number (represented in decimal) between 0 and 255. The value should be 255.0.0.0 for a Class A network, 255.255.0.0 for a Class B network, and 255.255.255.0 for a Class C network, but custom subnet masks are allowed.
Default Gateway	IP address that determines where packets with a destination address outside the current subnet should be sent. This is usually the address of a router or a host acting as an IP gateway. If your network is not part of an intranet, or you do not want the Switch to be accessible outside your local network, you can leave this field unchanged.
VLAN Name	This allows the entry of a VLAN Name from which a management station will be allowed to manage the Switch using TCP/IP (in-band via Web manager or Telnet). Management stations that are on VLANs other than the one entered here will not be able to manage the Switch in-band unless their IP addresses are entered in the Security IP Management window. If VLANs have not yet been configured for the Switch, the default VLAN contains all of the Switch's ports. There are no entries in the Security IP Management table, by default, so any management station that can connect to the Switch can access the Switch until a management VLAN is specified or Management Station IP Addresses are assigned.

Click **Apply** to implement the changes.

This window also contains the current IPv6 setup on the Switch. Configuring IPv6 interfaces can be done in under the Interface Settings heading, by clicking the link **IPv6 Interface Settings**, which will be discussed in the next section.

Setting the Switch's IP Address using the Console Interface

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. The default Switch IP address can be changed to meet the specification of your networking address scheme.

The IP address for the Switch must be set before the Web-based manager can manage the switch. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known. The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

- Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the x's represent the IP address to be assigned to the IP interface named System and the y's represent the corresponding subnet mask.
- Alternatively, the user can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the x's represent the IP address to be assigned to the IP interface named System and the z represents the corresponding number of subnets in CIDR notation.

The IP interface named System on the Switch can be assigned an IP address and subnet mask, which can then be used to connect a management station to the Switch's Telnet or Web-based management agent.

Successful entry of the command will produce a “Success” message, indicating that the command execution was correctly. The user may now utilize this address to configure or manage the Switch through Telnet, the Command Line Interface (CLI) or the Web-based management (GUI).

Interface Settings

The IP address may initially be set using the console interface prior to connecting to it through the Ethernet. If the Switch IP address has not yet been changed, read the introduction of the *xStack® DGS-3400 Series CLI Manual* or return to Section 4 of this manual for more information. To change IP settings using the Web manager, users must access the **IP Address** window (**Administration > IP Address**). Open **Administration** folder and click **Interface Settings** to access two folders to set up IP interfaces on the Switch, one for IPv4 addresses, **IPv4 Interface Settings**, and one for IPv6 addresses, **IPv6 Interface Settings**.

IPv4 Interface Settings

To view this window, click **Administration > Interface Settings > IPv4 Interface Settings**, as shown below.

Add Clear All										
Total Entries: 1										
IPv4 Interface Settings										
Interface Name	IP Address	Subnet Mask	VLAN Name	Secondary	Proxy ARP	Proxy Local ARP	IP Directed Broadcast	Interface Admin State	Modify	Delete
System	10.90.90.90	255.0.0.0	default	False	Disabled	Disabled	Disabled	Enabled	Modify	X

Figure 2 - 3 IPv4 Interface Settings window

To manually assign the Switch's IPv4 address and its related configurations, click the **Add** button, revealing the following window to configure.

IPv4 Interface Settings - Add	
Interface Name	<input type="text"/>
IP Address	<input type="text" value="0.0.0.0"/>
Subnet Mask	<input type="text" value="0.0.0.0"/>
VLAN Name	<input type="checkbox"/> <input type="text"/>
Interface Admin State	Disabled ▾
Secondary	False ▾
Proxy ARP	Disabled ▾
Proxy Local ARP	Disabled ▾
Apply	
Show All IP Interface Entries	

Figure 2 - 4 IPv4 Interface Settings - Add window

To change the settings for a configured Interface, click the corresponding **Modify** button, which will display the following window for the user to configure.

IPv4 Interface Settings - Edit	
Interface Name	System
IP Address	10.90.90.90
Subnet Mask	255.0.0.0
VLAN Name	<input type="checkbox"/> default
Interface Admin State	Enabled ▾
Secondary	False ▾
Proxy ARP	Disabled ▾
Proxy Local ARP	Disabled ▾
IP Directed Broadcast	Disabled ▾
<input type="button" value="Apply"/>	
Show All IP Interface Entries	

Figure 2 - 5 IPv4 Interface Settings - Edit window

Enter a name for the new interface to be added in the Interface Name field (if editing an IP interface, the Interface Name will already be in the top field as seen in the window above). Enter the interface's IP address and subnet mask in the corresponding fields. Pull the Interface Admin State pull-down menu to *Enabled* and click **Apply** to enter to make the IP interface effective. To view entries in the **IP Interface Settings**, click the [Show All IP Interface Entries](#) hyperlink. Use the **Save Services > Save Changes** to enter the changes into NV-RAM.

The following fields can be set or modified:

Parameter	Description
Interface Name	This field displays the name for the IP interface or it is used to add a new interface created by the user. The default IP interface is named "System".
IP Address	This field allows the entry of an IPv4 address to be assigned to this IP interface.
Subnet Mask	This field allows the entry of a subnet mask to be applied to this IP interface.
VLAN Name	This field displays the VLAN name directly associated with this interface.
Interface Admin. State	Use the pull-down menu to enable or disable configuration on this interface.
Secondary	Use the pull-down menu to set the IP interface as <i>True</i> or <i>False</i> . <i>True</i> will set the interface as secondary and <i>False</i> will denote the interface as the primary interface of the VLAN entered above. <i>Secondary</i> interfaces can only be configured if a <i>primary</i> interface is first configured.
Proxy ARP	Use the pull-down menu to enable or disable the proxy ARP state on the IP interface.
Proxy Local ARP	Use the pull-down menu to enable or disable the proxy local ARP. This function allows the Switch to respond to the proxy ARP, if the source IP and destination IP are in the same interface.
IP Directed Broadcast	Use the pull-down menu to enable or disable the IP directed-broadcast state of a specified interface.

Click **Apply** to implement the changes.



NOTE: The Switch's factory default IP address is 10.90.90.90 with a subnet mask of 255.0.0.0 and a default gateway of 0.0.0.0.

IPv6 Interface Settings

This window is used to set up IPv6 interfaces and addresses for the Switch.

To view this window, click **Administration > Interface Settings > IPv6 Interface Settings**, as shown below.

The screenshot shows the IPv6 Interface Settings window. At the top, there are 'Add' and 'Clear All' buttons. Below them, it says 'Total Entries: 1'. The main content is a table with the following data:

Interface Name	VLAN Name	Interface Admin State	DHCPv6 Client State	Modify	Delete
System	default	Enabled	Disabled	Modify	X

Figure 2 - 6 IPv6 Interface Settings window

To add a new IPv6 interface, click the **Add** button, which will display the following window.

The screenshot shows the 'IPv6 Interface Settings - Add' window. It contains three input fields: 'Interface Name', 'VLAN Name', and 'Interface Admin State'. The 'Interface Admin State' field is a dropdown menu currently set to 'Enabled'. There is an 'Apply' button at the bottom right and a link 'Show All IPv6 Interface Entries' at the bottom left.

Figure 2 - 7 IPv6 Interface Settings - Add window

To add an Interface, enter an **Interface Name** in the field provided, along with a corresponding **VLAN Name**, set the **Interface Admin. State** to *Enabled* and click **Apply**. Newly created interfaces will appear in the **IPv6 Interface Settings** window.

To change the settings for a configured Interface, click the corresponding **Modify** button, which will display the following window for the user to configure.

IPv6 Interface Settings - Edit	
Interface Name	System
Automatic Link Local Address	Disabled
Link-Local Address	
Global Unicast Address	
VLAN Name	default
Interface Admin State	Enabled
DHCPv6 Client State	Disabled
IPv6 Address	
NS Retransmit Time (ms)	0
Hop Limit	64
Prefix Options	
Prefix	
Preferred Life Time	604800
Valid Life Time	2592000
On Link Flag	Enabled
Autonomous Flag	Enabled
Router Advertisement Settings	
RA Router Advertisement	Disabled
RA Router Life Time (sec)	1800
RA Reachable Time	1200000
RA Retransmit Time (ms)	0
RA Managed Flag	Disabled
RA Other Configure Flag	Disabled
RA Max Router AdvInterval (sec)	600
RA Min Router AdvInterval (sec)	198
<input type="button" value="Apply"/>	
Show All IPv6 Interface Entries	

Figure 2 - 8 IPv6 Interface Settings - Edit window

The following fields may be viewed or modified.

Parameter	Description
Interface Name	This field displays the name for the IP interface, or it is used to add a new interface. The default IP interface is named "System". The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For Global IPv6 addresses, this field may be omitted.
Automatic Link Local Address	Use this pull-down menu to enable or disable the Automatic Link Local Address. When enabled, the switch will automatically create an IPv6 link-local address for the switch. Once the user enables this feature and clicks Apply , an IPv6 address will be produced based on the MAC address of the switch and the new entry will appear in the following Link-Local Address field.
Link-local Address	This field displays the IPv6 address created automatically by the Switch, based on the MAC Address of the Switch. This is a site local address used only for local routing.
Global Unicast Address	This field is the unicast address that will be used by the Switch for packets coming from outside the site-local address, or the public IPv6 address, when connected directly to the Internet.

VLAN Name	This field states the VLAN Name directly associated with this interface.
Interface Admin State	Use the pull-down menu to enable or disable configuration on this interface.
DHCPv6 Client State	Use the pull-down menu to enable or disable the DHCPv6 client state of the interface.
IPv6 Address	Use this field to set a Global Unicast Address for the Switch. This address will be used to access the network outside of the local link.
NS Retransmit Time	Use this field to set the interval, in seconds that this Switch will produce Neighbor Solicitation packets to be sent out over the local network. This is used to discover IPv6 neighbors on the local link. The user may select a time between 0 and 65535 milliseconds. Very fast intervals, represented by a low number, are not recommended for this field.
Hop Limit	This field sets the number of nodes that this Router Advertisement packet will pass before being dropped. This number is set to depreciate by one after every node it reaches and will be dropped once the Hop Limit reaches 0. The user may set the Hop Limit between 0 and 255 with a default value of 64.
Prefix Options	
Prefix	Use this field to set a prefix for Global Unicast IPv6 addresses to be assigned to other nodes on the link-local network. This prefix is carried in the Router Advertisement message to be shared on the link-local network. The user must first have a Global Unicast Address set for the Switch.
Preferred Life Time	This field states the time that this prefix is advertised as being preferred on the link local network, when using stateless address configuration. The user may configure a time between 0 and 4294967295 milliseconds, with a default setting of 604800 milliseconds.
Valid Life Time	This field states the time that this prefix is advertised as valid on the link local network, when using stateless address configuration. The user may configure a time between 0 and 4294967295 milliseconds.
On Link Flag	Setting this field to <i>Enabled</i> will denote, within the IPv6 packet, that the IPv6 prefix configured here is assigned to this link-local network. Once traffic has been successfully sent to these nodes with this specific IPv6 prefix, the nodes will be considered reachable on the link-local network.
Autonomous Flag	Setting this field to <i>Enabled</i> will denote that this prefix may be used to autoconfigure IPv6 addresses on the link-local network.
Router Advertisement Settings	
RA Router Advertisement	Use this pull-down menu to enable or disable the switch as being capable of accepting solicitation from a neighbor, and thus becoming an IPv6 neighbor. Once enabled, this Switch is now capable of producing Router Advertisement messages to be returned to querying neighbors.
RA Router Lifetime (sec)	This time represents the validity of this interface to be the default router for the link-local network. A value of 0 represents that this Switch should not be recognized as the default router for this link-local network. The user may set a time between 0 and 9000 seconds with a default setting of 1800 seconds.
RA Reachable Time	This field will set the time that remote IPv6 nodes are considered reachable. In essence, this is the Neighbor Unreachability Detection field once confirmation of the access to this node has been made. The user may set a time between 0 and 36000000 milliseconds with a default setting of 1200000 milliseconds. A very low value is not recommended.
RA Retransmit Time (ms)	Used to set an interval time between 0 and 4294967295 milliseconds for the dispatch of router advertisements by this interface over the link-local network, in response to a Neighbor Solicitation message. If this Switch is set as the default router for this local link, this value should not exceed the value stated in the Life Time field previously mentioned. Setting this field to zero will specify that this switch will not specify the Retransmit Time for the link-local network. (therefore it will be specified by another router on the link-local network. The default value is 0 milliseconds.

RA Managed Flag	Use the pull-down menu to enable or disable the Managed flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get both Global and link-local IPv6 addresses for the Switch. The default setting is <i>Disabled</i> .
RA Other Configure Flag	Use the pull-down menu to enable or disable the Managed flag. When enabled, this will trigger the router to use a stateful autoconfiguration process to get configuration information that is not address information, yet is important to the IPv6 settings of the Switch. The default setting is <i>Disabled</i> .
RA Max Router AdvInterval (sec)	Used to set the maximum interval time between the dispatch of router advertisements by this interface over the link-local network. This entry must be no less than 4 seconds (4000 milliseconds) and no more than 1800 seconds. The user may configure a time between 4 and 1800 seconds with a default setting of 600 seconds.
RA Min Router AdvInterval (sec)	Used to set the minimum interval time between the dispatch of router advertisements by this interface over the link-local network. This entry must be no less than 3 seconds and no more than .75 (3/4) of the MaxRtrAdvInterval. The user may configure a time between 3 and 1350 seconds with a default setting of 198 seconds.

Click **Apply** to implement the changes.

Stacking

From firmware release v2.00 of this Switch, the xStack® DGS-3400 series now supports switch stacking, where a set of twelve switches can be combined to be managed by one IP address through Telnet, the GUI interface (web), the console port or through SNMP. Each switch of this series has either two or three stacking slots located at the rear of the device, which can be used to add 10-gigabit DEM-410CX or DEM-410X stacking modules, sold separately. After adding these stacking ports, the user may connect these ports together using copper or fiber stacking cables (also sold separately) in one of two possible topologies.

Duplex Ring – As shown in Figure 2-9, the Duplex Ring stacks switches in a ring or circle format where data can be transferred in two directions. This topology is very resilient because if there is a break in the ring, data can still be transferred through the stacking cables between switches in the stack.

Duplex Chain – As shown in Figure 2-10, The Duplex Chain topology stacks switches together in a chain-link format. Using this method, data transfer is only possible in one direction and if there is a break in the chain, then data transfer will obviously be affected.

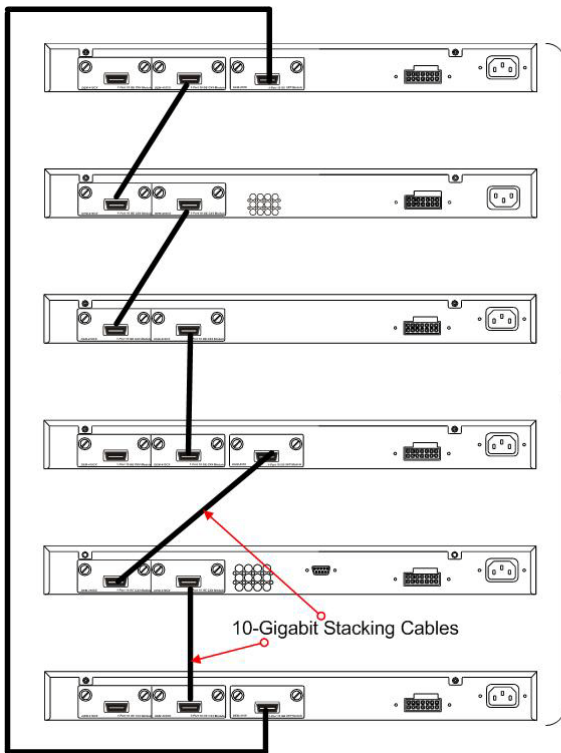


Figure 2 - 9 Switches stacked in a Duplex Ring

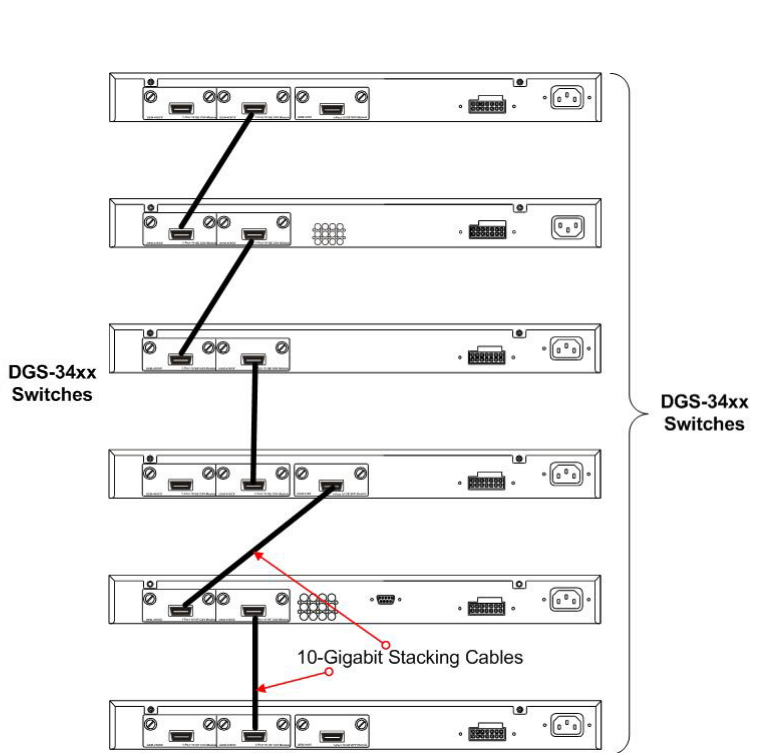


Figure 2 - 10 Switches stacked in a Duplex Chain

Within each of these topologies, each switch plays a role in the Switch stack. These roles can be set by the user per individual Switch, or if desired, can be automatically determined by the switch stack. Three possible roles exist when stacking with the xStack® DGS-3400 series.



NOTE: Only ports 26 and 27 of the DGS-3427 support stacking. Port 25 cannot be used for stacking, and can only be used as a 10-Gigabit uplink port.

Primary Master – The Primary Master is the leader of the stack. It will maintain normal operations, monitor operations and the running topology of the Stack. This switch will also assign Stack Unit IDs, synchronize configurations and transmit commands to remaining switches in the switch stack. The Primary Master can be manually set by assigning this Switch the highest priority (a lower number denotes a higher priority) before physically assembling the stack, or it can be determined automatically by the stack through an election process, which determines the lowest MAC address. It will then assign that switch as the Primary Master, if all priorities are the same. The Primary master is physically displayed by the seven segment LED to the far right on the front panel of the switch where this LED will flash between its given Box ID and ‘H’.

Backup Master – The Backup Master is the backup to the Primary Master, and will take over the functions of the Primary Master if the Primary Master fails or is removed from the Stack. It also monitors the status of neighboring switches in the stack, will perform commands assigned to it by the Primary Master and will monitor the running status of the Primary Master. The Backup Master can be set by the user by assigning this Switch the second highest priority before physically assembling the stack, or it can be determined automatically by the stack through an election process which determines the second lowest MAC address and then will assign that switch as the Backup Master, if all priorities are the same.

Slave – Slave switches constitute the rest of the switch stack and although not Primary or Backup Masters, they can be placed into these roles when these other two roles fail or are removed from the stack. Slave switches perform operations requested by the master, monitor the status of neighbor switches in the stack and the stack topology and adhere to the Backup Master’s commands once it becomes a Primary Master. Slave switches will do a self-check to determine if it is to become the Backup Master if the Backup Master is promoted to the Primary Master, or if the Backup Master fails or is removed from the switch stack. If both Primary and Backup masters fail, or are removed from the Switch stack, it will determine if it is to become the Primary Master. These roles will be determined, first by priority and if the priority is the same, the lowest MAC address.

Once switches have been assembled in the topology desired by the user and powered on, the stack will undergo three processes until it reaches a functioning state.

Initialization State – This is the first state of the stack, where the runtime codes are set and initialized and the system conducts a peripheral diagnosis to determine each individual switch is functioning properly.

Master Election State – Once the codes are loaded and initialized, the stack will undergo the Master Election State where it will discover the type of topology used, elect a Primary Master and then a Backup Master.

Synchronization State – Once the Primary Master and the Backup Master have been established, the Primary Master will assign Stacking Unit IDs to switches in the stack, synchronize configurations for all switches and then transmit commands to the rest of the switches based on the user’s configurations of the Primary Master.

Once these steps have been completed, the switch stack will enter a normal operating mode.

Stack Switch Swapping

The stacking feature of the xStack® DGS-3400 supports “hot swapping” of switches in and out of the running stack. Users may remove or add switches to the stack without powering down or largely affecting the transfer of data between switches in the stack, with a few minor provisions.

When switches are “hot inserted” into the running stack, the new switch may take on the Backup Master or Slave role, depending on configurations set on the newly added switch, such as configured priority or MAC address. The new device will not be the Primary Master, if adding one switch at a time to the Stack. Yet, if adding two stacks together that have both previously undergone the election process, and therefore both have a Primary Master and a Backup master, a new Primary Master will be elected from one of the already existing Primary Masters, based on priority or MAC address. This Primary Master will take over all of the Primary Master’s roles for all new switches that were hot inserted. This process is done using discovery packets that circulate through the switch stack every 1.5 seconds until the discovery process has been completed.

The “hot remove” action means removing a device from the stack while the stack is still running. The hot removal is detected by the stack when it fails to receive heartbeat packets during its specified interval from a device, or when one of the stacking ports links is down. Once the device has been removed, the remaining switches will update their stacking topology database to reflect the change. Any one of the three roles, Primary Master, Backup Master or Slave, may be removed from the stack, yet different processes occur for each specific device removal.

If a Slave device has been removed, the Primary Master will inform other switches of the hot remove of this device through the use of unit leave messages. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well.

If the Backup Master has been hot removed, a new Backup Master will be chosen through the election process previously described. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. Then the Backup Master will begin backing up the Primary Master when the database synchronization has been completed by the stack.

If the Primary Master is removed, the Backup Master will assume the Primary Master’s role and a new Backup Master will be chosen using the election process. Switches in the stack will clear the configurations of the unit removed, and dynamically learned databases, such as ARP, will be cleared as well. The new Primary Master will inherit the MAC and IP address of the previous Primary Master to avoid conflict within the stack and the network itself.

If both the Primary Master and the Backup Master are removed, the election process is immediately processed and a new Primary Master and Backup Master are determined. Switches in the stack will clear the configurations of the units removed, and dynamically learned databases, such as ARP, will be cleared as well. Static switch configurations still remain in the database of the remaining switches in the stack and those functions will not be affected.



NOTE: If there is a Box ID conflict when the stack is in the discovery phase, the device will enter a special standalone topology mode. Users can only get device information, configure Box IDs, save and reboot. All stacking ports will be disabled and an error message will be produced on the local console port of each device in the stack. Users must reconfigure Box IDs and reboot the stack.

Stacking Mode Settings

To begin the stacking process, users must first enable this device for stacking by using the Stacking Mode Settings window.

To view this window, click **Administration > Stacking > Mode Settings**, as shown below.

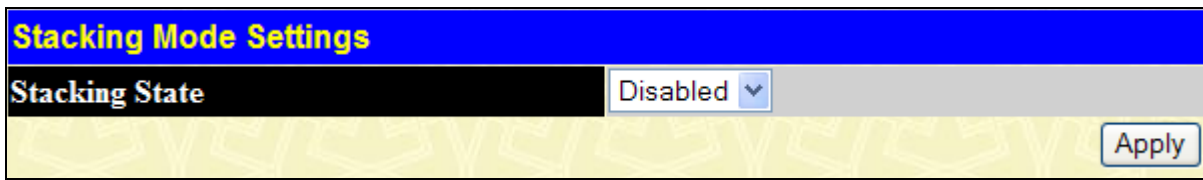


Figure 2 - 11 Stacking Mode Settings window

Use the pull-down menu, choose *Enabled* and click **Apply** to allow stacking of this Switch.

Force Master Role Settings

This window is used to ensure the master role is unchanged when adding a new device to the current stacking topology. If the state is enabled, when the device is in the election state, it still uses the original priority setting and MAC to compare device priority. After stacking is stable, the master’s priority will become zero. If stacking topology changes afterwards, the Master device will use priority zero and MAC address to determine the new primary master.

To view this window, click **Administration > Stacking > Force Master Role Settings**, as shown below.

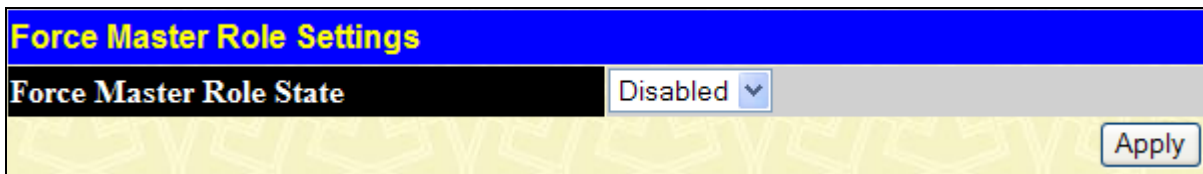


Figure 2 - 12 Force Master Role Settings window

Use the pull-down menu, choose *Enabled* and click **Apply** and the mater’s priority become zero after the stacking has stabilized.

Information configured in this window is found in the **Monitoring > Stacking Information**.

Box Information

This window is used to configure stacking parameters associated with all switches in the xStack® DGS-3400 Series. The user may configure parameters such as box ID, box priority and pre-assigning model names to switches to be entered into the switch stack.

To view this window, click **Administration > Stacking > Box Information**, as shown below.

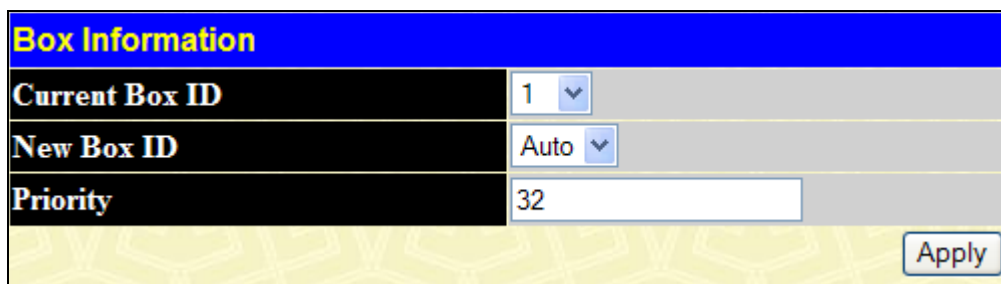


Figure 2 - 13 Box Information window

Parameter	Description
Current Box ID	The Box ID of the switch in the stack to be configured.
New Box ID	The new box ID of the selected switch in the stack that was selected in the Current Box ID field. The user may choose any number between 1 and 12 to identify the switch in the switch stack. <i>Auto</i> will automatically assign a box number to the switch in the switch stack.
Priority	Displays the priority ID of the Switch. The range is between 1 and 63. The lower the number, the

higher the priority. The box (switch) with the lowest priority number in the stack is the Primary Master switch. The Primary Master switch will be used to configure applications of the switch stack.

Information configured in this window is found in **Monitoring > Stacking Information**.



NOTE: Configured box priority settings will not be implemented until users physically save it using the Web GUI or the CLI.

Port Configuration

Port Configuration

To view this window, click **Administration > Port Configuration > Port Configuration**, as shown on the right:

To configure switch ports:

1. Choose the port or sequential range of ports using the **From/To** port pull-down menus.
2. Use the remaining pull-down menus to configure the parameters described below:

Port Configuration						
Unit	From	To	State	Flow Control	Learning	Medium Type
1	Port 1	Port 1	Enabled	Disabled	<input checked="" type="checkbox"/> Enabled	Copper
Speed/Duplex			Capability Advertised			Auto Negotiation
Auto			<input type="checkbox"/> 10 Half <input type="checkbox"/> 10 Full <input type="checkbox"/> 100 Half <input type="checkbox"/> 100 Full <input type="checkbox"/> 1000 Full			<input type="checkbox"/> Restart Auto <input type="button" value="Apply"/>
Port Auto Negotiation Information Table-Unit 1						
Port	State	Speed/Duplex	Flow Control	Connection	Learning	
1	Enabled	Auto	Disabled	Link Down	Enabled	
2	Enabled	Auto	Disabled	Link Down	Enabled	
3	Enabled	Auto	Disabled	100M/Full/None	Enabled	
4	Enabled	Auto	Disabled	Link Down	Enabled	
5	Enabled	Auto	Disabled	Link Down	Enabled	
6	Enabled	Auto	Disabled	Link Down	Enabled	
7	Enabled	Auto	Disabled	Link Down	Enabled	
8	Enabled	Auto	Disabled	Link Down	Enabled	
9	Enabled	Auto	Disabled	Link Down	Enabled	
10	Enabled	Auto	Disabled	Link Down	Enabled	
11	Enabled	Auto	Disabled	Link Down	Enabled	
12	Enabled	Auto	Disabled	Link Down	Enabled	
13	Enabled	Auto	Disabled	Link Down	Enabled	
14	Enabled	Auto	Disabled	Link Down	Enabled	
15	Enabled	Auto	Disabled	Link Down	Enabled	
16	Enabled	Auto	Disabled	Link Down	Enabled	
17	Enabled	Auto	Disabled	Link Down	Enabled	
18	Enabled	Auto	Disabled	Link Down	Enabled	
19	Enabled	Auto	Disabled	Link Down	Enabled	
20	Enabled	Auto	Disabled	Link Down	Enabled	
21 (C)	Enabled	Auto	Disabled	Link Down	Enabled	
21 (F)	Enabled	Auto	Disabled	Link Down	Enabled	
22 (C)	Enabled	Auto	Disabled	Link Down	Enabled	
22 (F)	Enabled	Auto	Disabled	Link Down	Enabled	
23 (C)	Enabled	Auto	Disabled	Link Down	Enabled	
23 (F)	Enabled	Auto	Disabled	Link Down	Enabled	
24 (C)	Enabled	Auto	Disabled	Link Down	Enabled	
24 (F)	Enabled	Auto	Disabled	Link Down	Enabled	

Figure 2 - 14 Port Configuration window

The following parameters can be configured:

Parameter	Description
Unit	Select the unit to configure.
From / To	These two fields are use to select a port or range of ports.

State	Toggle the State field to either enable or disable a given port or group of ports.
Flow Control	Displays the flow control scheme used for the various port configurations. Ports configured for full-duplex use 802.3x flow control, half-duplex ports use backpressure flow control, and Auto ports use an automatic selection of the two. The default is Disabled.
Learning	Enable or disable MAC address learning for the selected ports. When Enabled, destination and source MAC addresses are automatically listed in the forwarding table. When learning is Disabled, MAC addresses must be manually entered into the forwarding table. This is sometimes done for reasons of security or efficiency. See the section on Forwarding/Filtering for information on entering MAC addresses into the forwarding table. The default setting is Enabled.
Medium Type	If configuring the Combo ports, this defines the type of transport medium to be used, whether copper or fiber.
Speed/Duplex	<p>Use the Speed/Duplex pull-down menu to select the speed and duplex/half-duplex state of the port. <i>Auto</i> denotes auto-negotiation between 10 and 1000 Mbps devices, in full- or half-duplex. The <i>Auto</i> setting allows the port to automatically determine the fastest settings the device the port is connected to can handle, and then to use those settings. Options are <i>Auto</i>, <i>10M/Half</i>, <i>10M/Full</i>, <i>100M/Half</i>, <i>100M/Full</i>, <i>1000M/Full_Master</i> and <i>1000M/Full_Slave</i>, and <i>1000M/Full</i>. There is no automatic adjustment of port settings with any option other than <i>Auto</i>.</p> <p>The Switch allows the user to configure two types of gigabit connections; <i>1000M/Full_Master</i> and <i>1000M/Full_Slave</i>. Gigabit connections only support full duplex connections and take on certain characteristics that are different from the other choices listed.</p> <p>The <i>1000M/Full_Master</i> and <i>1000M/Full_Slave</i> parameters refer to connections running a 1000BASE-T cable for connection between the Switch port and other device capable of a gigabit connection. The master setting (<i>1000M/Full_Master</i>) will allow the port to advertise capabilities related to duplex, speed and physical layer type. The master setting will also determine the master and slave relationship between the two connected physical layers. This relationship is necessary for establishing the timing control between the two physical layers. The timing control is set on a master physical layer by a local source. The slave setting (<i>1000M/Full_Slave</i>) uses loop timing, where the timing comes from a data stream received from the master. If one connection is set for <i>1000M/Full_Master</i>, the other side of the connection must be set for <i>1000M/Full_Slave</i>. Any other configuration will result in a link down status for both ports.</p>
Capability Advertised	The speed and duplex capability are advertised during auto negotiation. If the speed of a port is set to auto, this defines the speed and duplex that the port can be supported. The partner can determine the speed and duplex according to the information.
Auto Negotiation	Tick the check box to restart auto negotiation.

Click **Apply** to implement the new settings on the Switch.

Port Error Disabled

The following window will display the information about ports that have had their connection status disabled, for reasons such as STP loopback detection or link down status.

To view this window, click **Administration > Port Configuration > Port Error Disabled**, as shown below.

Port Error Disabled Table			
Port	State	Connection	Reason
4	Enabled	Err-Disabled	STP LBD
7	Enabled	Err-Disabled	STP LBD
47	Enabled	Err-Disabled	STP LBD

Figure 2 - 15 Port Error Disabled window

The following parameters are displayed:

Parameter	Description
Port	Displays the port that has been error disabled.
State	Describes the current running state of the port, whether <i>Enabled</i> or <i>Disabled</i> .
Connection	This field will read the uplink status of the individual ports, whether <i>Enabled</i> or <i>Disabled</i> .
Reason	Describes the reason why the port has been error-disabled, such as a STP loopback occurrence.

Port Description

The Switch supports a port description feature where the user may name various ports on the Switch.

To view this window, click **Administration > Port Configuration > Port Description**, as shown on the right.

Port Description					
Unit	From	To	Medium Type	Description	Apply
1	Port 1	Port 1	Copper	<input type="text"/>	<input type="button" value="Apply"/>
Port Description Table-Unit 1					
Port	Description				
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					
19					
20					
21 (C)					
21 (F)					
22 (C)					
22 (F)					
23 (C)					
23 (F)					
24 (C)					
24 (F)					

Figure 2 - 16 Port Description window

The following parameters can be configured:

Parameter	Description
Unit	Select the unit to configure.
From / To	These two fields are use to select a port or range of ports.
Medium Type	If configuring the Combo ports, this defines the type of transport medium to be used, whether <i>Copper</i> or <i>Fiber</i> .
Description	Enter the description for the selected port(s).

Click **Apply** to set the descriptions in the Port Description Table.

Port Auto Negotiation Information

This window allows the user to view the current configurations of all the ports on the Switch. Use the drop-down menu to select which unit to view.

To view this window, click **Administration > Port Configuration > Port Auto Negotiation Information**, as shown below.

Unit 1				
Port Auto Negotiation Information Table-Unit 1				
Port	Auto Negotiation	Capability Bits	Capability Advertised Bits	Capability Received Bits
1	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
2	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
3	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full
4	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
5	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
6	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
7	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
8	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
9	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
10	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
11	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
12	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	
13	Enabled	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	10M_Half,10M_Full ,100M_Half,100M_Full ,1000M_Full	

Figure 2 - 17 Port Auto Negotiation Information Table window

Port Details

This window is used to view detailed port information for individual ports on a particular unit. Use the drop-down menus to select the specific port of the unit you wish to view and click **Find**.

To view this window, click **Administration > Port Configuration > Port Details**, as shown below.

Unit	1	Port	Port 1	Find
Port Details				
Port	1:1			
Port Status	Link Down			
Description				
Hardware Type	Gigabits Ethernet			
MAC Address	00-21-91-53-3E-C8			
Bandwidth	1000000Kbit			
Auto-Negotiation	Enabled			
Duplex Mode	Full Duplex			
Flow Control	Disabled			
MDI	Auto			
Address Learning	Enabled			
Loopback Mode	Disabled			
Last Clear of Counter	1 hours 10 mins ago			
BPDU Hardware Filtering Mode	Disabled			
Queuing Strategy				
TX Load	0/100, 0bits/sec, 0packets/sec			
RX Load	0/100, 0bits/sec, 0packets/sec			
RX Counter				
Broadcast	0			
Multicast	0			
CRC Errors	0			
Dropped Packets	0			
Undersizes	0			
Oversizes	0			
Fragments	0			
Jabber	0			
TX Counter				
Excessive Deferrals	0			
Late Collisions	0			
Excess Collision	0			
Single Collision	0			
Collision	0			

Figure 2 - 18 Port Details window

Port Media Type

This window is used to display the port media type available on each unit. To view a particular switch in the stack use the drop-down menu to select the unit.

To view this window, click **Administration > Port Configuration > Port Media Type**, as shown below.

Unit	
1	
Port Media Type	
Port	Type
1	1000Base-T
2	1000Base-T
3	1000Base-T
4	1000Base-T
5	1000Base-T
6	1000Base-T
7	1000Base-T
8	1000Base-T
9	1000Base-T
10	1000Base-T
11	1000Base-T
12	1000Base-T
13	1000Base-T
14	1000Base-T
15	1000Base-T
16	1000Base-T
17	1000Base-T
18	1000Base-T
19	1000Base-T
20	1000Base-T
21	1000Base-X
22	1000Base-X
23	1000Base-X
24	1000Base-X

Figure 2 - 19 Port Media Type window

Cable Diagnostics

This window is used to control the cable diagnostics and determine where and what kind of errors have occurred on the cable. This function is primarily used for administrators to view tests on copper cables.

To view this window, click **Administration > Port Configuration > Cable Diagnostics**, as shown below.

Unit Port

Cable Diagnostics

Unit	Port	Type	Link Status	Test Result	Cable Length(M)
<p>The cable diagnostics feature is designed primarily for administrators or customer service representatives to verify and test copper cables; it can rapidly determine the quality of the cables and the types of error.</p> <p>Note:</p> <ol style="list-style-type: none"> 1. If nothing is displayed in the Cable Length (M) column, the cable length is "Not Available". This is due to the FE port being unable to obtain cable length either because its link partner is powered-off, or the cables used are broken and/or bad in quality. 2. The maximum cable length is limited to 120 meters. 3. Deviation is +/-5 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 5 m in length. 4. The utility also measures cable fault and identifies the fault in length according to the distance from this switch. 					

Figure 2 - 20 Cable Diagnostics window

User Accounts

Use the **User Account Management** window to control user privileges, create new users and view existing User Accounts.

To view this window, click **Administration > User Accounts**, as shown below.

User Accounts		
User Name	Access Right	
RG	Admin	<input type="button" value="Add"/> <input type="button" value="Modify"/>

Figure 2 - 21 User Accounts window

To add a new user, click the **Add** button, and the window below displays:

User Account Add Table	
User Name	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
Access Right	Admin <input type="text" value="v"/>
<input type="button" value="Apply"/>	
Show All User Account Entries	

Figure 2 - 22 User Accounts - Add window

To modify or delete an existing user, click the **Modify** button for the corresponding user, and the window below displays:

Figure 2 - 23 User Accounts - Modify window

The following parameters are displayed or can be configured:

Parameter	Description
User Name	Enter a name for the account, or display the name of the selected account.
Old Password	Enter the original password of the existing account.
New Password	Enter a new password for the account.
Confirm new Password	Retype the new password to confirm.
Access Right	Use the pull-down menu to select the access right of the account or display the access right of the selected account.
Encrypt	Tick the check box and select the type of encryption (<i>Admin</i> or <i>SHA_1</i>) from the pull-down menu.
Encrypt Password	Enter the password for the type of encryption.

Click the [Show All User Account Entries](#) link to return to the User Accounts window. Click **Apply** to implement the changes. Click **Delete** in the User Account Modify Table window to remove the selected user account.

Password Encryption

Password encryption allows the user to encrypt a password for additional security.

To view this window, click **Administration > Password Encryption**, as shown below.

Figure 2 - 24 Password Encryption window

The following parameters can be configured:

Parameter	Description
Encryption State	Use the pull-down menu to enable or disable the password encryption. Select <i>Enabled</i> to change the password into encrypted form. When password encryption is <i>Disabled</i> , the password will be in plain text form. However, if the user specifies the password in encrypted

	form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in encrypted form and cannot be reverted back to plaintext form.
--	--

Click **Apply** to implement the changes.

Mirror

This section contains information for mirroring port configurations, including Port Mirror Global Settings and Port Mirror Settings.

Port Mirror Global Settings

This window is used to configure the port mirror status without having to modify the settings in Port Mirror Settings window.

To view this window, click **Administration > Mirror > Port Mirror Global Settings**, as shown below.



Figure 2 - 25 Port Mirror Global Settings window

The following parameters can be configured:

Parameter	Description
Porting Mirror Global State	Use the pull-down menu to enable or disable the port mirror status.

Click **Apply** to implement the changes.

Port Mirror Settings

The Switch supports up to four port mirror groups. It allows to copy frames transmitted and received on a port and redirect the copies to another port. You can attach a monitoring device to the mirrored port, such as a sniffer or an RMON probe, to view details about the packets passing through the first port. This is useful for network monitoring and troubleshooting purposes.

To view this window, click **Administration > Mirror > Port Mirror Settings**, as shown below.

Add

Group ID (1-4) Find

View All

Total Entries: 1

Port Mirror Settings						
Group	State	Target Port	RX Source Ports	TX Source Ports	Modify	Delete
1	Enabled				Modify	X

Figure 2 - 26 Port Mirroring window

Enter an ID in the **Group ID (1-4)** field and click **Find** to see all the entry that belongs to the group in the lower half of the window. Click **View All** to see all the entries. Click **X** to remove the corresponding entry.

To add a new mirror port, click the **Add** button, and the window below appears:

Port Mirror Settings - Add

Group ID (1-4)

Apply

[Show All Port Mirror Entries](#)

Figure 2 - 27 Port Mirroring - Add window

To modify an existing mirror port, click the **Modify** button of the corresponding entry, and the window below appears:

Port Mirror Settings - Edit

Group ID (1-4)

Target Port

State

Source Ports Action

RX Source Ports

TX Source Ports

Apply

Note(1): The "Source Port" and "Target Port" should be different, or the setup will be invalid.

Note(2): The mirror target port should not be a non-master member port of aggregation.

[Show All Port Mirror Entries](#)

Figure 2 - 28 Port Mirroring - Edit window

The following parameters are displayed or can be configured:

Parameter	Description
-----------	-------------

Group ID (1-4)	Enter or display the group ID this entry belongs to.
Target Port	Tick the check box and enter the port which received the copies from the source port.
State	Use the pull-down menu to enable or disable the mirror group function.
Source Ports Action	User the pull-down menu to add or delete the source port.
RX Source Ports	Only the received packets on the mirror group source ports will be mirrored to the mirror group target port.
TX Source Ports	Only the sent packets on the mirror group source ports will be mirrored to the mirror group target port.

Click the [Show All Port Mirror Entries](#) link to return to the Port Mirror Settings window. Click **Apply** to implement the changes.



NOTE: You cannot mirror a fast port onto a slower port. For example, if you try to mirror the traffic from a 100 Mbps port onto a 10 Mbps port, this can cause throughput problems. The port you are copying frames from should always support an equal or lower speed than the port to which you are sending the copies. Also, the target port for the mirroring cannot be a member of a trunking group. Please note a target port and a source port cannot be the same port.



NOTE: Except the master port of a trunking group, target mirror ports cannot be members of a trunking group. Attempting to do so will produce an error message and the configuration will not be set.

Mirroring within the Switch Stack

Users may configure mirroring between switches in the switch stack but certain conditions and restrictions apply.

1. When mirroring is configured in the stack, the primary master and the backup master will save and synchronize these mirroring configurations in their respective databases. Therefore, if the primary master is removed, the backup master will still hold the mirroring configurations set.
2. If the device hot-removed from the stack holds the target port for the mirroring function, the primary master will disable the mirroring function for the whole stack.
3. Stacking ports cannot be source ports or target mirror ports.

System Log

This section contains information for configuring various attributes and properties for System Log Configurations, including System Log Host, System Log Save Mode Settings, and System Log Source Interface Settings.


System Log Host

This window is used to send system log messages to up to four designated servers using the **System Log Server**.

To view this window, click **Administration > System Log > System Log Host**, as shown below.

System Log Host							
Index	Server IP	Severity	Facility	UDP Port	Status	Modify	Delete
1	10.90.90.1	Emergency(0)	Local0	514	Disabled	Modify	X

Figure 2 - 29 System Log Host window

Click  to remove the corresponding entry.

To add a new system log server, click the **Add** button, and the window below appears:

System Log Server Settings - Add	
Index (1-4)	1
Server IP	0.0.0.0
Severity	Emergency (0-7)
Facility	Local0
UDP Port (514 or 6000-65535)	514
Status	Disabled
<input type="button" value="Apply"/>	
Show All System Log Servers	

Figure 2 - 30 Configure System Log Server - Add window

To modify an existing system log server, click the **Modify** button of the corresponding entry, and the window below appears:

System Log Server Settings - Edit	
Index (1-4)	1
Server IP	10.90.90.1
Severity	Emergency (0-7)
Facility	Local0
UDP Port (514 or 6000-65535)	514
Status	Disabled
<input type="button" value="Apply"/>	
Show All System Log Servers	

Figure 2 - 31 Configure System Log Server - Edit window

The following parameters are displayed or can be configured:

Parameter	Description
Index(1-4)	System log server settings index (1-4).
Server IP	The IPv4 address of the System log server.
Severity	This drop-down menu allows you to select the level of messages that will be sent. The options

	are <i>Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug, All</i> and <i>Level</i> . The default severity is <i>Emergency</i> .																																																				
Facility	<p>Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the “local use” facilities or they may use the “user-level” Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values that the Switch currently now.</p> <table border="1"> <thead> <tr> <th>Numerical Code</th> <th>Facility</th> <th>Numerical Code</th> <th>Facility</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>kernel messages</td> <td>12</td> <td>NTP subsystem</td> </tr> <tr> <td>1</td> <td>user-level messages</td> <td>13</td> <td>log audit</td> </tr> <tr> <td>2</td> <td>mail system</td> <td>14</td> <td>log alert</td> </tr> <tr> <td>3</td> <td>system daemons</td> <td>15</td> <td>clock daemon</td> </tr> <tr> <td>4</td> <td>security/authorization messages</td> <td>16</td> <td>local use 0 (local0)</td> </tr> <tr> <td>5</td> <td>messages generated internally by syslog line printer subsystem</td> <td>17</td> <td>local use 1 (local1)</td> </tr> <tr> <td>7</td> <td>network news subsystem</td> <td>18</td> <td>local use 2 (local2)</td> </tr> <tr> <td>8</td> <td>UUCP subsystem</td> <td>19</td> <td>local use 3 (local3)</td> </tr> <tr> <td>9</td> <td>clock daemon</td> <td>20</td> <td>local use 4 (local4)</td> </tr> <tr> <td>10</td> <td>security/authorization messages</td> <td>21</td> <td>local use 5 (local5)</td> </tr> <tr> <td>11</td> <td>FTP daemon</td> <td>22</td> <td>local use 6 (local6)</td> </tr> <tr> <td></td> <td></td> <td>23</td> <td>local use 7 (local7)</td> </tr> </tbody> </table>	Numerical Code	Facility	Numerical Code	Facility	0	kernel messages	12	NTP subsystem	1	user-level messages	13	log audit	2	mail system	14	log alert	3	system daemons	15	clock daemon	4	security/authorization messages	16	local use 0 (local0)	5	messages generated internally by syslog line printer subsystem	17	local use 1 (local1)	7	network news subsystem	18	local use 2 (local2)	8	UUCP subsystem	19	local use 3 (local3)	9	clock daemon	20	local use 4 (local4)	10	security/authorization messages	21	local use 5 (local5)	11	FTP daemon	22	local use 6 (local6)			23	local use 7 (local7)
Numerical Code	Facility	Numerical Code	Facility																																																		
0	kernel messages	12	NTP subsystem																																																		
1	user-level messages	13	log audit																																																		
2	mail system	14	log alert																																																		
3	system daemons	15	clock daemon																																																		
4	security/authorization messages	16	local use 0 (local0)																																																		
5	messages generated internally by syslog line printer subsystem	17	local use 1 (local1)																																																		
7	network news subsystem	18	local use 2 (local2)																																																		
8	UUCP subsystem	19	local use 3 (local3)																																																		
9	clock daemon	20	local use 4 (local4)																																																		
10	security/authorization messages	21	local use 5 (local5)																																																		
11	FTP daemon	22	local use 6 (local6)																																																		
		23	local use 7 (local7)																																																		
UDP Port (514 or 6000-65535)	Type the UDP port number used for sending Syslog messages. The default is 514.																																																				
Status	Choose <i>Enabled</i> or <i>Disabled</i> to activate or deactivate.																																																				

To set the system log server configuration, click **Apply**. To return to the System Log Host window, click the [Show All System Log Servers](#) link.

System Log Save Mode Settings

This window may be used to choose a method for which to save the switch log to the flash memory on the Switch.

To view this window, click **Administration > System Log > System Log Save Mode Settings**, as shown below.

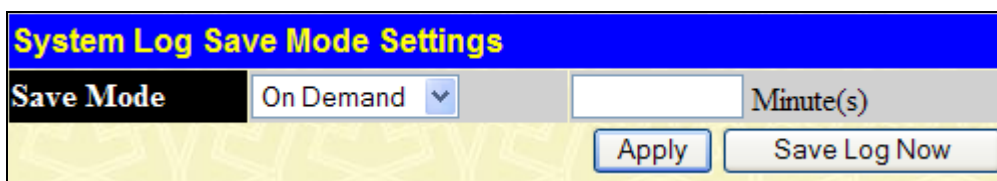


Figure 2 - 32 System Log Save Mode Settings window

The following parameters can be configured:

Parameter	Description
Save Mode	<p>Use the pull-down menu to choose the method for saving the switch log to the Flash memory. There are three options:</p> <p><i>Time Interval</i> – Configure a time interval by which the switch will save the log files.</p> <p><i>On Demand</i> – Only save log files when manually telling the Switch to do so. Go to Save Services > Save Changes to manually save log.</p> <p><i>On Trigger</i> – Save log files to the Switch every time when a log event occurs on the Switch.</p>
Minute(s)	When <i>Time Interval</i> is selected in Save Mode , set a time between 1 and 65535 minutes in the field. The default value is 1 minute.

Click **Apply** to implement the changes. Click **Save Log Now** to immediately save log files currently on the Switch.

System Log Source Interface Settings

This window may be used to choose a method for which to save the switch log to the flash memory on the Switch.

To view this window, click **Administration > System Log > System Log Source Interface Settings**, as shown below.

Syslog Source Interface Settings		
Interface Name	<input type="text"/>	
IPv4 Address	<input type="checkbox"/>	<input type="text"/>
		<input type="button" value="Apply"/>
Syslog Source Interface Table		
Interface Name	IPv4 Address	Delete

Figure 2 - 33 System Log Save Mode Settings window

The following parameters can be configured:

Parameter	Description
Interface Name	Enter the name of the interface.
IPv4 Address	Tick the check box and enter the IPv4 address.

Click **Apply** to add the entry to the Syslog Source Interface Table. Click to remove the corresponding entry.

System Severity Settings

The Switch can be configured to allow alerts be logged or sent as a trap to an SNMP agent or both. The level at which the alert triggers either a log entry or a trap message can be set as well. Use this window to set the criteria for alerts. The current settings are displayed below the System Severity Table.

To view this window, click **Administration > System Severity Settings**, as shown below.

System Severity Settings	
System Severity	Trap
Severity Level	Emergency (0-7)
<input type="button" value="Apply"/>	
System Severity Table	
System Severity Log	Information(6)
System Severity Trap	Information(6)

Figure 2 - 34 System Severity Settings window

Use the drop-down menus to configure the parameters described below.

Parameter	Description
-----------	-------------

System Severity	Choose how the alerts are used from the drop-down menu. Select <i>log</i> to send the alert of the Severity Type configured to the Switch's log for analysis. Choose <i>trap</i> to send it to an SNMP agent for analysis, or select <i>all</i> to send the chosen alert type to an SNMP agent and the Switch's log for analysis.
Severity Level	Choose what level of alert will trigger sending the log entry or trap message as defined by the Severity Name. Select <i>Emergency</i> to send only Emergency events to the Switch's log or SNMP agent. Select <i>Alert</i> to send Emergency and alert events to the Switch's log or SNMP agent. Select <i>Critical</i> to send emergency, alert and critical events to the Switch's log or SNMP agent. Select <i>Error</i> to send error, critical, alert and emergency events to the Switch's log or SNMP agent. Select <i>Warning</i> to send warning, error, critical, alert and emergency events to the Switch's log or SNMP agent. Select <i>Notice</i> to send notice, warning, error, critical, alert and emergency events to the Switch's log or SNMP agent. Select <i>Information</i> to send information, notice, warning, error, critical, alert and emergency events to the Switch's log or SNMP agent. Select <i>Debug</i> to send debug, information, notice, warning, error, critical, alert and emergency events to the Switch's log or SNMP agent.

Click **Apply** to implement the new System Severity Settings.

Command Logging Settings

This window is used to enable or disable the command logging settings.

To view this window, click **Administration > Command Logging Settings**, as shown below.

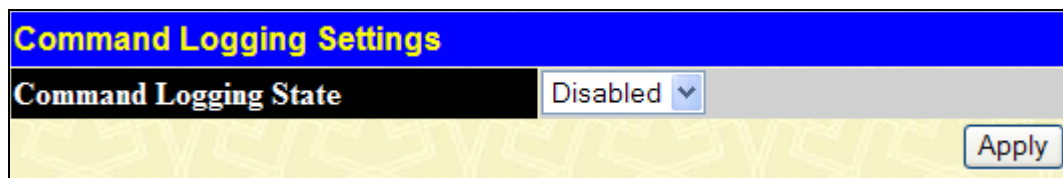


Figure 2 - 35 Command Logging Settings window



NOTE: When the switch is under the booting procedure, all configuration commands will not be logged. When the user uses AAA authentication to logged in, the user name should not be changed if the user has used the Enable Admin function to replace its privilege.

SNTP Settings

Time Settings

This window is used to configure the time settings for the Switch.

To view this window, click **Administration > SNTP Settings > Time Settings**, as shown below.

Time Settings-Current Time	
System Boot Time	7 Apr 2010 13:40:06
Current Time	7 Apr 2010 16:26:10
Time Source	System Clock
SNTP Settings	
SNTP State	Disabled <input type="button" value="v"/>
SNTP Primary Server	0.0.0.0 <input type="text"/>
SNTP Secondary Server	0.0.0.0 <input type="text"/>
SNTP Poll Interval in Seconds (30-99999)	720 <input type="text"/>
<input type="button" value="Apply"/>	
Time Settings - Set Current Time	
Year	2002 <input type="button" value="v"/>
Month	January <input type="button" value="v"/>
Day	01 <input type="button" value="v"/>
Time in HH MM SS	00 <input type="button" value="v"/> 00 <input type="button" value="v"/> 00 <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 2 - 36 Time Settings window

The following parameters are displayed or can be configured:

Parameter	Description
Time Settings - Current Time	
System Boot Time	Displays the time when the Switch was initially started for this session.
Current Time	Displays the Current Time.
Time Source	Displays the time source for the system.
SNTP Settings	
SNTP State	Use this pull-down menu to <i>Enabled</i> or <i>Disabled</i> SNTP.
SNTP Primary Server	The IP address of the primary server from which the SNTP information will be taken.
SNTP Secondary Server	The IP address of the secondary server from which the SNTP information will be taken.
SNTP Poll Interval in Seconds (30-99999)	The interval, in seconds, between requests for updated SNTP information.
Time Settings - Set Current Time	
Year	Enter the current year, to update the system clock.
Month	Enter the current month, to update the system clock.
Day	Enter the current day, to update the system clock.
Time in HH MM SS	Enter the current time in hours, minutes, and seconds.

Click **Apply** to implement your changes.

Time Zone and DST

The following window is used to configure time zone and daylight savings time settings for SNTP.

To view this window, click **Administration > SNMP Settings > Time Zone and DST**, as shown below.

Time Zone and DST

Daylight Saving Time State: Disabled

Daylight Saving Time Offset in Minutes: 60

Time Zone Offset: From GMT in +/-HH:MM: + 00 00

DST Repeating Settings

From: Which Week: First

From: Day of Week: Sunday

From: Month: April

From: Time in HH MM: 00 00

To: Which Week: Last

To: Day of Week: Sunday

To: Month: October

To: Time in HH MM: 00 00

DST Annual Settings

From: Month: April

From: Day: 29

From: Time in HH MM: 00 00

To: Month: October

To: Day: 12

To: Time in HH MM: 00 00

Apply

Figure 2 - 37 Time Zone and DST Settings window

The following parameters can be set:

Parameter	Description
Time Zone and DST	
Daylight Saving Time State	Use this pull-down menu to enable or disable the DST Settings.
Daylight Saving Time Offset in Minutes	Use this pull-down menu to specify the amount of time that will constitute your local DST offset - 30, 60, 90, or 120 minutes.
Time Zone Offset from GMT in +/- HH:MM	Use these pull-down menus to specify your local time zone's offset from Greenwich Mean Time (GMT.)
DST Repeating Settings - Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October.	
From: Which Day	Enter the week of the month that DST will start on.
From: Day of Week	Enter the day of the week that DST will start on.

From: Month	Enter the month DST will start on.
From: Time in HH:MM	Enter the time of day that DST will start on.
To: Which Day	Enter the week of the month the DST will end.
To: Day of Week	Enter the day of the week that DST will end.
To: Month	Enter the month that DST will end.
To: Time in HH:MM	Enter the time DST will end.
DST Annual Settings - Using annual mode will enable DST seasonal time adjustment. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14.	
From: Month	Enter the month DST will start on, each year.
From: Day	Enter the day of the month DST will start on, each year.
From: Time in HH:MM	Enter the time of day DST will start on, each year.
To: Month	Enter the month DST will end on, each year.
To: Day	Enter the day of the month DST will end on, each year.
To: Time in HH:MM	Enter the time of day that DST will end on, each year.

Click **Apply** to implement changes to the Time Zone and DST window.

MAC Notification Settings

MAC Notification is used to monitor MAC addresses learned and entered into the forwarding database.

To view this window, click **Administration** > **MAC Notification Settings**, as shown on the right.

Global Settings

The following parameters may be viewed and modified:

Parameter	Description
State	Enable or disable MAC notification globally on the Switch
Interval (1-2147483647 sec)	The time in seconds between notifications.
History size (1-500)	The maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

Port Settings

To change MAC notification settings for a port or group of ports on the Switch, configure the following parameters.

Parameter	Description
Unit	Choose the switch in the switch stack for which to configure these settings.
From / To	Select a port or group of ports to enable for MAC notification using the pull-down menus.
State	Enable or disable MAC Notification for the ports selected using the pull-down menu.

Click **Apply** to implement the changes.

New MAC Notification Global Settings

State: Disabled

Interval (1-2147483647 sec): 1

History Size (1-500): 1

Apply

MAC Notification Port Settings

Unit	From	To	State	Apply
1	Port 1	Port 1	Disabled	Apply

Apply

MAC Notification Port State Table-Unit 1

Port	State
1	Disabled
2	Disabled
3	Disabled
4	Disabled
5	Disabled
6	Disabled
7	Disabled
8	Disabled
9	Disabled
10	Disabled
11	Disabled
12	Disabled
13	Disabled
14	Disabled
15	Disabled
16	Disabled
17	Disabled
18	Disabled
19	Disabled
20	Disabled
21	Disabled
22	Disabled
23	Disabled
24	Disabled

Figure 2 - 38 New MAC Notification Global Settings window

TFTP Services

Trivial File Transfer Protocol (TFTP) services allow the Switch's firmware to be upgraded by transferring a new firmware file from a TFTP server to the Switch. A configuration file can also be downloaded into the Switch from a TFTP server. Switch configuration settings can be saved and a history and attack log can be uploaded from the Switch to the TFTP server. The Switch

supports dual image storage for configuration and firmware. The firmware and configuration images are indexed by ID number 1 or 2. To change the boot firmware image, use the **Config Firmware Image** window (**Administration > Multiple Image Services > Config Firmware Image**). The default Switch settings will use Image ID 1 as the boot configuration or firmware.

To view this window, click **Administration > TFTP Services**, as shown below.

Figure 2 - 39 TFTP Services window

The following parameters can be set:

Parameter	Description
Active	Select a service for the TFTP server to perform from the drop down window: <i>Download Firmware</i> – Enter the IP address of the TFTP server and specify the path and filename of the new firmware on the TFTP server. <i>Download Configuration</i> – Enter the IP address of the TFTP server, and the path and filename for the Configuration file on the TFTP server. <i>Upload Configuration</i> – Enter the IP address of the TFTP server and the path and filename for the switch settings on the TFTP server. <i>Upload Log</i> – Enter the IP address of the TFTP server and the path and filename for the history log on the TFTP server. <i>Upload Attack Log</i> – Enter the IP address of the TFTP server and the path and filename for the attack log on the TFTP server.
Unit	Select the switch in the switch stack from which, or to which to upload or download files. Tick the ALL check box to denote all switches in the switch stack.
Image ID	For firmware downloads, select the Image ID of the firmware. The Switch can hold two firmware images in its memory. <i>Image ID 1</i> will always be the boot up firmware for the Switch unless specified by the user. Choosing <i>Active</i> will download the firmware to the Boot Up Image ID, depending on the user’s configuration. Information on configuring Image IDs can be found in this section, under the heading Multiple Image Services .
Configuration ID	When downloading the configuration, select the ID of the configuration. The Switch can hold two configuration images in its memory. <i>Image ID 1</i> will always be the boot up configuration for the Switch unless specified by the user. Choosing <i>Active</i> will download the configuration to the Boot Up Image ID, depending on the user’s configuration. Information on configuring Image IDs can be found in this section, under the heading Multiple Image Services . For configuration uploads, select the Image ID of the configuration. Choosing <i>Active</i> will upload the Boot Up Image ID configuration to the TFTP server. And user can upload configuration of Image 1 or 2 by choosing Image ID.

Server IPv4 Address	Enter the IPv4 address of the server from which to download firmware and configuration or upload configuration and log.
Server IPv6 Address	Enter the IPv6 address of the server from which to download firmware and configuration or upload configuration and log. The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For Global IPv6 addresses, this field may be omitted.
Domain Name	Click the radio button and enter the domain name of TFTP Server.
File Name	Enter the path and filename of the firmware or configuration file to upload or download. The file to be uploaded or downloaded must have the same path with the TFTP server.
Filter	This is used to filter the configuration data that relates to upload configuration.

Click **Start** to record the IP address of the TFTP server and to initiate the file transfer.

Multiple Image Services

The **Multiple Image Services** folder allows users of the Switch to configure and view information regarding firmware located on the Switch. The Switch allows two firmware images to be stored in its memory and either can be configured to be the boot up firmware for the Switch. For information regarding firmware images located on the Switch, click the **Firmware Information** link. The default setting will have the boot up firmware stored as Image 1, but the user may set either stored firmware to be the boot up firmware by using the **Config Firmware Image** window.

Firmware Information

The following window allows the user to view information about current firmware images stored on the Switch.

To view this window, click **Administration > Multiple Image Services > Firmware Information**, as shown below.

Firmware Information						
Box	ID	Version	Size	Update Time	From	User
1	1	*2.70.B43	4019934	2010/03/11 13:55:57	10.90.90.10(R)	
1	2	(empty)				

*' means boot up firmware
(R) means firmware update through Serial Port (RS232)
(T) means firmware update through Telnet
(S) means firmware update through SNMP
(W) means firmware update through Web
(SIM) means firmware update through Single IP Management

Figure 2 - 40 Firmware Information window

The following parameters are displayed:

Parameter	Description
ID	States the image ID number of the firmware in the Switch's memory. The Switch can store 2

	firmware images for use. Image ID 1 will be the default boot up firmware for the Switch unless otherwise configured by the user.
Version	States the firmware version.
Size	States the size of the corresponding firmware, in bytes.
Update Time	States the specific time the firmware version was downloaded to the Switch.
From	States the IP address of the origin of the firmware. There are five ways firmware may be downloaded to the Switch. Boot Up files are denoted by an asterisk (*) next to the file. R – If the IP address has this letter attached to it, it denotes a firmware upgrade through the Console Serial Port (RS-232). T – If the IP address has this letter attached to it, it denotes a firmware upgrade through Telnet. S – If the IP address has this letter attached to it, it denotes a firmware upgrade through the Simple Network Management Protocol (SNMP). W – If the IP address has this letter attached to it, it denotes a firmware upgrade through the web-based management interface. SIM – If the IP address has this letter attached to it, it denotes a firmware upgrade through the Single IP Management feature.
User	States the user who downloaded the firmware. This field may read “Anonymous” or “Unknown” for users that are not identified.

Config Firmware Image

The following window is used to configure firmware set in the Switch.

To view this window, click **Administration > Multiple Image Services > Config Firmware Image**, as shown below.

Figure 2 - 41 Config Firmware Image window

The following parameters can be set:

Parameter	Description
Image	The Switch allows two firmware images to be stored in its memory and either can be configured to be the boot up firmware for the Switch. Use the pull-down menu to choose the image.
Unit	Select the switch in the switch stack from which, or to which to upload or download files. Tick the ALL check box to denote all switches in the switch stack.
Action	Use the pull-down menu to toggle the actions between <i>Delete</i> and <i>Boot</i> .

To boot up a firmware image, select it from the Image pull-down menu, change the Action to *Boot* and click **Apply**. To delete a firmware image, select it from the Image pull-down menu, change the Action field to *Delete* and click **Apply**.

RCP

RCP (Remote Copy Protocol) is a UNIX Remote Shell service which allows files to be copied between a server and client. RCP is an application that operates above the TCP protocols, and uses port number 514 as the TCP destination port.

The RCP application uses client server architecture and the client can be any machine running the RCP client application.

A Switch that supports the RCP client allows users to copy firmware images, configurations and log files between the Switch and RCP Server.

Switches that do not support a file system should still be able to run an RCP client to copy firmware images, configurations and logs between the switch and RCP server.

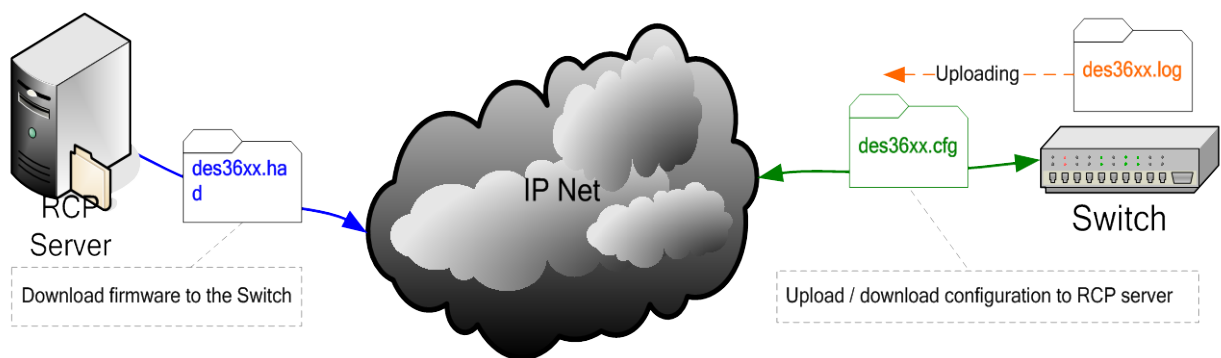


Figure 2 - 42 Remote Copy Protocol between an RCP server and an Ethernet Switch

As illustrated in Figure 2 - 49, a user can:

- a) Upload a configuration file from the Switch to the RCP Server.
- b) Download a firmware file from the RCP Server to the Switch.
- c) Upload the Log file from the Switch to the RCP Server.
- d) Download the configuration file from the RCP Server to the Switch.

RCP Server Settings

This window is used to configure the global RCP server information. The global RCP Server setting can be used when the Server or remote user name is not specified. ONLY one RCP server can be configured.

To view this window, click **Administration > RCP > RCP Server Settings**, as shown below.

Figure 2 - 43 RCP Server Settings window

The following parameters can be configured:

Parameter	Description
Action	Toggle the action between <i>Add</i> and <i>Clear</i> .
Type	Select to enter the information in IP Address and/or User Name fields. Available options are <i>IP Address</i> , <i>User Name</i> and <i>Both</i> .
IP Address	Enter the IP address of the global RCP server.
User Name	Enter the remote user name.

Click **Apply** to implement the changes.

RCP Services

This window is use to configure the services that provided by the RCP server.

To view this window, click **Administration > RCP > RCP Services**, as shown below.

Figure 2 - 44 RCP Server Settings window

The following parameters can be configured:

Parameter	Description
Operation	Use the pull-down menu to select the method for copying files. Options are <i>Download Firmware</i> ,

	<i>Download Configuration, Upload Configuration, Upload Log, and Upload Attack Log.</i>
RCP Server IPv4 Address	Enter the IP address of the RCP Server.
User Name	Enter the remote user name on the RCP server.
Local File Name	Enter the file name in the field. Tick the Increment , and the existing configuration will not be cleared before applying the new configuration.
Unit Number	Select the switch in the switch stack from which, or to which to upload or download files. Tick the ALL check box to denote all switches in the switch stack.
Image ID	Use the pull-down menu to select the Image file ID.
Configuration ID	Use the pull-down menu to select the configuration file ID.
Filter	This is used to filter the configuration data that relates to upload configuration.

Click **Apply** to implement the changes.

Ping Test

Ping is a small program that sends ICMP Echo packets to the IP address you specify. The destination node then responds to or “echoes” the packets sent from the Switch. This is very useful to verify connectivity between the Switch and other nodes on the network.

IPv4 Ping Test

The following window is used to Ping an IPv4 address.

To view this window, click **Administration > Ping Test > IPv4 Ping Test** as shown below.

Figure 2 - 45 IPv4 Ping Test window

The following parameters can be configured:

Parameter	Description
-----------	-------------

Target IP Address	Click the radio button and enter the Target IP Address to be pinged.
Domain Name	Click the radio button and enter the domain name of the host.
Repeat Times	The user may use the Infinite times radio button, in the Repeat Pinging for field, which will tell the ping program to keep sending ICMP Echo packets to the specified IP address until the program is stopped. The user may opt to choose a specific number of times to ping the Target IP Address by clicking its radio button and entering a number between 1 and 255.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination.
Source IP Address	Tick the check box and enter the source IP address of the ping packets.

Click **Start** to initiate the Ping program.

IPv6 Ping Test

The following window is used to Ping an IPv6 address.

To view this window, click **Administration > Ping Test > IPv6 Ping Test**, as shown below.

Figure 2 - 46 IPv6 Ping Test window

This window allows the following parameters to be configured to ping an IPv6 address.

Parameter	Description
Target IPv6 Address	Enter an IPv6 address to be pinged.
Interface	The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. For Global IPv6 addresses, this field may be omitted.

Repeat Times	Enter the number of times desired to attempt to ping the IPv6 address configured in this window. Users may enter a number of times between 1 and 255.
Size	Use this field to set the datagram size of the packet, or in essence, the number of bytes in each ping packet. Users may set a size between 1 and 6000 bytes with a default setting of 100 bytes.
Timeout	Select a timeout period between 1 and 99 seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.
Source IPv6 Address	Tick the check box and enter the source IPv6 address of the ping packets.

Click **Start** to initialize the Ping program.

IPv6 Neighbor

IPv6 neighbors are devices on the link-local network that have been detected as being IPv6 devices. These devices can forward packets and keep track of the reachability of routers, as well as if changes occur within link-layer addresses of nodes on the network or if identical unicast addresses are present on the local link. The following two windows are used to view IPv6 neighbors, and add or delete them from the Neighbor cache.

IPv6 Neighbor Settings

The following window is used to view, configure and delete current IPv6 neighbors of the Switch.


To view this window, click **Administration > IPv6 Neighbor > IPv6 Neighbor Settings**, as shown below.

Figure 2 - 47 IPv6 Neighbor Settings window

The following fields can be configured or viewed:

Parameter	Description
Interface Name	Enter the interface name of the IPv6 neighbor you wish to find.
Neighbor IPv6 Address	Enter the neighbor IPv6 address of the entry you wish to find.
State	To find specific entries, tick the check box and select either Static or Dynamic . <i>Static</i> – Select Static to view all statically entered IPv6 neighbors on the Switch. <i>Dynamic</i> – Select Dynamic to view all dynamically configured neighbor devices which are IPv6 neighbors of the IP interface previously created.
IPv6 Neighbor Settings	
Neighbor IPv6 Address	Display the IPv6 address of the neighbor device.

State	Display the running state of the corresponding IPv6 neighbor. The user may see six possible entries in this field, which are Incomplete, Stale, Probe, Reachable, Delay or Static.
Link Layer MAC Address	Display the MAC address of the corresponding IPv6 device.
Port	Display the port for IPv6 neighbor settings.
Interface	Display the Interface name associated with this IPv6 address.
VID	Display which VLAN learned the IPv6 address of the neighbor device.

To search for an entry, enter the appropriate information and click **Find**. To add a new entry click **Add**, the following window will be displayed. To remove an entry, click the corresponding  button. To completely clear the IPv6 Neighbor Settings, click the **Clear All** button. To add a new entry, click the **Add** button, revealing the following window to configure:

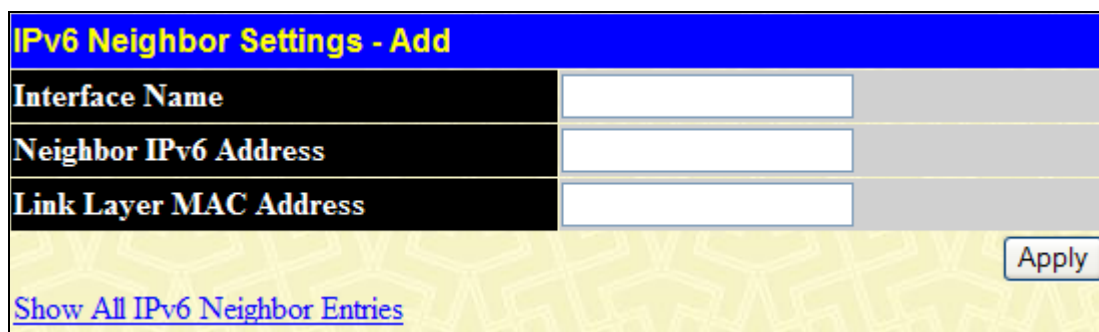


Figure 2 - 48 IPv6 Neighbor Settings – Add window

The following fields can be set or viewed:

Parameter	Description
Interface Name	Enter the name of the Interface associated with this entry.
Neighbor IPv6 Address	The IPv6 address of the neighbor entry. Specify the address using the hexadecimal IPv6 Address (IPv6 Address is hexadecimal number, for example 1234::5D7F).
Link Layer MAC Address	The MAC address of the IPv6 neighbor entry.

After entering the appropriate information, click **Apply** to implement the changes. To return to the IPv6 Neighbor window, click the [Show All IPv6 Neighbor Entries](#) link.

Route Redistribution Settings

Route redistribution allows routers on the network, which are running different routing protocols to exchange routing information. This is accomplished by comparing the routes stored in the various routers' routing tables and assigning appropriate metrics. This information is then exchanged among the various routers according to the individual router's current routing protocol.


To view this window, click **Administration > Route Redistribution Settings**, as shown below.

Route Redistribution Settings				
Dst. Protocol	Src. Protocol	Action	Metric (0-16)	
RIP	Static	Add	<input type="text"/>	
				Apply
Route Redistribution Table				
Src. Protocol	Dst. Protocol	Type	Metric	Delete

Figure 2 - 49 Route Redistribution Settings window

The following fields can be configured:

Parameter	Description
Dst. Protocol	Use the pull-down menu to select the target protocol.
Src. Protocol	Use the pull-down menu to select the source protocol.
Action	Add or Edit the entry.
Metric (0-16)	Enter the RIP route metric value for the redistributed routes. The valid value is 0 to 16. The default value is 0.

Click **Apply** to implement the changes. To remove an entry, click the corresponding  button.

Static/Default Route Settings

The Switch supports only static routing for IPv4 and IPv6 formatted addressing. Users can create up to 128 static route entries for IPv4 and IPv6 combined. Manually configured static routes can route IP packets, and the local route also can route IP packets. For each device that is a part of the DGS-3400 network, users may only configure one IP address as a static route.

For IPv4 static routes, once a static route has been set, the Switch will send an ARP request packet to the next hop router that has been set by the user. Once an ARP response has been retrieved by the switch from that next hop, the route becomes enabled. If a response is not received from the next hop device after three ARP requests have been sent, the configured static route will remain in a link-down status.

The Switch also supports a floating static route, which means that the user may create an alternative static route to a different next hop device located in the other network. This secondary next hop device route is considered as a backup static route for when the primary static route is down. If the primary route is lost, the backup route will uplink and its status will become Active.

IPv4 Static/Default Route Settings

Entries into the Switch's forwarding table can be made using both MAC addresses and IP addresses. Static IP forwarding is accomplished by the entry of an IP address into the Switch's Static IP Routing Table.

To view this window, click **Administration > Static/Default Route Settings > IPv4 Static/Default Route Settings**, as shown below.

Figure 2 - 50 IPv4 Static/Default Route Settings window

This window shows the following values:

Parameter	Description
IP Address	The IPv4 address of the Static/Default Route.
Subnet Mask	The corresponding Subnet Mask of the IP address entered into the table.
Gateway	The corresponding Gateway of the IP route entered into the table.
Metric	Represents the metric value of the IP route entered into the table. This field may read a number between 1 and 65535.
Protocol	Represents the protocol used for the Routing Table entry of the IP route.
Backup	Represents the Backup state for which this IP route is configured. This field may read Primary or Backup.
Status	Displays whether the entry is <i>Active</i> or <i>Inactive</i> .


To remove an entry, click the corresponding  button. To add a new entry, click the **Add** button, revealing the following window to configure:

Figure 2 - 51 Static/Default Route Settings - Add window

The following fields can be set:

Parameter	Description
IP Address	Allows the entry of an IP address that will be a static entry into the Switch's Routing Table.
Subnet Mask	Allows the entry of a subnet mask corresponding to the IP address above.
Gateway	Allows the entry of an IP address of a gateway for the IP route above.
Metric (1-65535)	Allows the entry of a routing protocol metric representing the number of routers between the Switch and the IP address above.
Backup State	The user may choose between <i>Primary</i> and <i>Backup</i> . If the Primary Static/Default Route fails, the Backup Route will support the entry. Please take note that the Primary and

Backup entries cannot have the same Gateway.

Click **Apply** to implement the changes. To return to the IPv4 Static/Default Route Settings window, click the [Show All Static/Default Route Entries](#) link.

IPv6 Static/Default Route Settings

A static entry of an IPv6 address can be entered into the Switch's routing table for IPv6 formatted addresses.

To view this window, click **Administration > Static/Default Route Settings > IPv6 Static/Default Route Settings**, as shown below.

IPv6 Address/PrefixLen	Interface	Next Hop Address	Metric	Protocol	Backup	Status	Delete
Total Entries: 0							

Figure 2 - 52 IPv6 Static/Default Route Settings window

This window shows the following values:

Parameter	Description
IPv6 Address/PrefixLen	The IPv6 address and corresponding Prefix Length of the IPv6 static route entry.
Interface	The IP Interface where the static IPv6 route is created.
Next Hop Address	The corresponding IPv6 address for the next hop Gateway address in IPv6 format.
Metric (1-65535)	The metric of the IPv6 interface entered into the table representing the number of routers between the Switch and the IPv6 address above. Metric values allowed are between 1 and 65535.
Protocol	Represents the status for the IPv6 routing table entry.
Status	Displays whether the entry is <i>Active</i> or <i>Inactive</i> .

To remove an entry, click the corresponding button. To add a new entry, click the **Add** button, revealing the following window to configure:

Figure 2 - 53 IPv6 Static Route Settings – Add window

The following fields can be set:

Parameter	Description
IPv6 Address/Prefix Length	Specify the address and mask information using the format as IPv6 address / prefix length (IPv6 address is hexadecimal number, prefix length is decimal number, for example 1234::5D7F/32). Clicking the default check box will set the IPv6 address as unspecified and the Switch will automatically find the default route. This defines the entry as a 1 hop IPv6 default route.
IP Tunnel Name	The tunnel name of the next hop. When enter a name in this field, it indicates that the route to be deleted is an IP tunnel route.
Interface Name	The IP Interface where the static IPv6 route is to be created.
Next Hop Address	Enter the IPv6 address for the next hop Gateway address in IPv6 format.
Metric (1-65535)	The metric representing the number of routers between the Switch and the IPv6 address above.
Backup State	Use the drop-down menu to select between <i>Primary</i> and <i>Backup</i> . If the Primary Static/Default Route fails, the Backup Route will support the entry. The Primary and Backup entries cannot have the same Gateway.

Click **Apply** to implement the changes. To return to the IPv6 Static/Default Route Settings window, click the [Show All IPv6 Static/Default Route Entries](#) link.

Route Preference Settings

To view this window, click **Administration > Route Preference Settings**, as shown below.

Route Preference Settings	
RIP (1-999)	100
Static (1-999)	60
Default (1-999)	1
Local	0
Apply	

Figure 2 - 54 Route Preference Settings window

The following fields can be configured:

Parameter	Description
RIP (1-999)	Enter a value between 1 and 999 to set the route preference for RIP. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 100.
Static (1-999)	Enter a value between 1 and 999 to set the route preference for Static. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 60.
Default (1-999)	Enter a value between 1 and 999 to set the route preference for Default. The lower the value, the higher the chance the specified protocol will be chosen as the best path for routing packets. The default value is 1.

Click **Apply** to implement the changes.

Gratuitous ARP Settings

An ARP announcement (also known as Gratuitous ARP) is a packet (usually an ARP Request) containing a valid SHA and SPA for the host which sent it, with TPA equal to SPA. Such a request is not intended to solicit a reply, but merely updates the ARP caches of other hosts which receive the packet.

This is commonly done by many operating systems on startup, and helps to resolve problems which would otherwise occur if, for example, a network card had recently been changed (changing the IP address to MAC address mapping) and other hosts still had the old mapping in their ARP cache

To view this window, click **Administration > Gratuitous ARP Settings**, as shown below.

Gratuitous ARP Settings				
Send on IPIF status up	Disabled			
Send on Duplicate_IP_Detected	Disabled			
Gratuitous ARP Learning	Disabled			
Apply				
Gratuitous ARP Table				
IP Interface Name	Gratuitous ARP Trap	Gratuitous ARP Log	Gratuitous ARP Periodical Send Interval	Modify
System	Disabled	Disabled	0	Modify

Figure 2 - 55 Gratuitous ARP Settings window

The following fields can be set or viewed:

Parameter	Description
Send on IPIF status up	This is used to enable/disable the sending of gratuitous ARP request packets while an IPIF interface comes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is <i>Disabled</i> , and only one ARP packet will be broadcast.
Send on Duplicate_IP_Detected	This is used to enable/disable the sending of gratuitous ARP request packets while a duplicate IP is detected. By default, the state is <i>Disabled</i> . Duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address.
Gratuitous ARP Learning	This is used to enable/disable updating ARP cache based on the received gratuitous ARP packet. If a switch receives a gratuitous ARP packet, it should add or update the ARP entry. This is <i>Disabled</i> by default.

Once you have made the desired gratuitous ARP setting changes, click **Apply**.

To modify a current entry, click the corresponding **Modify** button, which will reveal the following window to be configured:

Gratuitous ARP Table - Edit	
IP Interface Name	System
Gratuitous ARP Trap	Disabled
Gratuitous ARP Log	Disabled
Gratuitous ARP Periodical Send Interval	0
Apply	
Show All Gratuitous ARP Entries	

Figure 2 - 56 Gratuitous ARP Table - Edit window

The following fields can be set or viewed:

Parameter	Description
IP Interface Name	Displays the name of the interface that is being edited.
Gratuitous ARP Trap & Log	The switch can trap and log IP conflict events to inform the administrator. By default, trap is Disabled and event log is also disabled.
Gratuitous ARP Periodical Send Interval	This is used to configure the interval for the periodical sending of gratuitous ARP request packets. By default, the interval is 0.

Click **Apply** to implement the changes. To return to the Gratuitous ARP Settings window, click the [Show All Gratuitous ARP Entries](#) link.

Static ARP Settings

Address Resolution Protocol (ARP) is a TCP/IP protocol that converts IP addresses into physical addresses. This table allows network managers to view, define, modify and delete ARP information for specific devices.

Static entries can be defined in the **ARP Table**. When static entries are defined, a permanent entry is entered and is used to translate IP address to MAC addresses.

To view this window, click **Administration > Static ARP Settings**, as shown below.

Interface Name	IP Address	MAC Address	Type	Modify	Delete
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local	Modify	X
System	10.90.90.90	00-21-91-53-3E-C8	Local	Modify	X
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local	Modify	X

Figure 2 - 57 Static ARP Settings window

To completely clear the Static ARP Settings, click the **Clear All** button. To add a new entry, click the **Add** button, revealing the following window to configure:

Static ARP Settings - Add	
IP Address	0.0.0.0
MAC Address	00-00-00-00-00-00
Apply	
Show All Static ARP Entries	

Figure 2 - 58 Static ARP Settings - Add window

To modify a current entry, click the corresponding **Modify** button of the entry to be modified, revealing the following window to configure:

Figure 2 - 59 Static ARP Settings - Edit window

The following fields can be set or viewed:

Parameter	Description
IP Address	The IP address of the ARP entry. This field cannot be edited in the Static ARP Settings – Edit window.
MAC Address	The MAC address of the ARP entry.

After entering the IP Address and MAC Address of the Static ARP entry, click **Apply** to implement the new entry. To return to the Static ARP Settings window, click the [Show All Static ARP Entries](#) link.

DHCP Auto Configuration Settings

This window is used to enable the DHCP auto-configuration feature on the Switch. When enabled, the Switch is instructed to receive a configuration file from a TFTP server, which will set the Switch to become a DHCP client automatically on boot up. To employ this method, the DHCP server must be set up to deliver the TFTP server IP address and configuration file name information in the DHCP reply packet. The TFTP server must be up and running and hold the necessary configuration file stored in its base directory when the request is received from the Switch. For more information about loading a configuration file for use by a client, see the DHCP server and/or TFTP server software instructions. The user may also consult the Upload screen description located in the Maintenance section of this manual.

If the Switch is unable to complete the DHCP auto configuration, the previously saved configuration file present in the Switch's memory will be used.

To view this window, click **Administration > DHCP Auto Configuration Settings** as shown below.

Figure 2 - 60 DHCP Auto Configuration Settings window

To enable the DHCP Auto Configuration State, use the pull-down menu to choose *Enabled* and click the **Apply** button.

DHCP/BOOTP Relay

The relay hops count limit allows the maximum number of hops (routers) that the DHCP/BOOTP messages can be relayed through to be set. If a packet's hop count is more than the hop count limit, the packet is dropped. The range is between 1 and 16 hops, with a default value of 4. The relay time threshold sets the minimum time (in seconds) that the Switch will wait before forwarding a BOOTP REQUEST packet. If the value in the seconds field of the packet is less than the relay time threshold, the packet will be dropped. The range is between 0 and 65,536 seconds, with a default value of 0 seconds.

DHCP / BOOTP Relay Global Settings

To view this window, click **Administration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Global Settings** as shown below.

DHCP/BOOTP Relay Global Settings	
DHCP/BOOTP Relay State	Disabled ▾
DHCP/BOOTP Relay Hops Count Limit (1-16)	4
DHCP/BOOTP Relay Time Threshold (0-65535)	0 sec
DHCP Vendor Class Identifier Option 60 State	Disabled ▾
DHCP Client Identifier Option 61 State	Disabled ▾
DHCP Relay Agent Information Option 82 State	Disabled ▾
DHCP Relay Agent Information Option 82 Check	Disabled ▾
DHCP Relay Agent Information Option 82 Policy	Replace ▾
<input type="button" value="Apply"/>	

Figure 2 - 61 DHCP/ BOOTP Relay Global Settings window

The following fields can be set:

Parameter	Description
DHCP/BOOTP Relay State	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCP/BOOTP Relay service on the Switch. The default is <i>Disabled</i> .
DHCP/BOOTP Relay Hops Count Limit (1-16)	This field allows an entry between 1 and 16 to define the maximum number of router hops DHCP/BOOTP messages can be forwarded across. The default hop count is 4.
DHCP/BOOTP Relay Time Threshold (0-65535)	Allows an entry between 0 and 65535 seconds, and defines the maximum time limit for routing a DHCP/BOOTP packet. If a value of 0 is entered, the Switch will not process the value in the seconds field of the BOOTP or DHCP packet. If a non-zero value is entered, the Switch will use that value, along with the hop count to determine whether to forward a given BOOTP or DHCP packet.
DHCP Vendor Class Identifier Option 60 State	This function <i>Enables</i> or <i>Disables</i> the DHCP Vendor class identifier option 60 state. When option 60 is enabled, if the packet does not have option 60, then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 60 or per IPIF configured servers. If the relay servers are determined based on option 60, then the IPIF configured servers will be ignored. If the relay servers are not determined by option 60 then the IPIF configured servers will be used to determine the relay servers.
DHCP Client Identifier Option 61 State	This function <i>Enables</i> or <i>Disables</i> the DHCP Client identifier option 61 state. When option 61 State is enabled, if the packet does not have option 61, then the relay servers cannot be determined based on option 61. The relay servers will be determined based on option 61 and the IPIF configured servers will be ignored. If the relay servers are not determined either by option 60 or option 61, then IPIF configured servers will be used to determine the relay servers.
DHCP Relay Agent Information Option 82 State	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCP Agent Information Option 82 on the Switch. The default is <i>Disabled</i>.</p> <p><i>Enabled</i> –When this field is toggled to <i>Enabled</i> the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can</p>

	<p>implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request.</p> <p><i>Disabled-</i> If the field is toggled to <i>Disabled</i> the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.</p>
<p>DHCP Relay Agent Information Option 82 Check</p>	<p>This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the Switches ability to check the validity of the packet's option 82 field.</p> <p><i>Enabled</i> – When the field is toggled to <i>Enable</i>, the relay agent will check the validity of the packet's option 82 field. If the switch receives a packet that contains the option-82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages.</p> <p><i>Disabled</i> – When the field is toggled to <i>Disabled</i>, the relay agent will not check the validity of the packet's option 82 field.</p>
<p>DHCP Relay Agent Information Option 82 Policy</p>	<p>This field can be toggled between <i>Replace</i>, <i>Drop</i>, and <i>Keep</i> by using the pull-down menu. It is used to set the Switches policy for handling packets when the DHCP Relay Agent Information Option 82 Check is set to <i>Disabled</i>. The default is <i>Replace</i>.</p> <p><i>Replace</i> – The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>Drop</i> – The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client.</p> <p><i>Keep</i> – The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client.</p>

Click **Apply** to implement any changes that have been made.



NOTE: If the Switch receives a packet that contains the option-82 field from a DHCP client and the information-checking feature is enabled, the Switch drops the packet because it is invalid. However, in some instances, users may configure a client with the option-82 field. In this situation, disable the information-check feature so that the Switch does not remove the option-82 field from the packet. Users may configure the action that the Switch takes when it receives a packet with existing option-82 information by configuring the DHCP Agent Information Option 82 Policy.

The Implementation of DHCP Information Option 82

The `config dhcp_relay option_82` command configures the DHCP relay agent information option 82 setting of the switch. The formats for the circuit ID sub-option and the remote ID sub-option are as follows:



NOTE: For the circuit ID sub-option of a standalone switch, the module field is always zero.

Circuit ID sub-option format:

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Module	Port
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

- a. Sub-option type
- b. Length
- c. Circuit ID type
- d. Length
- e. VLAN: the incoming VLAN ID of DHCP client packet.
- f. Module: For a standalone switch, the Module is always 0; For a stackable switch, the Module is the Unit ID.
- g. Port: The incoming port number of DHCP client packet, port number starts from 1.

Remote ID sub-option format:

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 byte	1 byte	1 byte	1 byte	6 bytes

1. Sub-option type
2. Length
3. Remote ID type
4. Length
5. MAC address: The Switch's system MAC address.

Figure 2 - 62 Circuit ID and Remote ID Sub-option Format

DHCP/BOOTP Relay Interface Settings


This window allows the user to set up a server, by IP address, for relaying DHCP/ BOOTP information. The user may enter a previously configured IP interface on the Switch that will indicate which interface is able to support the dhcp relay function. Properly configured settings will be displayed in the BOOTP Relay Table at the bottom of the following window, once the user clicks the **Add** button under the **Apply** heading. The user may add up to four server IPs per IP interface on the Switch.

To view this window, click **Administration > DHCP/BOOTP Relay > DHCP/BOOTP Relay Interface Settings** as shown below.

Figure 2 - 63 DHCP/BOOTP Relay Interface Settings window

The following parameters can be configured or viewed:

Parameter	Description
Interface	The IP interface on the Switch that will be connected directly to the client.
Server IP	Enter the IP address of the DHCP/BOOTP server. Up to four server IPs can be configured per IP Interface

Click **Add** to include this Server To remove an entry, click the corresponding  button.

DHCP Relay Option 60 Default Settings

This window allows the user to configure the DHCP Relay Option 60 Default servers. When there are no matching servers found for the packet based on option 60, the relay servers will be determined by the default relay server setting. Similarly, when there is no match found for the packet, the relay servers will be determined based on the default relay servers.


To view this window, click **Administration > DHCP/BOOTP Relay > DHCP Relay Option 60 Default Settings**, as shown below.

Figure 2 - 64 DHCP Relay Option 60 Default Settings window

The following parameters can be configured:

Parameter	Description
-----------	-------------

Relay IP Address	Enter the specified IP address for the DHCP relay forward.
Mode	Use the pull-down menu to choose either <i>Relay</i> or <i>Drop</i> . When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet will be relayed based on the relay rules.

Click **Add** to add a new Relay IP Address entry. Click **Apply** to implement the changes. To remove any entry, click the corresponding  button.

DHCP Relay Option 60 Settings

This window is used to configure option 60 relay rules on the Switch. Different strings can be specified for the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.

To view this window, click **Administration > DHCP/BOOTP Relay > DHCP Relay Option 60 Settings**, as shown below.

Figure 2 - 65 DHCP Relay Option 60 Table window

To find a particular entry, enter the correct IP Address or String and click **Search**. Click the **View All** button to see all the entries in the table at the bottom half of the window. To delete an entry, enter the appropriate *IP address/String* and relay IP address information, and click **Delete**. To delete all the entries, click **Clear All**. To add a new entry click **Add** the following window will appear:

Figure 2 - 66 DHCP Relay Option 60 Table - Add window

The following parameters may be configured:

Parameter	Description
String	Enter the specified string, up to a maximum of 255 alphanumeric characters.
Server IP	Enter the relay server IP address.
Match Type	Use the drop-down menu to select either <i>Exact Match</i> or <i>Partial Match</i> .

	<p><i>Exact Match</i> – The option 60 string in the packet must fully match the specified string.</p> <p><i>Partial Match</i> – The option 60 string in the packet only needs to partially match the specified string.</p>
--	--

Click **Apply** to implement the changes. To return to the DHCP Relay Option 60 Table window, click the [Show DHCP Relay Option 60 Table](#) link.

DHCP Relay Option 61 Default Settings

This window is used to configure the DHCP Relay Option 61 Default Settings. These settings are used to determine the rule to process those packets that have no option 61 matching rules.

To view this window, click **Administration > DHCP/BOOTP Relay > DHCP Relay Option 61 Default Settings**, as shown below.

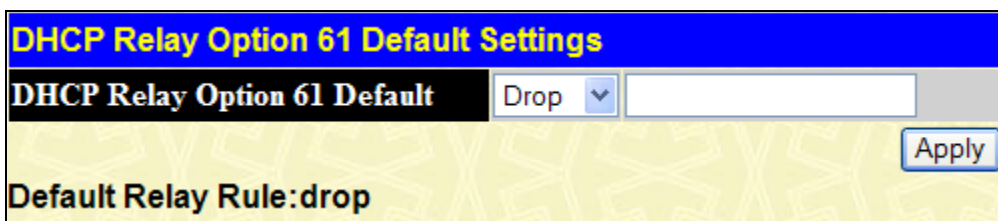


Figure 2 - 67 DHCP Relay Option 61 Default Settings window

The following parameters can be configured:

Parameter	Description
DHCP Relay Option 61 Default	<p>Use the pull-down menu to choose either <i>Relay</i> or <i>Drop</i>. When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet will be relayed based on the relay rules.</p> <p>Enter the IP Address of the entry you wish to configure.</p>

Click **Apply** to implement the changes.

DHCP Relay Option 61 Settings

This command is used to add a rule to the relay server based on option 61. The matching rule can be based on either the MAC address or by using a user-specified string. Only one relay server can be specified for a MAC address or a string. If the existing relay servers are determined based on option 60, and one relay server is determined based on option 61, the final relay servers will be the union of these two sets of servers.

To view this window, click **Administration > DHCP/BOOTP Relay > DHCP Relay Option 61 Settings**, as shown below.

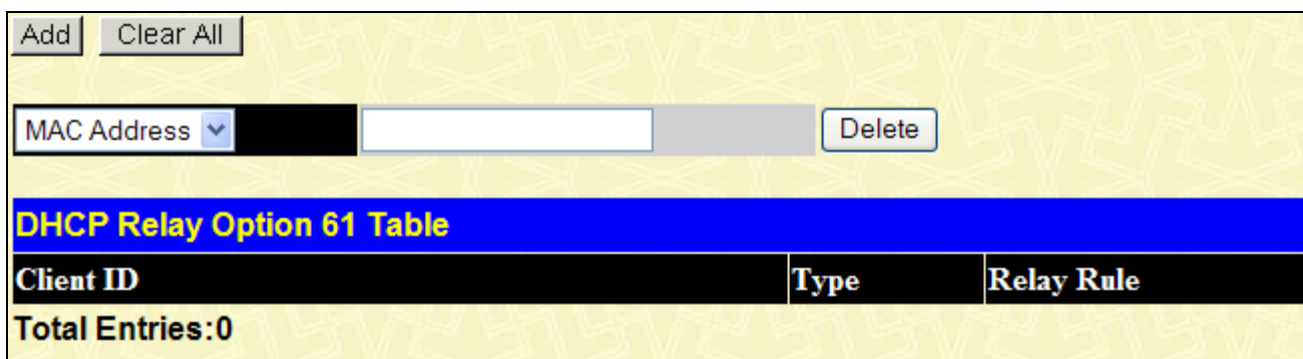


Figure 2 - 68 DHCP Relay Option 61 Table window

To remove an entry, enter the appropriate *MAC Address* or *String* information and click **Delete**. To delete all entries click **Clear All**. To add a new entry click **Add** the following window will appear.

Figure 2 - 69 DHCP Relay Option 61 Table - Add window

The following parameters can be configured:

Parameter	Description
Client ID	Click the radio buttons to select the method of identification for the Client ID either MAC Address or String. The MAC Address will specify the hardware address of the client and the String will specify the client ID. Choose a method and enter the appropriate information into the box provided.
Relay Rule	Click the radio buttons to choose either <i>Relay</i> or <i>Drop</i> . When drop is specified, the packet with no matching rules found will be dropped without further process. When relay is selected the packet will be relayed based on the relay rules. Choose a method and enter the appropriate information into the box provided.

Click **Apply** to implement the changes.

DHCP/BOOTP Local Relay Settings

This window is used to configure the global settings of DHCP/BOOTP local relay.

To view this window, click **Administration > DHCP/BOOTP Local Relay Settings**, as shown below.

Figure 2 - 70 DHCP/BOOTP Local Relay Global Settings window

The following parameters are displayed or can be configured:

Parameter	Description
Global State	Use the pull-down menu to enable or disable the status.
VLAN State	Use the pull-down menu to enable or disable the VLAN status.
VLAN Name	Enter the name of VLAN.

VID List	Display the VLAN list.
-----------------	------------------------

Click **Apply** to implement the changes.

DHCPv6 Relay

This section contains information for configuring DHCPv6 relay, including DHCP v6 Relay Global Settings and DHCPv6 Relay Interface Settings.

DHCPv6 Relay Global Settings

This window is used to set up the DHCPv6 relay global status.

To view this window, click **Administration > DHCPv6 Relay > DHCPv6 Relay Global Settings** as shown below.

Figure 2 - 71 DHCPv6 Relay Global Settings window

The following fields can be configured:

Parameter	Description
Global State	This field can be toggled between <i>Enabled</i> and <i>Disabled</i> using the pull-down menu. It is used to enable or disable the DHCPv6 Relay service on the Switch. The default is <i>Disabled</i> .
Hops Count (1-32)	This field allows an entry between 1 and 32 to define the maximum number of router hops DHCPv6 messages can be forwarded across. The default hop count is 4.

Click **Apply** to implement the changes.

DHCPv6 Relay Interface Settings

This window displays the current DHCPv6 relay configurations.

To view this window, click **Administration > DHCPv6 Relay > DHCPv6 Relay Interface Settings** as shown below.

Figure 2 - 72 DHCPv6 Relay Interface Settings window

To search for an entry, enter the Interface Name and click **Find**. To display all current entries on the Switch click **View All**. To change a current entry, click the corresponding **Modify** button of the entry, revealing the following window to configure:

Figure 2 - 73 DHCPv6 Relay Interface Settings - Edit window

The following fields are displayed or can be configured:

Parameter	Description
Interface Name	Display the IPv6 relay interface name.
Hops Count (1-32)	This field allows an entry between 1 and 32 to define the maximum number of router hops DHCPv6 messages can be forwarded across. The default hop count is 4.
State	Use the pull-down menu to enable or disable DHCPv6 relay on.

Click **Apply** to implement the changes. To return to the DHCPv6 Relay Interface Settings window, click the [Show All DHCPv6 Relay Interface Entries](#) link.

To see server addresses of an interface, click the corresponding **View** button to see the following window:

Figure 2 - 74 DHCPv6 Relay Interface Settings - View window

The following fields are displayed or can be configured:

Parameter	Description
Interface Name	Display the IPv6 relay interface name.
DHCPv6 Server Address	Enter the IPv6 destination address to forward DHCPv6 packets.

Click **Apply** to implement the changes. To remove any entry, click the corresponding  button. To return to the DHCPv6 Relay Interface Settings window, click the [Show All DHCPv6 Relay Interface Entries](#) link.

DHCP Server

For this release, the Switch now has the capability to act as a DHCP server to devices within its locally attached network. DHCP, or Dynamic Host Configuration Protocol, allows the switch to delegate IP addresses, subnet masks, default gateways and other IP parameters to devices that request this information. This occurs when a DHCP enabled device is booted on or attached to the locally attached network. This device is known as the DHCP client and when enabled, it will emit query messages on the network before any IP parameters are set. When the DHCP server receives this request, it returns a response to the client, containing the previously mentioned IP information that the DHCP client then utilizes and sets on its local configurations.

The user can configure many DHCP related parameters that it will utilize on its locally attached network, to control and limit the IP settings of clients desiring an automatic IP configuration, such as the lease time of the allotted IP address, the range of IP addresses that will be allowed in its DHCP pool, the ability to exclude various IP addresses within the pool as not to make identical entries on its network, or to assign the IP address of an important device (such as a DNS server or the IP address of the default route) to another device on the network.

Users also have the ability to bind IP addresses within the DHCP pool to specific MAC addresses in order to keep consistent the IP addresses of devices that may be important to the upkeep of the network that require a static IP address. The Switch supports 1024 DHCP pool entries along with eight pools.

DHCP Server Global Settings

The following window will allow users to globally enable the switch as a DHCP server and set the DHCP Ping Settings to test connectivity between the DHCP Server and Client.

To view this window, click **Administration > DHCP Server > DHCP Server Global Settings**, as shown below.

Figure 2 - 75 DHCP Server Settings window

The following parameters may be configured:

Parameter	Description
DHCP Server Global State	Use the pull-down menu to globally enable or disable the switch as a DHCP server.
Ping Packets (Number 2-10)	Enter a number between 2 and 10 to denote the number of ping packets that the Switch will send out on the network containing the IP address to be allotted. If the ping request is not returned, the IP address is considered unique to the local network and then allotted to the requesting client. The default setting is 2 packets.
Ping Timeout (Millisecond 500-2000)	The user may set a time between 500 and 2000 milliseconds that the Switch will wait before timing out a ping packet. The default setting is 500 milliseconds.

Click **Apply** to implement the changes.

DHCP Server Exclude Address Settings


The following window will allow the user to set an IP address, or a range of IP addresses that are NOT to be included in the range of IP addresses that the Switch will allot to clients requesting DHCP service. To set an IP address or range of IP addresses, enter the Begin Address of the range and then the End Address of the range and click **Apply**. Set address ranges will appear in the DHCP Exclude Address Table in the bottom half of the window, as shown below.

To view this window, click **Administration > DHCP Server > DHCP Server Exclude Address Settings**, as shown below.

Figure 2 - 76 Create DHCP Excluded Address window

The following parameters may be configured:

Parameter	Description
Begin Address	Enter the starting IP address of the range of IP addresses to be excluded from the DHCP pool.
End Address	Enter the final IP address of the range of IP addresses to be excluded from the DHCP pool.

Click **Apply** to implement changes made. To remove any entry, click the corresponding  button. To delete all the entries, click **Clear All**.

DHCP Server Pool Settings

The following windows will allow users to create and then set the parameters for the DHCP Pool of the switch's DHCP server.

To view the following window, click **Administration > DHCP Server > DHCP Server Pool Settings**, as shown below.

Create DHCP Pool

Pool Name		
------------------	--	--

DHCP Server Pool Table

Pool Name	Modify	Display	Delete
RG	<input type="button" value="Modify"/>	<input type="button" value="View"/>	<input type="button" value="X"/>

Total Entries: 1

Figure 2 - 77 Create DHCP Pool window

Users must first create the pool by entering a name of up to 12 alphanumeric characters into the Pool Name field and clicking **Apply**. To remove an entry in the table, click the corresponding button. To configure the settings of a pool in the DHCP Server Pool Table, click the corresponding **Modify** button to reveal the following window:

Config DHCP Pool

Pool Name	RG
IP Address	
Netmask	
Domain Name	
DNS Server Address	0.0.0.0
	0.0.0.0
	0.0.0.0
NetBIOS Name Server	0.0.0.0
	0.0.0.0
	0.0.0.0
NetBIOS Node Type	Broadcast <input type="button" value="v"/>
Default Router	0.0.0.0
	0.0.0.0
	0.0.0.0
Pool Lease	1 Days <input type="button" value="v"/> 00 Hours <input type="button" value="v"/> 00 Minutes <input type="checkbox"/> Infinite
Boot File	
Next Server	0.0.0.0

[Show All DHCP Pool Entries](#)

Figure 2 - 78 Config DHCP Pool window

The following parameters can be configured or viewed:

Parameter	Description
Pool Name	Denotes the name of the DHCP pool for which you are currently adjusting the parameters.
IP Address	Enter the IP address to be assigned to requesting DHCP Clients. This address will not be chosen but the first 3 sets of numbers in the IP address will be used for the IP address of requesting DHCP Clients. (ex. If this entry is given the IP address 10.10.10.2, then assigned addresses to DHCP Clients will resemble 10.10.10.x, where x is a number between 1 and 255 but does not include the assigned 10.10.10.2)
Netmask	Enter the corresponding Netmask of the IP address assigned above.
Domain Name	Enter the domain name for the DHCP client. This domain name represents a general group of networks that collectively make up the domain. The Domain Name may be an alphanumeric string of up to 64 characters.
DNS Server Address	Enter the IP address of a DNS server that is available to the DHCP client. The DNS Server correlates IP addresses to host names when queried. Users may add up to three DNS Server addresses.
Net BIOS Name Server	Enter the IP address of a Net BIOS Name Server that will be available to a Microsoft DHCP Client. This Net BIOS Name Server is actually a WINS (Windows Internet Naming Service) Server that allows Microsoft DHCP clients to correlate host names to IP addresses within a general grouping of networks. The user may establish up to three Net BIOS Name Servers.
NetBIOS Node Type	This field will allow users to set the type of node server for the previously configured Net BIOS Name server. Using the pull-down menu, the user has four node type choices: <i>Broadcast</i> , <i>Peer to Peer</i> , <i>Mixed</i> , and <i>Hybrid</i> .
Default Router	Enter the IP address of the default router for a DHCP Client. Users must configure at least one address here, yet up to three IP addresses can be configured for this field. The IP address of the default router must be on the same subnet as the DHCP client.
Pool Lease	Using this field, the user can specify the lease time for the DHCP client. This time represents the amount of time that the allotted address is valid on the local network. Users may set the time by entering the days into the open field and then use the pull-down menus to precisely set the time by hours and minutes. Users may also use the Infinite check box to set the allotted IP address to never be timed out of its lease. The default setting is 1 day.
Boot File	This field is used to specify the Boot File that will be used as the boot image of the DHCP client. This image is usually the operating system that the client uses to load its IP parameters.
Next Server	This field is used to identify the IP address of the device that has the previously stated boot file.

Click **Apply** to implement changes made. To return to the Create DHCP Pool window, click the [Show All DHCP Pool Entries](#) link.

To view the previously set parameters for a configured DHCP Pool, click the corresponding **View** button in the Create DHCP Pool window, which will produce the following window:

DHCP Server Pool Display	
Pool Name	RG
IP Address	-----
Netmask	-----
Domain Name	
DNS Server Address	0.0.0.0
	0.0.0.0
	0.0.0.0
NetBIOS Name Server	0.0.0.0
	0.0.0.0
	0.0.0.0
NetBIOS Node Type	Broadcast
Default Router	0.0.0.0
	0.0.0.0
	0.0.0.0
Pool Lease	1 Days, 0 Hours, 0 Minutes
Boot File	
Next Server	0.0.0.0

[Show All DHCP Server Pool Entries](#)

Figure 2 - 79 DHCP Server Pool Display window

To return to the Create DHCP Pool window, click the [Show All DHCP Server Pool Entries](#) link.

DHCP Server Dynamic Binding

The following window will allow users to view dynamically bound IP addresses of the DHCP server. These IP addresses are ones that were allotted to clients on the local network and are now bound to the device stated by its MAC address.

To view this window, click **Administration > DHCP Server > DHCP Server Dynamic Binding**, as shown below.

Pool Name	<input style="width: 95%;" type="text"/>	<input type="button" value="Find"/>	<input type="button" value="Clear"/>
------------------	--	-------------------------------------	--------------------------------------

DHCP Server Dynamic Binding Table

Pool Name	IP Address	Hardware Address	Type	Status	Life Time (sec)
Total Entries: 0					

[Show All DHCP Server Dynamic Binding Table Entries](#)

Figure 2 - 80 DHCP Server Dynamic Binding Table window

The following parameters may be configured or viewed:

Parameter	Description
-----------	-------------

Pool Name	To find the dynamically bound entries of a specific pool, enter the Pool Name into the field and click Find . Dynamically bound entries of this pool will be displayed in the table. To clear the corresponding Pool Name entries of this table, click Clear .
Pool Name	This field will denote the Pool Name of the displayed dynamically bound DHCP entry.
IP Address	This field will display the IP address allotted to this device by the DHCP Server feature of this Switch.
Hardware Address	This field will display the MAC address of the device that is bound to the corresponding IP address.
Type	This field will display the type of node server being used for the previously configured Net BIOS Name server of this entry.
Status	This field will display the Status of the entry, whether it was dynamically bound or manually bound.
Life Time (sec)	This field will display, in seconds, the time remaining on the lease for this IP address.

To clear all entries, click **Clear All**. To see all the entries, click the [Show All DHCP Server Dynamic Binding Table Entries](#) link.

DHCP Server Manual Binding

The following windows will allow users to view and set manual DHCP entries. Manual DHCP entries will bind an IP address with the MAC address of a client within a DHCP pool. These entries are necessary for special devices on the local network that will always require a static IP address that cannot be changed.

To view this window, click **Administration > DHCP Server > DHCP Server Manual Binding**, as shown below.

Figure 2 - 81 DHCP Server Manual Binding Table window

Users may view statically bound DHCP entries within a DHCP pool by entering the Pool Name and clicking **Find**. Results will be displayed in the DHCP Server Manual Binding Table. To delete a pool, enter the name in **Pool Name** and click **Clear**. To see all the entries, click the [Show All DHCP Server Manual Binding Table Entries](#) link. To set a manual DHCP Binding entry, click the **Add** button, which will produce the following window to configure.

Figure 2 - 82 Create DHCP Pool Manual Binding window

The following parameters may be configured or viewed.

Parameter	Description
Pool Name	Enter the name of the DHCP pool within which will be created a manual DHCP binding entry.
IP Address	Enter the IP address to be statically bound to a device within the local network that will be specified by entering the Hardware Address in the following field.
Hardware Address	Enter the MAC address of the client to be statically bound to the IP address entered in the previous field.
Type	This field is used to specify the type of connection for which this manually bound entry will be set. <i>Ethernet</i> will denote that the manually bound device is connected directly to the Switch, while the <i>IEEE802</i> denotes that the manually bound device is outside the local network of the Switch.

Click **Apply** to set the entry. To return to the DHCP Server Manual Binding Table window, click the [Show All Manual Binding Entries](#) link.

DHCPv6 Server

DHCPv6 is the abbreviation of Dynamic Host Configuration Protocol for IPv6, a client/server protocol that provides managed configuration of devices. The primary function of DHCPv6 Server is to assign IPv6 addresses to a client. This function is conceptually the same as IPv4 DHCP Server.

In DHCPv6 server address pool function, the user can configure a new address pool name and a range of available IPv6 addresses for address pool. All IPv6 addresses in a DHCPv6 address pool are valid for assigning to the DHCPv6 clients. The user also can use 'excluded-address' to reserve the IPv6 addresses that the user doesn't want to assign the IPv6 addresses to a client (e.g. the IPv6 address of DNS server and the IPv6 address of DHCPv6 server).The clients query DNS servers when they need to correlate host names to IPv6 address. The Switch supports DNS server and Domain name configuration.

The server supports manual binding for a DHCPv6 client. An address binding is a mapping between the IPv6 address and DUID of a client. Manual bindings are IPv6 addresses that have been manually mapped to the DUID of hosts which are the administrator manual set. The manual binding address is based on pool, the address must be in the range of the pool, to configure a manual binding, at the user needs to specify the address pool, and then specify the client's DUID, the IPv6 address of the client.

When the configurations of the DHCPv6 Server have changed, user must re-enable dhcpv6_server (If the state of the DHCPv6 server is enabled, first disable dhcpv6_server, then enable dhcpv6_server) to validate the configuration.

DHCPv6 Server Global Settings

The following window is used to configure the DHCPv6 server global status.

To view this window, click **Administration > DHCPv6 Server > DHCPv6 Server Global Settings**, as shown below.



Figure 2 - 83 DHCPv6 Server Global Settings window

The following parameters may be configured:

Parameter	Description
Global State	Use the pull-down menu to globally enable or disable the switch as a DHCP server.

Click **Apply** to implement the changes.

DHCPv6 Server Pool Settings

The window is used to see all the DHCPv6 server pool entries.

To view the following window, click **Administration > DHCPv6 Server > DHCPv6 Server Pool Settings**, as shown below.

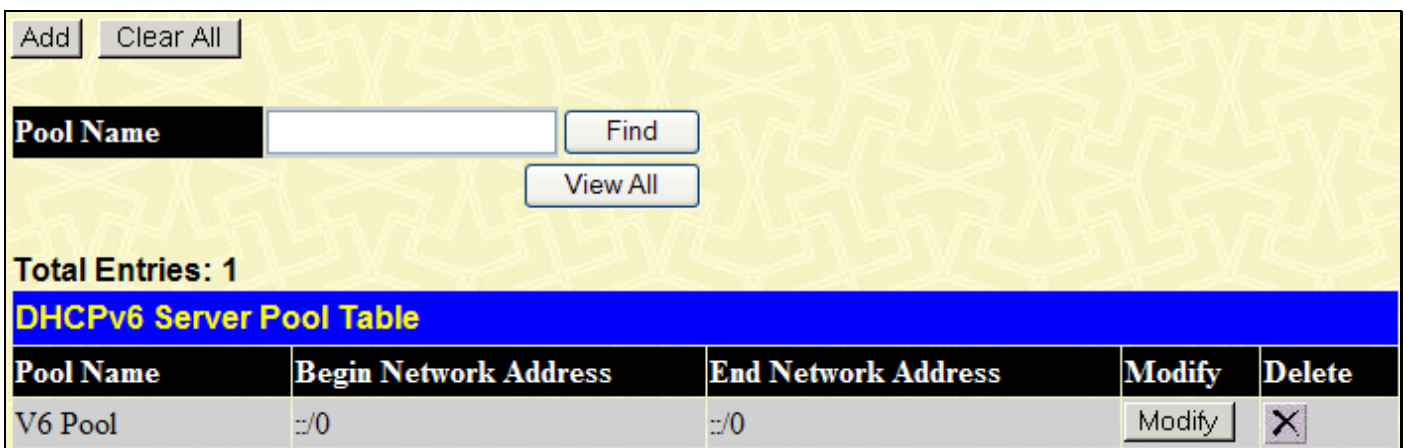


Figure 2 - 84 DHCPv6 Pool Table window

To find the DHCPv6 server pool entries, enter the Pool Name into the field and click **Find**. Click **View All** to see all the entries. To clear all Pool Name entries of this table, click **Clear All**. To create pool name, click **Add**, which will produce the following window to configure.

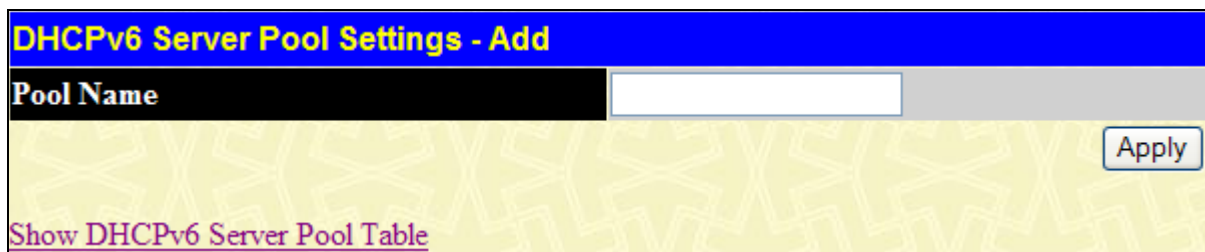


Figure 2 - 85 DHCPv6 Pool Table - Add window

The following parameters may be configured:

Parameter	Description
Pool Name	Enter a name of the DHCPv6 server pool.

Click **Apply** to implement the changes. To return to the DHCPv6 Server Pool Table window, click the [Show DHCPv6 Server Pool Table](#) link.

To configure the settings of a pool in the DHCPv6 Server Pool Table, click the corresponding **Modify** button to reveal the following window:

Figure 2 - 86 DHCPv6 Pool Table - Edit window

The following parameters can be configured or viewed:

Parameter	Description
Pool Name	Display the name of the DHCPv6 server pool.
Begin Network Address	The starting IPv6 network address of the DHCPv6 pool.
End Network Address	The final IPv6 network address of the DHCPv6 pool.
Domain Name	Enter a name that is used by the client as default domain name.
DNS Server	Enter the DNS server IPv6 address for this pool. Users may specify up to two DNS server addresses.
Preferred Lifetime (60-4294967295)	Enter the amount of time in seconds that the IPv6 address, based on the specified pool, remains in preferred state.
Valid Lifetime (60-4294967295)	Enter the amount of time in seconds that the IPv6 address, based on the specified pool, remains in valid state.

Click **Apply** to implement the changes. To return to the DHCPv6 Server Pool Table window, click the [Show DHCPv6 Server Pool Table](#) link.

DHCPv6 Server Manual Binding Settings

This window displays the DHCPv6 server manual binding pool information.

To view this window, click **Administration > DHCPv6 Server > DHCPv6 Server Manual Binding Settings** as shown below.

Pool Name Find Delete

View All

Total Entries: 1

DHCPv6 Server Manual Binding Brief Table

Pool Name	IPv6 Address
V6 Pool	View

Figure 2 - 87 DHCPv6 Server Manual Biding Brief Table window

To find the DHCPv6 server manual binding entries, enter the Pool Name into the field and click **Find**. Click **View All** to see all the entries. To remove an entry from the table, enter the Pool Name into the field and click **Delete**. To configure more settings, click **View** to see the following window:

DHCPv6 Server Manual Binding Settings - Add

Pool Name

IPv6 Address (e.g.: 2233::1)

Client DUID

Apply

Total Entries: 0

DHCPv6 Server Manual Binding Table

Pool Name	IPv6 Address	Identifier (DUID)	Delete
-----------	--------------	-------------------	--------

[Show DHCPv6 Server Manual Binding Brief Table](#)

Figure 2 - 88 DHCPv6 Server Manual Biding Brief Table - View window

The following fields can be configured or viewed:

Parameter	Description
Pool Name	Display the name of the DHCPv6 server pool.
IPv6 Address	Enter the IPv6 address to be statically bound to a device.
Client DUID	Enter the DUID of the device to be statically bound to the IPv6 address entered in the previous field. The DUID format is '0--9', 'a--f' or 'A--F'.

Click **Apply** to implement the changes. To remove any entry, click the corresponding  button. To return to the DHCPv6 Server Manual Binding Brief Table window, click the [Show DHCPv6 Server Manual Binding Brief Table](#) link.

DHCPv6 Server Dynamic Binding Settings

This window displays the DHCPv6 server dynamic binding pool information.

To view this window, click **Administration > DHCPv6 Server > DHCPv6 Server Dynamic Binding Settings**, as shown below.

Clear All

Pool Name Find Clear

View All

Total Entries: 1

DHCPv6 Server Dynamic Binding Brief Table

Pool Name	Detail
V6 Pool	View

Figure 2 - 89 DHCPv6 Server Dynamic Biding Brief Table window

To find the DHCPv6 server dynamic binding entries, enter the Pool Name into the field and click **Find**. Click **View All** to see all the entries. To remove an entry from the table, enter the Pool Name into the field and click **Clear**. To see more detail settings, click **View** to see the following window:

Total Entries: 0

DHCPv6 Server Dynamic Binding Table

Pool Name	IPv6 Address	Identifier (DUID)	Preferred (sec)	Valid (sec)
Show DHCPv6 Server Dynamic Binding Brief Table				

Figure 2 - 90 DHCPv6 Server Dynamic Biding Brief Table - View window

To return to the DHCPv6 Server Manual Binding Brief Table window, click the [Show DHCPv6 Server Dynamic Binding Brief Table](#) link.

DHCPv6 Server Interface Settings

This window displays the DHCPv6 server interface settings.

To view this window, click **Administration > DHCPv6 Server > DHCPv6 Server Interface Settings** as shown below.

Interface Name Find

View All

Total Entries: 1

DHCPv6 Server Interface Table

Interface Name	DHCPv6 Server State	Modify
System	Enabled	Modify

Figure 2 - 91 DHCPv6 Server Interface Table window

To find the DHCPv6 server interfaces, enter the Interface Name into the field and click **Find**. Click **View All** to see all the entries. To see change the DHCPv6 server interface settings, click **Modify** to see the following window to configure:

Figure 2 - 92 DHCPv6 Server Dynamic Interface Table - Edit window

The following fields can be configured or viewed:

Parameter	Description
Interface Name	Display the name of the interface.
DHCPv6 Server State	Use the pull-down menu to enable or disable the DHCPv6 server status.

Click **Apply** to implement the changes. To return to the DHCPv6 Server Interface Table window, click the [Show DHCPv6 Server Interface Table](#) link.

DHCPv6 Server Excluded Address Settings

This window displays the DHCPv6 server excluded address information.

To view this window, click **Administration > DHCPv6 Server > DHCPv6 Server Excluded Address Settings** as shown below.

Figure 2 - 93 DHCPv6 Server Excluded Address Brief Table window

To find the DHCPv6 server excluded address entries, enter the Pool Name into the field and click **Find**. Click **View All** to see all the entries. To remove an entry from the table, enter the Pool Name into the field and click **Delete**. To see more detail settings, click **View** to see the following window:

DHCPv6 Server Excluded Address Settings - Add

Pool Name: V6 Pool

Begin Address: (e.g.: 2233::1)

End Address: (e.g.: 2233::1)

Apply

DHCPv6 Server Excluded Address Table

Pool Name	Range	Begin Address	End Address	Delete
-----------	-------	---------------	-------------	--------

[Show DHCPv6 Server Excluded Address Brief Table](#)

Figure 2 - 94 DHCPv6 Server Excluded Address Brief Table - View window

The following fields can be configured or viewed:

Parameter	Description
Pool Name	Display the name of the pool.
Begin Address	Enter the starting IP address of the range of IP addresses to be excluded from the DHCPv6 pool.
End Address	Enter the final IP address of the range of IP addresses to be excluded from the DHCPv6 pool.

Click Apply to implement the changes. To return to the DHCPv6 Server Excluded Address Brief Table window, click the [Show DHCPv6 Server Excluded Address Brief Table](#) link.

Filter DHCP Server

The Dynamic Host Configuration Protocol (DHCP) automates the assignment of IP addresses, subnet masks, default routers, and other IP parameters. The assignment usually occurs when the DHCP configured machine boots up or regains connectivity to the network. The DHCP client sends out a query requesting a response from a DHCP server on the locally attached network. The DHCP server then replies to the client with its assigned IP address, subnet mask, DNS server and default gateway information.

This function allows DHCP server packets except those that have been IP/client MAC bound to be filtered. The DHCP Server Screening is used to configure the state of the function for filtering of DHCP server packets and to add or delete the DHCP server/client binding entry. This command has two purposes firstly to filter all DHCP server packets on the specified port(s) and secondly to allow some DHCP server packets to be forwarded if they are on the pre-defined server IP address/MAC address binding list. Thus the DHCP server can be restricted to service a specified DHCP client. This is useful when there are two or more DHCP servers present on a network.

Filter DHCP Server Global Settings

This window is used to enable the settings for the Filter DHCP Server Global Settings on the Switch.

To view this table, click **Administration > Filter DHCP Server > Filter DHCP Server Global Settings**, as shown below.

DHCP Server Filter Global Settings

Trap / Log: Disabled

Illegal Server Log Suppress Duration: 5 min

Apply

Figure 2 - 95 DHCP Server Filter Global Settings window

The following parameters may be configured:

Parameter	Description
Trap/Log	Enable this function to record logs and send traps when the Switch detects the illegal DHCP server packets.
Illegal Server Log Suppress Duration	The DHCP Server Screening function filters any illegal DHCP server packets. The DHCP server who sends the illegal packets will be logged. This command is used to suppress the logging of DHCP servers who continue to send illegal DHCP packets. The same illegal DHCP server IP address that is detected will be logged only once regardless of how many illegal packets are sent. The log can be suppressed by 1 minute, 5 minutes or 30 minutes. The default value is 5 minutes.

Click **Apply** to implement the changes.

Filter DHCP Server Port Settings

This window is used to enable the settings for the Filter DHCP Server Port Settings.

To view this window, click **Administration > Filter DHCP Server > Filter DHCP Server Port Settings**, as shown below.

Figure 2 - 96 Filter DHCP Server Port State Settings window

The following parameters may be configured:

Parameter	Description
State	Use the pull-down menu to enable or disable the Filter DHCP Server Port State Settings.

Port List	Specify the ports that will enable or disable the filter DHCP server. Tick the All Ports check box to select all ports.
Filter DHCP Server Port Settings	
Action	Select <i>Add</i> or <i>Delete</i> to add or delete a filter DHCP server entry.
Server IP Address	The IP address of the DHCP server that specifies an allotted server IP address to the client.
Client MAC Address	Specify the MAC address of the client which allowed the requested IP address from the DHCP server.
Port List	Enter the list of ports to use the given filter DHCP server entry. Tick the All Ports check box to select all ports.

Click **Apply** to implement the changes.

Layer 2 Protocol Tunneling Settings

The Layer 2 Protocol Tunneling (L2PT) supports traffic of multiple customers across service provider networks. L2PT enables the BPDU's of the same customer's network to be multicast over specific VLANs in the service provider's network, which in turn will ensure the same geographically dispersed customer network can implement consistent spanning tree calculations across the service provider network.

To view this window, click **Administration > Layer 2 Protocol Tunneling Settings**, as shown below.

Figure 2 - 97 Layer 2 Protocol Tunneling Settings window

The following fields can be configured:

Parameter	Description
Layer 2 Protocol Tunneling State	Use the drop-down menu to choose <i>Enabled</i> or <i>Disabled</i> .
Unit	Select the unit to configure.

From / To	Specify the ports on which the BPDU Tunneling will be enabled or disabled.
Type	Use the drop-down menu to select the configuration type. <i>Tunnel</i> – Specifies that the BPDU is received from a tunnel port, this packets DA will be replaced by a reserved multicast address and then sent out to a providers network through the uplink port. <i>Uplink</i> – Specifies that the port is a normal switch port which connects to the network provider. The encapsulated PDU received on the uplink port shall be terminated and the DA is replaced with the STP/GVRP MAC address, the packet is then sent to the tunnel port in the same VLAN. <i>None</i> – When selected an encapsulated PDU is received on a port and the forwarding behavior follows the forwarding of general multicast addresses. <i>None</i> is the default.
STP/GVRP	Select the type of tunnel multicast address to be applied to the ports either <i>STP</i> or <i>GVRP</i> . An STP enabled port can not be configured as an STP tunnel port. A GVRP enabled port can not be configured as a GVRP tunnel port.

Click **Apply** to implement the changes.

RSPAN

RSPAN (Remote Switched Port Analyzer) is a feature used to monitor and analyze the traffic passing through ports. The character ‘R’ is short for ‘Remote’ which means that the mirror source ports and the destination port are not on the same Switch. So a remote mirror session consists of at least two switches. To achieve the remote mirroring function, the mirrored traffic is tagged with a reserved VLAN which is called an RSPAN VLAN, the RSPAN VLAN is reserved in such a way that traffic tagged with RSPAN will be mirrored toward the associated destination port.

There are three roles for switches in RSPAN.

Source switch – The switch which has the monitored ports or VLANs on it is the source switch. All packets on the source ports or VLANs are copied and sent to the destination switch. When the mirrored packets are sent out from the source switch, an RSPAN VLAN tag is added to every packet. The incoming port on the source switch for the mirrored packets is referred to as the **source port**.

Intermediate switch The function of the intermediate switch is to mirror traffic flowing in the RSPAN VLAN toward the RSAPN destination. A switch can be have the role of an RSAPN VLAN intermediate switch as well as the role of source switch for another RSPAN VLAN.

Destination Switch The port which is directly connected to a network analyzer, other monitoring, or security device is called the **destination port**. The switch which has a destination port is called the **destination switch**. The destination switch removes the RSPAN VLAN tags from the mirrored packets when the destination port is an untagged port in the RSPAN VLAN. If the destination port is a tagged port, the tags will be reserved.

RSPAN State Settings

This window allows the user to enable or disable the RSPAN settings on the Switch. The purpose of the RSPAN function is to mirror the packets to the remote switch. The packet travels from the switch where the monitored packet is received, through the intermediate switch, then to the switch where the sniffer is attached. The first switch is also named the source switch.

To view this window, click **Administration > RSPAN > RSPAN State Settings**, as shown below.

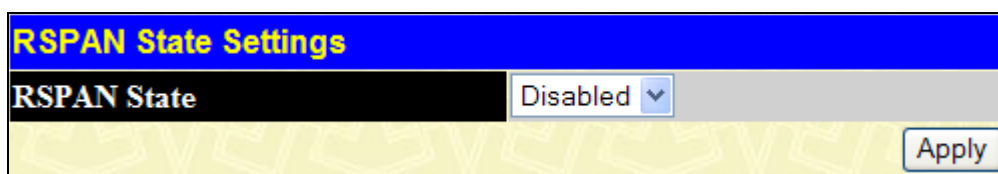


Figure 2 - 98 RSPAN State Settings window

Use the drop down menu to enable or disable the **RSPAN State** on the Switch, and click **Apply** to implement the changes.

RSPAN Settings

This window allows the user to search for a previously created VLAN and to view the RSPAN settings for it.

To view this window, click **Administration > RSPAN > RSPAN Settings**, as shown below.

Figure 2 - 99 RSPAN Settings window

The following fields can be configured:

Parameter	Description
VLAN Name	Enter the name of the VLAN you wish to Add, Find or Delete.
VID (1-4094)	Enter the VLAN ID of the VLAN you wish to Add, Find or Delete.
Target Port	The target port that receives the packets duplicated at the source port.
RX Source Ports	The goal of RX source ports is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that RSPAN session.
TX Source Ports	The goal of TX source ports is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch.
Redirect Port	RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

To remove an entry, use the radio button to enter VLAN name or VLAN ID in the field, and click the corresponding **Delete by VLAN** or **Delete By VID** icon. To search for an entry, use the radio button to enter VLAN name or VLAN ID in the field, and click the **Find by VLAN** or **Find by VID** button.

To modify an existing entry of its redirect settings, click the corresponding **Modify** button in Modify Redirect, revealing the following window to configure:

Figure 2 - 100 RSPAN Settings – Edit Redirect window

The following fields can be configured:

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN which will modify the RSPAN Entries.
VID (1-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN which will modify the RSPAN Entries.
Redirect Port Action	Use the drop down menu to select the configuration Redirect Ports Action. <i>Add</i> – Add Redirect ports. <i>Delete</i> – Delete Redirect ports.
Redirect Port	RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.

Click **Apply** to implement the changes. To return to the RSPAN Settings window, click the [Show All RSPAN Table](#) link.

To modify an existing entry of its source settings, click the corresponding **Modify** button in Modify Source, revealing the following window to configure:

Figure 2 - 101 RSPAN Settings – Edit Source window

The following fields can be configured:

Parameter	Description
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN which will

	modify the RSPAN Entries.
VID (1-4094)	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN which will to modify the RSPAN Entries.
Mirror Group ID (1-4)	Tick the check box and enter a group ID which mirror session is used for RSPAN source function.
Target Port	The target port that receives the packets duplicated at the source port.
Source Ports Action	Use the pull-down menu to select add, or delete a source port. Select <i>Source</i> to display the source port only.
RX Source Ports	The goal of RX source ports is to monitor as much as possible all the packets received by the source interface or VLAN before any modification or processing is performed by the switch. A copy of each packet received by the source is sent to the destination port for that RSPAN session.
TX Source Ports	The goal of TX source ports is to monitor as much as possible all the packets sent by the source interface after all modification and processing is performed by the switch.

DNS Relay

Computer users usually prefer to use text names for computers for which they may want to open a connection. Computers themselves, require 32 bit IP addresses. Somewhere, a database of network devices' text names and their corresponding IP addresses must be maintained.

The Domain Name System (DNS) is used to map names to IP addresses throughout the Internet and has been adapted for use within intranets.

For two DNS servers to communicate across different subnets, the DNS Relay of the Switch must be used. The DNS servers are identified by IP addresses.

Mapping Domain Names to Addresses

Name-to-address translation is performed by a program called a Name server. The client program is called a Name resolver. A Name resolver may need to contact several Name servers to translate a name to an address.

The Domain Name System (DNS) servers are organized in a somewhat hierarchical fashion. A single server often holds names for a single network, which is connected to a root DNS server - usually maintained by an ISP.

Domain Name Resolution

The domain name system can be used by contacting the name servers one at a time, or by asking the domain name system to do the complete name translation. The client makes a query containing the name, the type of answer required, and a code specifying whether the domain name system should do the entire name translation, or simply return the address of the next DNS server if the server receiving the query cannot resolve the name.

When a DNS server receives a query, it checks to see if the name is in its sub domain. If it is, the server translates the name and appends the answer to the query, and sends it back to the client. If the DNS server cannot translate the name, it determines what type of name resolution the client requested. A complete translation is called recursive resolution and requires the server to contact other DNS servers until the name is resolved. Iterative resolution specifies that if the DNS server cannot supply an answer, it returns the address of the next DNS server the client should contact.

Each client must be able to contact at least one DNS server, and each DNS server must be able to contact at least one root server.

The address of the machine that supplies domain name service is often supplied by a DHCP or BOOTP server, or can be entered manually and configured into the operating system at startup.

DNS Relay Global Settings

To view this window, click **Administration > DNS Relay > DNS Relay Global Settings**, as shown below.

DNS Relay Global Settings	
DNS State	Disabled ▾
Primary Name Server	0.0.0.0
Secondary Name Server	0.0.0.0
DNSR Cache State	Disabled ▾
DNSR Static Table State	Disabled ▾
Apply	

Figure 2 - 102 DNS Relay Global Settings window

The following fields can be set:

Parameter	Description
DNS State	This field can be toggled between <i>Disabled</i> and <i>Enabled</i> using the pull-down menu, and is used to enable or disable the DNS Relay service on the Switch.
Primary Name Server	Allows the entry of the IP address of a primary domain name server (DNS).
Secondary Name Server	Allows the entry of the IP address of a secondary domain name server (DNS).
DNSR Cache Status	This can be toggled between <i>Disabled</i> and <i>Enabled</i> . This determines if a DNS cache will be enabled on the Switch.
DNSR Static Table State	This field can be toggled using the pull-down menu between <i>Disabled</i> and <i>Enabled</i> . This determines if the static DNS table will be used or not.


Click **Apply** to implement changes made.

DNS Relay Static Settings

To view this window, click **Administration > DNS Relay > DNS Relay Static Settings**, as shown below.

DNS Relay Static Settings		
Domain Name	IP Address	Apply
<input type="text"/>	0.0.0.0	Add
Total Entries: 0		
DNS Relay Static Table		
Domain Name	IP Address	Delete

Figure 2 - 103 DNS Relay Static Settings window

To add an entry into the DNS Relay Static Table, simply enter a Domain Name with its corresponding IP address and click **Add** under the Apply heading. A successful entry will be presented in the table below, as shown in the example above. To erase an entry from the table, click its corresponding  under the Delete heading.

DNS Resolver

The DNS Resolver provides a solution to translate the domain name to an IP address for application on the switch itself.

DNS Resolver Global Settings

This window is used to configure the DNS resolver state and name server timeout.

To view this window, click **Administration > DNS Resolver > DNS Resolver Global Settings**, as shown below.

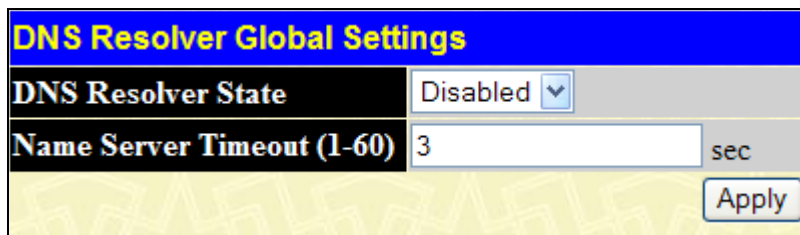


Figure 2 - 104 DNS Resolver Global Settings window

The following fields can be set:

Parameter	Description
DNS Resolver State	Use the pull-down menu to enable or disable the DNS resolver on the Switch. The default is <i>Disabled</i> .
Name Server Timeout (1-60)	Enter the maximum time waiting for a response from a specified name server. The range is 1 to 60 seconds. The default value is 3.

Click **Apply** to implement changes made.


DNS Resolver Static Name Server Settings

When adding a name server, if one primary name server exists in the static name server table and a new primary name server is added, the existing primary name server will be changed to a normal name server. If the added primary name server's IP address is the same as an existing normal name server's IP address, the existing normal name server will be changed to a primary name server, but won't add new name server. When no primary name server is specified, the first configured name server will automatically change to become the primary name server. If the deleted name server's IP address is the same as one of the existing name servers' IP addresses, regardless of whether a normal name server or primary name server, the name server will be deleted.

To view this window, click **Administration > DNS Resolver > DNS Resolver Static Name Server Settings**, as shown below.



Figure 2 - 105 DNS Resolver Static Name Server Table window

To remove an entry from the table, click its corresponding  under the Delete heading.

Click **Add** to reveal the following window to configure:

Figure 2 - 106 DNS Resolver Static Name Server Settings window

The following fields can be set:

Parameter	Description
Primary	Tick the check box to indicate the name server is a primary name server.
IP Address	Enter the DNS resolver name server IP address.

Click **Apply** to implement changes made.

DNS Resolver Dynamic Name Server Table

This read-only window is used to display the DNS resolver dynamic name server table.

To view this window, click **Administration > DNS Resolver > DNS Resolver Dynamic Name Server Table**, as shown below.


Figure 2 - 107 DNS Resolver Dynamic Name Server Table window

DNS Resolver Static Host Name Settings

This window is used to create or delete a static host name entry of the Switch. If the created host name entry exists in the dynamic host name table, the existing dynamic host name entry will be deleted, and the created host name entry is then added into the static host name table and a log for a duplicate is recorded.

To view this window, click **Administration > DNS Resolver > DNS Resolver Static Host Name Settings**, as shown below.

Figure 2 - 108 DNS Resolver Static Host Name Table window

To remove an entry from the table, click its corresponding  under the Delete heading.

Click **Add** to reveal the following window to configure:

Figure 2 - 109 DNS Resolver Static Host Name Settings window

The following fields can be set:

Parameter	Description
Host Name	Enter the host's host name.
IP Address	Enter the host's IP address.

Click **Apply** to implement changes made.


DNS Resolver Dynamic Host Name Table

This window is used to display or delete entries on the DNS Resolver Dynamic Host Name Table.

To view this window, click **Administration > DNS Resolver > DNS Resolver Dynamic Host Name Table**, as shown below.

Total Entries: 0			
DNS Resolver Dynamic Host Name Table			
Host Name	IP Address	TTL	Delete

Figure 2 - 110 DNS Resolver Dynamic Host Name Table window

To remove an entry from the table, click its corresponding  under the Delete heading.

SNMP Manager

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the Switch, switch group or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The Switch supports the SNMP versions 1, 2c, and 3. The default SNMP setting is disabled. You must enable SNMP. Once SNMP is enabled you can choose which version you want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v.1 and v.2, user authentication is accomplished using 'community strings', which function like passwords. The remote user SNMP application and the Switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored (dropped).

The default community strings for the Switch used for SNMP v.1 and v.2 management access are:

- **public** – Allows authorized management stations to retrieve MIB objects.
- **private** – Allows authorized management stations to retrieve and modify MIB objects.

SNMPv3 uses a more sophisticated authentication process that is separated into two parts. The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers. The second part describes what each user on that list can do as an SNMP manager.

The Switch allows groups of users to be listed and configured with a shared set of privileges. The SNMP version may also be set for a listed group of SNMP managers. Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMPv1 while assigning a higher level of security to another group, granting read/write privileges using SNMPv3.

Using SNMPv3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions. The functions allowed or restricted are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMPv3 in that SNMP messages may be encrypted. To read more about how to configure SNMPv3 settings for the Switch read the next section.

Traps

Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Switch generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast\Multicast Storm.

MIBs

The Switch in the Management Information Base (MIB) stores management and counter information. The Switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the Switch also supports its own proprietary enterprise MIB as an extended Management Information Base. Specifying the MIB Object Identifier may also retrieve the proprietary MIB. MIB values can be either read-only or read-write.

The Switch incorporates a flexible SNMP management for the switching environment. SNMP management can be customized to suit the needs of the networks and the preferences of the network administrator. Use the SNMP V3 menus to select the SNMP version used for specific tasks.

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. The administrator can specify the SNMP version used to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device.

SNMP settings are configured using the menus located on the SNMP V3 folder of the web manager. Workstations on the network that are allowed SNMP privileged access to the Switch can be restricted with the Management Station IP Address menu.

SNMP Trap Settings

The following window is used to enable and disable trap settings for the SNMP function on the Switch.

To view this window for configuration, click **Administration > SNMP Manager > SNMP Trap Settings**, as shown below.

SNMP Traps Settings

Traps State	Enabled
Authenticate Trap State	Enabled
Linkchange Trap State	Enabled

Apply

Linkchange Trap Settings

Unit	From	To	State	Apply
1	Port 1	Port 1	Enabled	Apply

Linkchange Trap Table

Port	State
1	Enabled
2	Enabled
3	Enabled
4	Enabled
5	Enabled
6	Enabled
7	Enabled
8	Enabled
9	Enabled
10	Enabled
11	Enabled
12	Enabled
13	Enabled
14	Enabled
15	Enabled
16	Enabled
17	Enabled
18	Enabled
19	Enabled
20	Enabled
21	Enabled
22	Enabled
23	Enabled
24	Enabled

Figure 2 - 111 SNMP Trap Settings window

To enable or disable the Traps State, Authenticate Trap State, and/or Linkchange Trap State use the corresponding pull-down menu to change and click **Apply**.

To enable or disable linkchange trap settings for individual ports, select the ports using the From and To drop-down menus, enable the State using the drop-down menu, and then click **Apply**.

SNMP User Table

This window displays all of the SNMP users currently configured on the Switch.

To view this window, click **Administration > SNMP Manager > SNMP User Table**, as shown below.

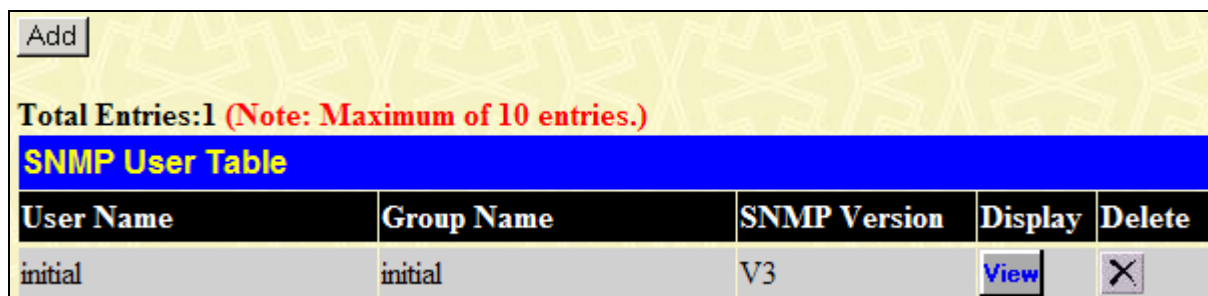



Figure 2 - 112 SNMP User Table window

To delete an existing **SNMP User Table** entry, click the  below the Delete heading corresponding to the entry you wish to delete.

To display the detailed entry for a given user, click the **View** button under the Display heading. This will open the **SNMP User Table Display** window, as shown below.

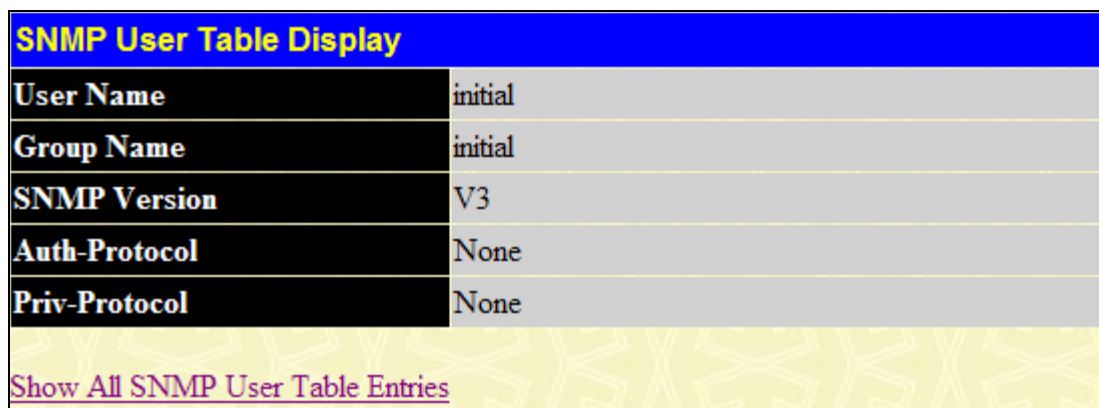


Figure 2 - 113 SNMP User Table - View window

The following parameters are displayed:

Parameter	Description
User Name	An alphanumeric string of up to 32 characters. This is used to identify the SNMP users.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	V3 – Indicates that SNMP version 3 is in use.
Auth-Protocol	<i>None</i> – Indicates that no authentication protocol is in use. <i>MD5</i> – Indicates that the HMAC-MD5-96 authentication level will be used. <i>SHA</i> – Indicates that the HMAC-SHA authentication protocol will be used.
Priv-Protocol	<i>None</i> – Indicates that no privacy (encryption) protocol is in use. <i>DES</i> – Indicates that DES 56-bit encryption is in use based on the CBC-DES (DES-56) standard.

To return to the SNMP User Table, click the [Show All SNMP User Table Entries](#) link.

To add a new entry to the SNMP User Table, click the **Add** button on the **SNMP User Table** window. This will open the **SNMP User Table Configuration** window, as shown below.

The image shows a web-based configuration window titled "SNMP User Table Configuration". It contains several fields and dropdown menus for configuring an SNMP user. The fields are: User Name (text input), Group Name (text input), SNMP Version (dropdown menu with "V3" selected), SNMP V3 Encryption (dropdown menu with "None" selected), Auth-Protocol by Password (dropdown menu with "MD5" selected, followed by a "Password" label and a text input field), Priv-Protocol by Password (dropdown menu with "None" selected, followed by a "Password" label and a text input field), Auth-Protocol by Key (dropdown menu with "MD5" selected, followed by a "Key" label and a text input field), and Priv-Protocol by key (dropdown menu with "None" selected, followed by a "Key" label and a text input field). At the bottom right, there is an "Apply" button. At the bottom left, there is a link that says "Show All SNMP User Table Entries".

Figure 2 - 114 SNMP User Table - Add window

The following parameters can be configured:

Parameter	Description
User Name	Enter an alphanumeric string of up to 32 characters. This is used to identify the SNMP user.
Group Name	This name is used to specify the SNMP group created can request SNMP messages.
SNMP Version	V3 – Specifies that SNMP version 3 will be used.
SNMP V3 Encryption	SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. Use the drop down menu to select the type of SNMP V3 encryption to be applied. The user can choose between <i>None</i> , <i>Password</i> or <i>Key</i> .
Auth-Protocol by Password / Key	<p><i>MD5</i> – Specifies that the HMAC-MD5-96 authentication level will be used. This is only operable when <i>V3</i> is selected in the SNMP Version field and the Encrypted check box has been ticked. This field will require the user to enter a password.</p> <p><i>SHA</i> – Specifies that the HMAC-SHA authentication protocol will be used. This is only operable when <i>V3</i> is selected in the SNMP Version field and the Encrypted check box has been ticked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.</p>
Priv-Protocol by Password / Key	<p><i>None</i> – Specifies that no privacy (encryption) protocol is in use.</p> <p><i>DES</i> – Specifies that DES 56-bit encryption is in use, based on the CBC-DES (DES-56) standard. This field is only operable when <i>V3</i> is selected in the SNMP Version field and the Encrypted check box has been ticked. This field will require the user to enter a password between 8 and 16 alphanumeric characters.</p>

To implement changes made, click **Apply**. To return to the SNMP User Table, click the [Show All SNMP User Table Entries](#) link.

SNMP View Table

This window is used to assign views to community strings that define which MIB objects can be accessed by a remote SNMP manager.

To view this window, click **Administration > SNMP Manager > SNMP View Table**, as shown below.

Add			
Total Entries:8 (Note: Maximum of 30 entries.)			
SNMP View Table			
View Name	Subtree	View Type	Delete
restricted	1.3.6.1.2.1.1	Included	X
restricted	1.3.6.1.2.1.11	Included	X
restricted	1.3.6.1.6.3.10.2.1	Included	X
restricted	1.3.6.1.6.3.11.2.1	Included	X
restricted	1.3.6.1.6.3.15.1.1	Included	X
CommunityView	1	Included	X
CommunityView	1.3.6.1.6.3	Excluded	X
CommunityView	1.3.6.1.6.3.1	Included	X

Figure 2 - 115 SNMP View Table window

To delete an existing SNMP View Table entry, click the corresponding button in the Delete column. To create a new entry, click the **Add** button which will reveal a new window.

SNMP View Table Configuration	
View Name	<input type="text"/>
Subtree OID	<input type="text"/>
View Type	Included <input type="button" value="v"/>
<input type="button" value="Apply"/>	
Show All SNMP View Table Entries	

Figure 2 - 116 SNMP View Table Configuration window

The SNMP View created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous window.

The following parameters can be configured:

Parameter	Description
View Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP view being created.
Subtree OID	Type the Object Identifier (OID) Subtree for the view. The OID identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager.
View Type	Select <i>Included</i> to ensure this object is included in the list of objects that an SNMP manager

can access. Select *Excluded* to exclude this object from the list of objects that an SNMP manager can access.

To implement your new settings, click **Apply**. To return to the **SNMP View Table** window, click the [Show All SNMP View Table Entries](#) link.

SNMP Group Table

An SNMP Group created with this table maps SNMP users (identified in the SNMP User Table) to the views created in the previous menu.

To view this window, click **Administration > SNMP Manager > SNMP Group Table**, as shown below.

SNMP Group Table				
Group Name	Security Model	Security Level	Display	Delete
public	SNMPv1	NoAuthNoPriv	View	<input type="checkbox"/>
public	SNMPv2	NoAuthNoPriv	View	<input type="checkbox"/>
initial	SNMPv3	NoAuthNoPriv	View	<input type="checkbox"/>
private	SNMPv1	NoAuthNoPriv	View	<input type="checkbox"/>
private	SNMPv2	NoAuthNoPriv	View	<input type="checkbox"/>
ReadGroup	SNMPv1	NoAuthNoPriv	View	<input type="checkbox"/>
ReadGroup	SNMPv2	NoAuthNoPriv	View	<input type="checkbox"/>
WriteGroup	SNMPv1	NoAuthNoPriv	View	<input type="checkbox"/>
WriteGroup	SNMPv2	NoAuthNoPriv	View	<input type="checkbox"/>

Figure 2 - 117 SNMP Group Table window

To delete an existing SNMP Group Table entry, click the corresponding under the Delete heading.

To display the current settings for an existing **SNMP Group Table** entry, click the **View** button located under the Display heading, which will show the following window.

SNMP Group Table Display	
Group Name	public
Read View Name	CommunityView
Write View Name	
Notify View Name	CommunityView
Security Model	SNMPv1
Security Level	NoAuthNoPriv

[Show All SNMP Group Table Entries](#)

Figure 2 - 118 SNMP Group Table Display window

To add a new entry to the Switch's SNMP Group Table, click the **Add** button in the upper left-hand corner of the **SNMP Group Table** window. This will open the **SNMP Group Table Configuration** window, as shown below.

The image shows a configuration window titled "SNMP Group Table Configuration". It contains several input fields and dropdown menus. The fields are: "Group Name", "Read View Name", "Write View Name", and "Notify View Name", each with a text input box. The "Security Model" field has a dropdown menu currently set to "SNMPv1". The "Security Level" field has a dropdown menu currently set to "NoAuthNoPriv". At the bottom right of the configuration area is an "Apply" button. Below the configuration area is a link that says "Show All SNMP Group Table Entries".

Figure 2 - 119 SNMP Group Table Configuration window

The following parameters can be configured:

Parameter	Description
Group Name	Type an alphanumeric string of up to 32 characters. This is used to identify the new SNMP group of SNMP users.
Read View Name	This name is used to specify the SNMP group created can request SNMP messages.
Write View Name	Specify a SNMP group name for users that are allowed SNMP write privileges to the Switch's SNMP agent.
Notify View Name	Specify a SNMP group name for users that can receive SNMP trap messages generated by the Switch's SNMP agent.
Security Model	<p><i>SNMPv1</i> – Specifies that SNMP version 1 will be used.</p> <p><i>SNMPv2</i> – Specifies that SNMP version 2c will be used. The SNMPv2 supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features.</p> <p><i>SNMPv3</i> – Specifies that the SNMP version 3 will be used. SNMPv3 provides secure access to devices through a combination of authentication and encrypting packets over the network.</p>
Security Level	<p>The Security Level settings only apply to SNMPv3.</p> <p><i>NoAuthNoPriv</i> – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthNoPriv</i> – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager.</p> <p><i>AuthPriv</i> – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted.</p>

To implement your new settings, click **Apply**. To return to the SNMP Group Table, click the [Show All SNMP Group Table Entries](#) link.

SNMP Community Table

Use this table to create an SNMP community string to define the relationship between the SNMP manager and an agent. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string:

- An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent.
- Any MIB view that defines the subset of all MIB objects will be accessible to the SNMP community.

- Read/write or read-only level permission for the MIB objects accessible to the SNMP community.

To view this window, click **Administration > SNMP Manager > SNMP Community Table**, as shown below.

SNMP Community Table			
Community Name	View Name	Access Right	
<input type="text"/>	<input type="text"/>	Read Only	
<input type="button" value="Apply"/>			
Total Entries:2 (Note: Maximum of 10 entries.)			
SNMP Community Table			
Community Name	View Name	Access Right	Delete
private	CommunityView	Read Write	<input type="button" value="X"/>
public	CommunityView	Read Only	<input type="button" value="X"/>

Figure 2 - 120 SNMP Community Table window

The following parameters can be configured:

Parameter	Description
Community Name	Type an alphanumeric string of up to 32 characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
View Name	Type an alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. The view name must exist in the SNMP View Table.
Access Right	<i>Read Only</i> – Specifies that SNMP community members using the community string created can only read the contents of the MIBs on the Switch. <i>Read Write</i> – Specifies that SNMP community members using the community string created can read from, and write to the contents of the MIBs on the Switch.

To implement the new settings, click **Apply**. To delete an entry from the SNMP Community Table, click the corresponding button under the Delete heading.

SNMP Host Table

Use this window to set up SNMP trap recipients. To delete an existing SNMP Host Table entry, click the corresponding button under the Delete heading.

To view this window, click **Administration > SNMP Manager > SNMP Host Table**, as shown below.

<input type="button" value="Add IPv4 Host"/>		<input type="button" value="Add IPv6 Host"/>	
Total Entries:0 (Note: Maximum of 10 entries.)			
SNMP Host Table			
Host IP Address	SNMP Version	Community Name/SNMPv3 User Name	Delete

Figure 2 - 121 SNMP Host Table window

Users now have the choice of adding an IPv4 or an IPv6 host to the SNMP host table. To add a new IPv4 entry to the Switch's SNMP Host Table, click the **Add IPv4 Host** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown below.

Figure 2 - 122 SNMP Host Table - Add IPv4 Host window

The following parameters can be configured:

Parameter	Description
Host IPv4 Address	Type the IPv4 address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	<p>V1 – This specifies that SNMP version 1 will be used.</p> <p>V2 – To specify that SNMP version 2 will be used.</p> <p>V3-NoAuth-NoPriv – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.</p> <p>V3-Auth-NoPriv – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.</p> <p>V3-Auth-Priv – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.</p>
Community String / SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

Click **Apply** to implement the changes. To return to the SNMP Host Table window, click the [Show All SNMP Host Table Entries](#) link.

To add a new IPv6 entry to the Switch's SNMP Host Table, click the **Add IPv6 Host** button in the upper left-hand corner of the window. This will open the **SNMP Host Table Configuration** window, as shown below.

Figure 2 - 123 SNMP Host Table - Add IPv6 Host window

The following parameters can be configured:

Parameter	Description
Host IPv6 Address	Type the IPv6 address of the remote management station that will serve as the SNMP host for the Switch.
SNMP Version	V1 – To specifies that SNMP version 1 will be used.

	<p>V2 – To specify that SNMP version 2 will be used.</p> <p>V3-NoAuth-NoPriv – To specify that the SNMP version 3 will be used, with a NoAuth-NoPriv security level.</p> <p>V3-Auth-NoPriv – To specify that the SNMP version 3 will be used, with an Auth-NoPriv security level.</p> <p>V3-Auth-Priv – To specify that the SNMP version 3 will be used, with an Auth-Priv security level.</p>
Community String / SNMP V3 User Name	Type in the community string or SNMP V3 user name as appropriate.

To implement your new settings, click **Apply**. To return to the SNMP Host Table window, click the [Show All SNMP Host Table Entries](#) link.

SNMP Engine ID

The Engine ID is a unique identifier used for SNMP V3 implementations. This is an alphanumeric string used to identify the SNMP engine on the Switch.

To view this window, click **Administration > SNMP Manager > SNMP Engine ID**, as shown below.

Figure 2 - 124 SNMP Engine ID window

To change the Engine ID, enter the new Engine ID in the space provided and click the **Apply** button.

Trap Source Interface Settings

This window is used to configure the trap source interface settings.

To view this window, click **Administration > Trap Source Interface Settings**, as shown below.

Figure 2 - 125 Trap Source Interface Settings window

The following parameters can be configured:

Parameter	Description
Interface Name	Enter a name of the interface.
IPv4 Address	Tick the check box and enter an IPv4 address.

IPv6 Address	Tick the check box and enter an IPv6 address.
---------------------	---

Click Apply to implement the changes. To remove an entry, click the corresponding  button.

PoE

The DGS-3426P switch supports Power over Ethernet (PoE) as defined by the IEEE 802.3af. Ports 1-24 can supply about 48 VDC power to Powered Devices (PDs) over Category 5 or Category 5E UTP Ethernet cables. The DGS-3426P follows the standard PSE (Power Sourcing Equipment) pinout *Alternative A*, whereby power is sent out over pins 1, 2, 3 and 6. The DGS-3426P works with all D-Link 802.3af capable devices.

The DGS-3426P includes the following PoE features:

Auto-discovery recognizes the connection of a PD (Powered Device) and automatically sends power to it.

The Auto-disable feature occurs under two conditions: first, if the total power consumption exceeds the system power limit; and second, if the per port power consumption exceeds the per port power limit.

Active circuit protection automatically disables the port if there is a short. Other ports will remain active.

Based on 802.3af/at PDs receive power according to the following classification:

Class	Maximum power available to PD
0	12.95W
1	3.84W
2	6.49W
3	12.95W

PSE provides power according to the following classification:

Class	Max power used by PSE
0	15.4W
1	4.0W
2	7.0W
3	15.4W
User define	16.8W

To configure the PoE features on the DGS-3426P, click **Administration > PoE**. The **PoE System Settings** window is used to assign a power limit and power disconnect method for the whole PoE system. To configure the **Power Limit** for the PoE system, enter a value between 37W and 370W for the DGS-3426P in the Power Limit field. The default setting is 370W. When the total consumed power exceeds the power limit, the PoE controller (located in the PSE) disconnects the power to prevent overloading the power supply.

PoE System Settings

This window is used to configure PoE settings on the Switch.

To view this window, click **Administration > PoE > PoE System Settings**, as shown below.

PoE System Settings						
Unit	1					
Power Limit (37-370W)	370					
Disconnect Method	Deny Next Port					
Management Mode	Power Limit					
Legacy PD	Disabled					
Apply						
PoE System Information						
Box ID	Power Limit	Power Consumption	Power Remained	Disconnection Method	Management Mode	Legacy PD
1	370	0	370	Deny Next Port	Power Limit	Disabled
<p>If Power Disconnection Method is set to deny next port, then the system can not utilize out of its maximum power capacity. The unused watt is 19W.</p>						

Figure 2 - 126 PoE System Settings window

The following parameters can be configured:

Parameter	Description
Unit	Choose the switch in the switch stack for which to configure the PoE settings. Users should note that not all switches in the xStack® DGS-3400 Series support PoE yet, when they are configured in a stack, the Primary Master switch will display the PoE settings to be configured for the stack, whether or not the Switch is a PoE supported device. However, only PoE supported switches have the PoE capability in the switch stack.
Power Limit (37-370W)	Sets the limit of power to be used from the Switch's power source to PoE ports. The user may configure a Power Limit between 37 and 370W for the DGS-3426P. The default setting is 370W.
Disconnect Method	The PoE controller uses either <i>Deny next port</i> or <i>Deny low priority port</i> to offset the power limit being exceeded and keep the Switch's power at a usable level. Use the drop-down menu to select a Disconnect Method. The default for the Power Disconnect Method is <i>Deny next port</i> . Both Power Disconnection Methods are described below: <i>Deny next port</i> – After the power limit has been exceeded, the next port attempting to power up is denied, regardless of its priority. <i>Deny low priority port</i> – After the power limit has been exceeded, the next port attempting to power up causes the port with the lowest priority to shut down to allow the high-priority and critical priority ports to power up.
Management Mode	Use the drop-down menu to select the management mode. <i>Power Limit</i> – Specifies that the previously set power limit will be implemented. <i>Auto</i> – Specifies that system will automatically determine the management mode.
Legacy PD	Use the drop-down menu to enable or disable detecting legacy PDs signal.

Click **Apply** to implement the changes.

PoE Port Settings

This window is used to configure the PoE port settings on the Switch.

To view this window, click **Administration > PoE > PoE Port Settings**:

PoE Port Settings									
Unit	From	To	State	Priority	Power Limit			Apply	
1	Port 1	Port 1	Enabled	Low	Class_0	User Define	<input checked="" type="checkbox"/>	15400	Apply

PoE Port Table								
Port	State	Class	Priority	Power (mW)	Power Limit(mW)	Voltage (Decivolt)	Current (mA)	Status
1	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
2	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
3	Enabled	0	Low	0	15400(User Define)	0	0	OFF: No standard PD connected
4	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
5	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
6	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
7	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
8	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
9	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
10	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
11	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
12	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
13	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
14	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
15	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
16	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
17	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
18	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
19	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
20	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
21	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
22	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
23	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection
24	Enabled	0	Low	0	15400(User Define)	0	0	OFF: Interim state during line detection

*: When system's management mode is auto, the power limit will not take effect.

Figure 2 - 127 PoE Port Settings window

The following parameters can be configured:

Parameter	Description
Unit	Choose the switch in the switch stack for which to configure the PoE settings. Users should note that not all switches in the xStack® DGS-3400 series support PoE yet, when they are configured in a stack, the Primary Master switch will display the PoE settings to be configured for the stack, whether or not the Switch is a PoE supported device. However, only PoE supported switches have the PoE capability in the switch stack.
From /To	Select a range of ports from the pull-down menus to be enabled or disabled for PoE.
State	Use the pull-down menu to enable or disable ports for PoE.

Priority	<p>Use the pull-down menu to select the priority of the PoE ports. Port priority determines the priority which the system attempts to supply the power to the ports. There are three levels of priority that can be selected, <i>Critical</i>, <i>High</i>, and <i>Low</i>. When multiple ports happen to have the same level of priority, the port ID will be used to determine the priority. The lower port ID has higher priority. The setting of priority will affect the ordering of supplying power. Whether the disconnect method is set to deny low priority port, the priority of each port will be used by the system to manage the supply of power to ports.</p>
Power Limit	<p>This function is used to configure the per-port power limit. If a port exceeds its power limit, it will shut down.</p> <p>Based on 802.3af/802.3at, there are different PD classes and power consumption ranges;</p> <p>Class 0 – 0.44~12.95W Class 1 – 0.44~3.84W Class 2 – 3.84~6.49W Class 3 – 6.49~12.95W</p> <p>The following is the power limit applied to the port for these four classes. For each class, the power limit is a little more than the power consumption range for that class. This takes into account any power loss on the cable. Thus, the following are the typical values;</p> <p>Class 0 : 15400mW Class 1 : 4000mW Class 2 : 7000mW Class 3 : 15400mW User define: 16800mW</p> <p>As well as these four pre-defined settings, users can directly specify any value ranging from 1000mW to 16800mW.</p>

Click **Apply** to implement the changes. The port status of all PoE configured ports is displayed in the PoE Port Table.

sFlow

sFlow is a feature on the Switch that allows users to monitor network traffic running through the switch to identify network problems through packet sampling and packet counter information of the Switch. The Switch itself is the sFlow agent where packet data is retrieved and sent to an sFlow Analyzer where it can be scrutinized and utilized to resolve the problem.

The Switch can configure the settings for the sFlow Analyzer but the remote sFlow Analyzer device must have an sFlow utility running on it to retrieve and analyze the data it receives from the sFlow agent.

The Switch itself will collect three types of packet data:

1. It will take sample packets from the normal running traffic of the Switch based on a sampling interval configured by the user.
2. The Switch will take a poll of the IF counters located on the switch.
3. The Switch will also take a part of the packet header. The length of the packet header can also be determined by the user.

Once this information has been gathered by the switch, it is packaged into a packet called an sFlow datagram, which is then sent to the sFlow Analyzer for analysis.

For a better understanding of the sFlow feature of this Switch, refer to the adjacent diagram.

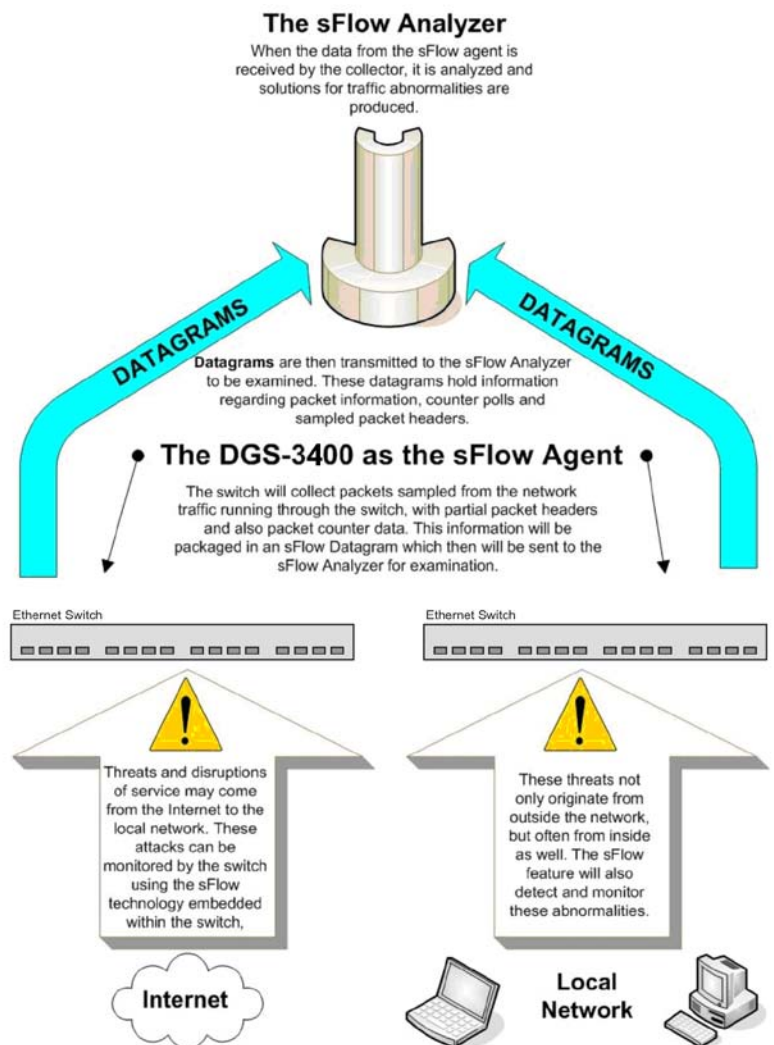


Figure 2 - 128 sFlow Basic Setup

sFlow Global Settings

The following window is used to globally enable the sFlow feature for the Switch. Simply use the pull-down menu and click **Apply** to enable or disable sFlow. This window will also display the sFlow version currently being utilized by the Switch, along with the sFlow Address that is the Switch's IP address.

To view this window, click **Administration > sFlow > sFlow Global Settings**, as shown below.

Figure 2 - 129 sFlow Global Settings window

The following parameters can be configured or viewed:

Parameter	Description
sFlow State	This field allows you to globally enable or disable sFlow.
sFlow Version	This displays the current sFlow version.
sFlow IPv4 Address	This displays the sFlow IPv4 address.
sFlow IPv6 Address	This displays the sFlow IPv6 address.

Click **Apply** to implement the changes.

sFlow Analyzer Settings

The following windows are used to configure the parameters for the remote sFlow Analyzer (collector) that will be used to gather and analyze sFlow Datagrams that originate from the Switch. Users must have the proper sFlow software set on the Analyzer in order to receive datagrams from the switch to be analyzed, and to analyze these datagrams. Users may specify up to four unique analyzers to receive datagrams, yet the virtual port used must be unique to each entry.


To view this window, click **Administration > sFlow > sFlow Analyzer Settings**, as shown below.

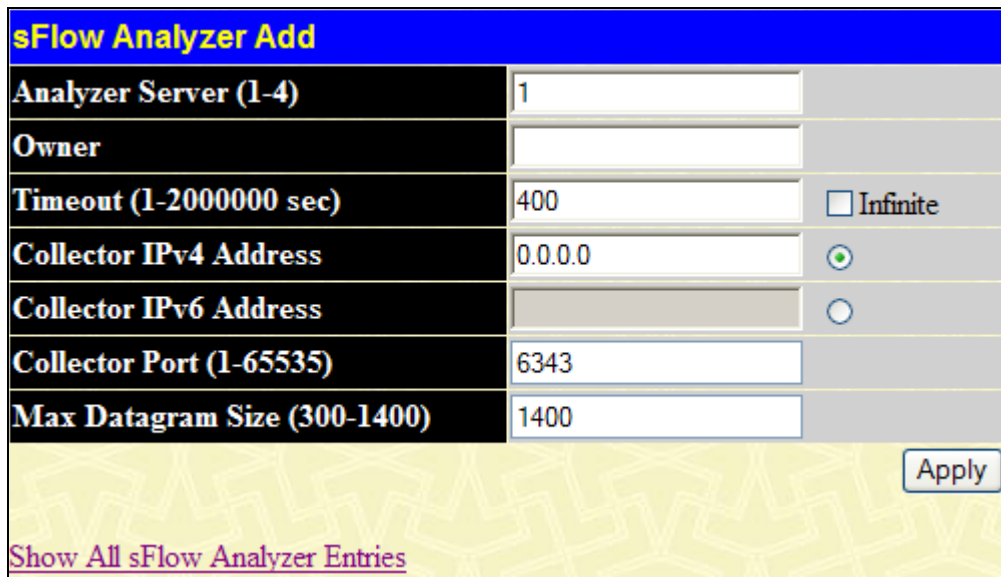
Figure 2 - 130 sFlow Analyzer Settings window

The following fields are displayed:

Parameter	Description
Server ID	This field denotes the ID of the Analyzer Server that has been added to the sFlow settings. Up to four entries can be added with the same UDP port.

Owner	Displays the owner of the entry made here. The user that added this sFlow Analyzer configured this name.
Timeout (sec)	Displays the configured time, in seconds, after which the Analyzer server will time out. When the server times out, all sFlow samples and counter polls associated with this server will be deleted.
Countdown Time	Displays the current time remaining before this Analyzer server times out. When the server times out, all sFlow samples and counter polls associated with this server will be deleted.
Collector Address	Displays the IP address of the sFlow Analyzer Server. This IP address is where sFlow datagrams will be sent for analysis.
Collector Port	Displays the previously configured UDP port where sFlow datagrams will be sent for analysis.
Max Datagram Size	This field displays the maximum number of data bytes in a single sFlow datagram that will be sent to this sFlow Analyzer Server.
Modify	Click the Modify button to display the sFlow Counter Analyzer Edit window, so that users may edit the settings for this server.

To remove an entry, click the  button. To add a new sFlow Analyzer, click the **Add** button in the previous window that will display the following window to be configured:



The image shows a configuration window titled "sFlow Analyzer Add". It contains several input fields and checkboxes:

- Analyzer Server (1-4)**: Input field with value "1".
- Owner**: Empty input field.
- Timeout (1-2000000 sec)**: Input field with value "400" and a checkbox for "Infinite" which is unchecked.
- Collector IPv4 Address**: Input field with value "0.0.0.0" and a radio button which is selected.
- Collector IPv6 Address**: Input field (disabled) and a radio button which is unselected.
- Collector Port (1-65535)**: Input field with value "6343".
- Max Datagram Size (300-1400)**: Input field with value "1400".

At the bottom right is an "Apply" button. At the bottom left is a link: [Show All sFlow Analyzer Entries](#).

Figure 2 - 131 sFlow Analyzer Settings – Add window

To change an sFlow Analyzer, click the corresponding **Modify** button in the sFlow Analyzer Settings window that will display the following window to be configured:

Figure 2 - 132 sFlow Analyzer Settings – Edit window

The following fields can be configured or viewed:

Parameter	Description
Analyzer Server (1-4)	Enter an integer from 1 to 4 to denote the sFlow Analyzer to be added. Up to four entries can be added.
Owner	Users may enter an alphanumeric string of up to 16 characters to define the owner of this entry. Users are encouraged to give this field a name that will help them identify this entry. When an entry is made in this field, the following Timeout field is automatically set to 400 seconds, unless the user alters the Timeout field.
Timeout (1-2000000 sec)	This field is used to specify the timeout for the Analyzer Server. When the server times out, all sFlow samples and counter polls associated with this server will be deleted. The user may set a time between 1 and 2000000 seconds with a default setting of 400 seconds. <i>Infinite</i> can be selected to ensure that it never times out.
Collector IPv4 Address	Click the radio button and enter the IPv4 address of the sFlow Analyzer Server. If this field is not specified, the entry will become 0.0.0.0 and therefore the entry will be inactive. Users must set this field.
Collector IPv6 Address	Click the radio button and enter the IPv6 address of the sFlow Analyzer Server.
Collector Port (1-65535)	The destination UDP port where sFlow datagrams will be sent. The default setting for this field is 6343.
Max Datagram Size (300-1400)	This field will specify the maximum number of data bytes that can be packaged into a single sFlow datagram. Users may select a value between 300 and 1400 bytes with a default setting of 1400 bytes.

Click **Apply** to save the changes.

sFlow Sampler Settings

This window will allow users to configure the Switch’s settings for taking sample packets from the network, including the sampling rate and the amount of the packet header to be extracted.

To view this window, click **Administration > sFlow > sFlow Sampler Settings**, as shown below.

Add Clear All


sFlow Sampler Settings

Port	Analyzer Server ID	Configured RX Rate	Configured TX Rate	Active RX Rate	Active TX Rate	Max Header Size	Modify	Delete
Total Entries: 0								

Figure 2 - 133 sFlow Sampler Settings window

The following fields are displayed:

Parameter	Description
Port	Displays the port from which packet samples are being extracted.
Analyzer Server ID	Displays the ID of the Analyzer Server where datagrams, containing the packet sampling information taken using this sampling mechanism, will be sent.
Configured RX/TX Rate	Displays the configured rate of packet sampling for this port based on a multiple of 256. For example, if a figure of 20 is in this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port.
Active RX/TX Rate	Displays the current rate of packet sampling being performed by the Switch for this port, based on a multiple of 256. For example, if a figure of 20 is in this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port.
Max Header Size	Displays the number of leading bytes of the sampled packet header. This sampled header will be encapsulated with the datagram to be forwarded to the Analyzer Server.

To remove an entry, click the corresponding  button. Click the **Clear All** button to delete all entries.

To add a new sFlow Sampler entry, click the **Add** button which will display the following window to be configured:

sFlow Sampler Add

Unit: 1

From: Port 1

To: Port 1

Analyzer Server ID (1-4): 1

RX Rate (0-65535): 0

TX Rate (0-65535): 0

Max Header Size (18-256): 128

Apply

[Show All sFlow Sampler Entries](#)

Figure 2 - 134 sFlow Sampler Settings - Add window

To change an sFlow Sampler, click the corresponding **Modify** button in the sFlow Sampler Settings window that will display the following window to be configured:

Figure 2 - 135 sFlow Sampler Settings - Edit window

The following fields can be configured or viewed:

Parameter	Description
Unit	Select the unit you wish to configure.
From / To	Choose the beginning and ending range of ports to be configured for packet sampling.
Analyzer Server ID (1-4)	Enter the previously configured Analyzer Server ID to state the device that will be receiving datagrams from the Switch. These datagrams will include the sample packet information taken using the sampling mechanism configured here.
RX Rate (0-65535)	Enter the sampling rate of packet RX sampling here. The value entered here is to be multiplied by 256 to get the percentage of packets sampled. For example, if the user enters a figure of 20 into this field, the switch will sample one out of every 5120 packets (20 x 256 = 5120) that pass through the individual port. Users may enter a value between 1 and 65535. An entry of 0 disables the packet sampling. Since this is the default setting, users are reminded to configure a rate here, otherwise this function will not function.
TX Rate (0-65535)	Enter the sampling rate of packet TX sampling here. The configured rate value multiplied by 256 to get the percentage of packets sampled.
Max Header Size (18-256)	This field will set the number of leading bytes of the sampled packet header. This sampled header will be encapsulated with the datagram to be forwarded to the Analyzer Server. The user may set a value between 18 and 256 bytes. The default setting is 128 bytes.

Click **Apply** to implement the changes.

sFlow Poller Settings

The following windows will allow the user to configure the settings for the Switch's counter poller. This mechanism will take a poll of the IF counters of the Switch and then package them with the other previously mentioned data into a datagram which will be sent to the sFlow Analyzer Server for examination.

To view this window, click **Administration > sFlow > sFlow Poller Settings**, as shown below.

The screenshot shows a web interface window titled "sFlow Counter Poller Settings". At the top left, there are two buttons: "Add" and "Clear All". Below the title bar is a table with five columns: "Port", "Analyzer Server ID", "Polling Interval (sec)", "Modify", and "Delete". The table is currently empty. Below the table, it says "Total Entries: 0".

Figure 2 - 136 sFlow Counter Poller Settings window

The following fields are displayed:

Parameter	Description
Port	Displays the port from which packet counter samples are being taken.
Analyzer Server ID	Displays the ID of the Analyzer Server where datagrams, containing the packet counter polling information taken using this polling mechanism, will be sent.
Polling Interval (sec)	The Polling Interval displayed here, is measured in seconds and will take a poll of the IF counters for the corresponding port, every time the interval reaches 0 seconds.

To remove an entry, click the corresponding button. Click the **Clear All** button to delete all entries.

To add a new sFlow Counter Poller setting, click the **Add** button which will display the following window to be configured.

The screenshot shows a web interface window titled "sFlow Counter Poller Add". It contains several configuration fields:

- Unit:** A dropdown menu with "1" selected.
- From:** A dropdown menu with "Port 1" selected.
- To:** A dropdown menu with "Port 1" selected.
- Analyzer Server ID (1-4):** An empty text input field.
- Polling Interval (20-120 sec):** A text input field followed by a checked checkbox and the label "Disabled".

 At the bottom right, there is an "Apply" button. At the bottom left, there is a link that says "Show All sFlow Counter Poller Entries".

Figure 2 - 137 sFlow Counter Poller Settings - Add window

To change an sFlow Counter Poller, click the corresponding **Modify** button in the sFlow Counter Poller Settings window that will display the following window to be configured:

The screenshot shows the 'sFlow Counter Poller Edit' window. It contains the following fields and values:

- Unit:** 1
- From:** Port 1
- To:** Port 1
- Analyzer Server ID (1-4):** 1
- Polling Interval (20-120 sec):** [Empty field] with a checked 'Disabled' checkbox.

At the bottom right is an 'Apply' button. At the bottom left is a link: [Show All sFlow Counter Poller Entries](#).

Figure 2 - 138 sFlow Counter Poller Settings - Edit window

The following parameters can be configured or viewed:

Parameter	Description
Unit	Select the unit you wish to configure.
From / To	Choose the beginning and ending range of ports to be configured for counter polling.
Analyzer Server ID (1-4)	Enter the previously configured Analyzer Server ID to state the device that will be receiving datagrams from the Switch. These datagrams will include the counter poller information taken using the polling mechanism configured here.
Polling Interval (20-120 sec)	Users may configure the Polling Interval here. The switch will take a poll of the IF counters every time this interval reaches 0, and this information will be included in the sFlow datagrams that will be sent to the sFlow Analyzer for examination. Ticking the Disabled check box will disable the counter polling for this entry.

Click **Apply** to implement the changes.

IP Multicast VLAN Replication

The following windows allow the user to configure the settings for IP Multicast VLAN Replication on the Switch.

IP Multicast VLAN Replication Global Settings

This window is used to enable the global settings for IP multicast VLAN replication on the Switch.

To view this window, click **Administration > IP Multicast VLAN Replication > IP Multicast VLAN Replication Global Settings**, as shown below.

The screenshot shows the 'IP Multicast VLAN Replication Global Settings' window. It contains the following fields and values:

- IP Multicast VLAN Replication State:** Enabled
- TTL:** Decrease
- Source MAC Address:** Replace

At the bottom right is an 'Apply' button.

Figure 2 - 139 IP Multicast VLAN Replication Global Settings window

The following fields may be set:

Parameter	Description
IP Multicast VLAN Replication State	<i>Enable</i> or <i>Disable</i> the IP Multicast VLAN Replication State on the Switch.
TTL	TTL specifies whether to decrease the time to live of a packet, the user can choose either <i>Decrease</i> or <i>No Decrease</i> . When a multicast packet is forwarded across VLANs, the time to live will be decreased by one. If <i>No Decrease</i> is specified, the time to live will not be decreased. By default, TTL will be decreased.
Source MAC Address	Specifies whether to replace the source MAC address of a packet, the user can choose either <i>Replace</i> or <i>No Replace</i> . By default, the source MAC address will be replaced.

Click **Apply** to implement changes.

IP Multicast VLAN Replication Settings

This window allows the user to create an IP Multicast VLAN replication entry. An IP Multicast VLAN Replication entry defines what traffic will be replicated and how the packet will be replicated.

To view this window, click **Administration > IP Multicast VLAN Replication > IP Multicast VLAN Replication Settings**, as shown below.

IP Multicast VLAN Replication Entry Add			
Entry Name	<input type="text"/>	Apply	
Total Entries: 1			
IP Multicast VLAN Replication Entries			
Entry Name	Source	Destination	Delete
RG	View	View	X

Figure 2 - 140 IP Multicast VLAN Replication Settings window

Enter a name for the IP Multicast Replication entry and click **Apply**. The new entry will appear in the IP Multicast VLAN Replication Entries Table.

The user can then configure the Source settings by clicking the corresponding **View** buttons , as shown below.

This table is used to configure the traffic to be replicated by the IP Multicast VLAN replication entry. The traffic is described by a source VLAN, a list of Multicast Group addresses and an optional source IP address associated with the multicast group.

IP Multicast VLAN Replication Source Edit

Entry Name	<input type="text" value="RG"/>		
VID / VLAN Name	<input type="text"/>	<input checked="" type="radio"/> VID <input type="radio"/> VLAN Name <input type="radio"/> Group	
Action	<input type="text" value="Add"/> ▼		
Multicast IP Address List	<input type="text"/>		
Source IP Address	<input type="text"/>		
<input type="button" value="Apply"/>			

Source VLAN Information

VLAN Name	<input type="text"/>
VID	<input type="text"/>

Multicast Group Address List

Entry Name	Multicast Group Address	Source Address	Delete
Show All IP Multicast VLAN Replication Entries			

Figure 2 - 141 IP Multicast VLAN Replication Settings - Source Edit window

The following fields may be set:

Parameter	Description
Entry Name	The name of the previously created IP Multicast VLAN Replication entry will be displayed.
VID / VLAN Name	Select VID and enter a source VLAN ID. Select VLAN Name and enter a source VLAN Name. When Group is selected, the user can configure the Action, Multicast IP Address List and the Source IP Address in the following fields.
Action	The user can specify to either <i>Add</i> or <i>Delete</i> the IP multicast address.
Multicast IP Address List	A multicast IP address list can be entered.
Source IP Address	A source IP Address can be specified.

Click **Apply** to implement the changes. To return to the IP Multicast VLAN Replication Settings window, click the [Show All IP Multicast VLAN Replication Entries](#) link.

The following table is used to set the Destination settings, to view this window click the corresponding **View** button in the IP Multicast VLAN Replication Entries table as shown below.

This table is used to configure the destination, so when traffic matches an IP Multicast VLAN Replication entry, it will be replicated based on the destination settings. Multiple destination entries can be defined and each destination entry specifies the VLAN and the outgoing port on which the traffic will be replicated. The outgoing port must be a member port of the VLAN, whether the egress packet is tagged or untagged based on the VLAN settings.

Figure 2 - 142 IP Multicast VLAN Replication Settings - Destination Edit window

The following fields may be set:

Parameter	Description
Entry Name	The name of the previously created IP Multicast VLAN Replication entry will be displayed.
VID / VLAN Name	Select VID and enter an outgoing VLAN ID. Select VLAN Name and enter an outgoing VLAN Name.
Port List(e.g.:1,6-9)	Enter the outgoing list of ports to be included in the destination settings.
Action	Use the drop-down menu to <i>Add</i> or <i>Delete</i> the destination.

Click **Apply** to implement the changes. To return to the IP Multicast VLAN Replication Settings window, click the [Show All IP Multicast VLAN Replication Entries](#) link.

Single IP Management (SIM) Overview

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. There are some advantages in implementing the “Single IP Management” feature:

1. SIM can simplify management of small workgroups or wiring closets while scaling the network to handle increased bandwidth demand.
2. SIM can reduce the number of IP address needed in your network.
3. SIM can eliminate any specialized cables for stacking connectivity and remove the distance barriers that typically limit your topology options when using other stacking technology.

Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

- SIM is an optional feature on the Switch and can easily be enabled or disabled through the Command Line Interface or Web Interface. SIM grouping has no effect on the normal operation of the Switch in the user's network.
- There are three classifications for switches using SIM. The Commander Switch (CS), which is the master switch of the group. Member Switch (MS), which is a switch that is recognized by the CS, which is a member of a SIM group. Candidate Switch (CaS), which is a Switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.
- A SIM group can only have one Commander Switch (CS).
- All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.
- A SIM group accepts up to 32 switches (numbered 1-32), not including the Commander Switch (numbered 0).
- There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.
- If multiple VLANs are configured, the SIM group will only utilize the Management VLAN on any switch.
- SIM allows intermediate devices that do not support SIM. This enables the user to manage switches that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The xStack® DGS-3400 Series switch may take on three different roles:

1. **Commander Switch (CS)** - This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:
 - It has an IP Address.
 - It is not a command switch or member switch of another Single IP group.
 - It is connected to the member switches through its management VLAN.
2. **Member Switch (MS)** - This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:
 - It is not a CS or MS of another IP group.
 - It is connected to the CS through the CS management VLAN.
3. **Candidate Switch (CaS)** - This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group of the xStack® DGS-3400 Series switch by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:
 - It is not a CS or MS of another Single IP group.
 - It is connected to the CS through the CS management VLAN

The following rules also apply to the above roles:

- Each device begins in a Candidate state.
- CSs must change their role to CaS and then to MS, to become a MS of a SIM group. Thus, the CS cannot directly be converted to a MS.

- The user can manually configure a CS to become a CaS.
- A MS can become a CaS by:
 - Being configured as a CaS through the CS.
 - If report packets from the CS to the MS time out.
- The user can manually configure a CaS to become a CS
- The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional xStack® DGS-3400 Series switch may join the group by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send it back to the administrator.

When a CaS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However, if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

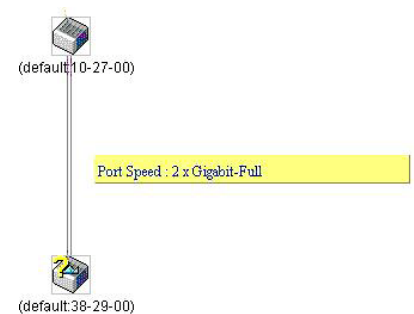
The Upgrade to v1.61

To better improve SIM management, the xStack® DES-3400 Series switches have been upgraded to version 1.61 in this release. Many improvements have been made, including:

1. The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintenance packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches.

There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

2. The topology map now includes new features for connections that are a member of a port trunking group. It will display the speed and number of Ethernet connections creating this port trunk group, as shown in the adjacent picture.



3. This version will support switch upload and downloads for firmware, configuration files and log files, as follows:

Firmware – The switch now supports MS firmware downloads from a TFTP server.

Configuration Files – This switch now supports downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server..

Log – The Switch now supports uploading MS log files to a TFTP server.

4. The user may zoom in and zoom out when utilizing the topology window to get a better, more defined view of the configurations.



NOTE: SIM Management does not support IPv6. For users wishing to utilize this function, switches in the SIM group must be configured with IPv4 addresses. IPv6 for SIM management will be supported in a future release of this switch.

Single IP vs. Switch Stacking

Single IP and Switch Stacking are two different entities and should not be equated by users. Within a switch stack, all functions are shared among switches in the stack and this switch stack is treated as one switch. Layer 2 and Layer 3 features, such as VLAN configurations and packet routing can be configured across switches in the stack. For example, mirroring functions can be shared within the stack, so a mirror target port may be on one switch in the stack and the source ports may be on another.

For Single IP Management, switches are separate entities that share a common IP address. Therefore, Layer 2 and Layer 3 functions CANNOT be shared among switches in the Single IP group. The purpose of the Single IP Management function is to share firmware and configuration files among switches within the Single IP Group. To have similar configurations on switches within the Single IP Group, users can upload identical configuration files to the Single IP Group using the **Configuration File Backup/Restore** window located under the Single IP heading on the switch, and described later in this section. Once this file is entered and uploaded to switches within the group, most configurations should be the same for the switches in the Single IP Group.

SIM Settings

All xStack® DGS-3400 Series Switches are set as Candidate (CaS) switches as their factory default configuration and Single IP Management will be disabled.

To view this window, click **Administration > Single IP Management Settings > SIM Settings**, as shown below.

The screenshot shows the 'SIM Settings' window. At the top, there is a blue header with the text 'SIM Settings'. Below the header, there is a section for 'SIM State' with a pull-down menu currently set to 'Disabled'. To the right of the 'SIM State' field is an 'Apply' button.

Figure 2 - 143 SIM Settings - Disable window

Change the **SIM State** to *Enabled* using the pull down menu and click **Apply**. The screen will then refresh and the **SIM Settings** window will look like this:

The screenshot shows the 'SIM Settings' window after being updated. The 'SIM State' pull-down menu is now set to 'Enabled'. Below it, the 'Role State' pull-down menu is set to 'Candidate'. There is an empty text input field for 'Group Name'. The 'Discovery Interval' is set to '30' with a range of '(30-90 sec)'. The 'Hold Time' is set to '100' with a range of '(100-255 sec)'. An 'Apply' button is located at the bottom right of the window.

Figure 2 - 144 SIM Settings - Enable window

Parameter	Description
SIM State	Use the pull-down menu to either enable or disable the SIM state on the Switch. <i>Disabled</i> will render all SIM functions on the Switch inoperable.
Role State	Use the pull-down menu to change the SIM role of the Switch. The two choices are: <i>Candidate</i> – A Candidate Switch (CaS) is not the member of a SIM group but is connected to

	a Commander Switch. This is the default setting for the SIM role of the DGS-3400 Series. <i>Commander</i> – Choosing this parameter will make the Switch a Commander Switch (CS). The user may join other switches to this Switch, over Ethernet, to be part of its SIM group. Choosing this option will also enable the Switch to be configured for SIM.
Group Name	Enter the name of the group the entry will be associated with.
Discovery Interval	The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to a Commander Switch will include information about other switches connected to it. (Ex. MS, CaS). The user may set the Discovery Interval from 30 to 90 seconds.
Hold Time	This parameter may be set for the time, in seconds; the Switch will hold information sent to it from other switches, utilizing the Discovery Interval. The user may set the hold time from 100 to 255 seconds.

Click **Apply** to implement the settings changed. After enabling the Switch to be a Commander Switch (CS), the **Single IP Management** folder will then contain four added links to aid the user in configuring SIM through the web, including **Topology**, **Firmware Upgrade**, **Configuration Backup/Restore** and **Upload Log**.

Topology

The **Topology** window will be used to configure and manage the Switch within the SIM group and requires Java script to function properly on your computer.

The Java Runtime Environment on your server should initiate and lead you to the topology window, as seen below.

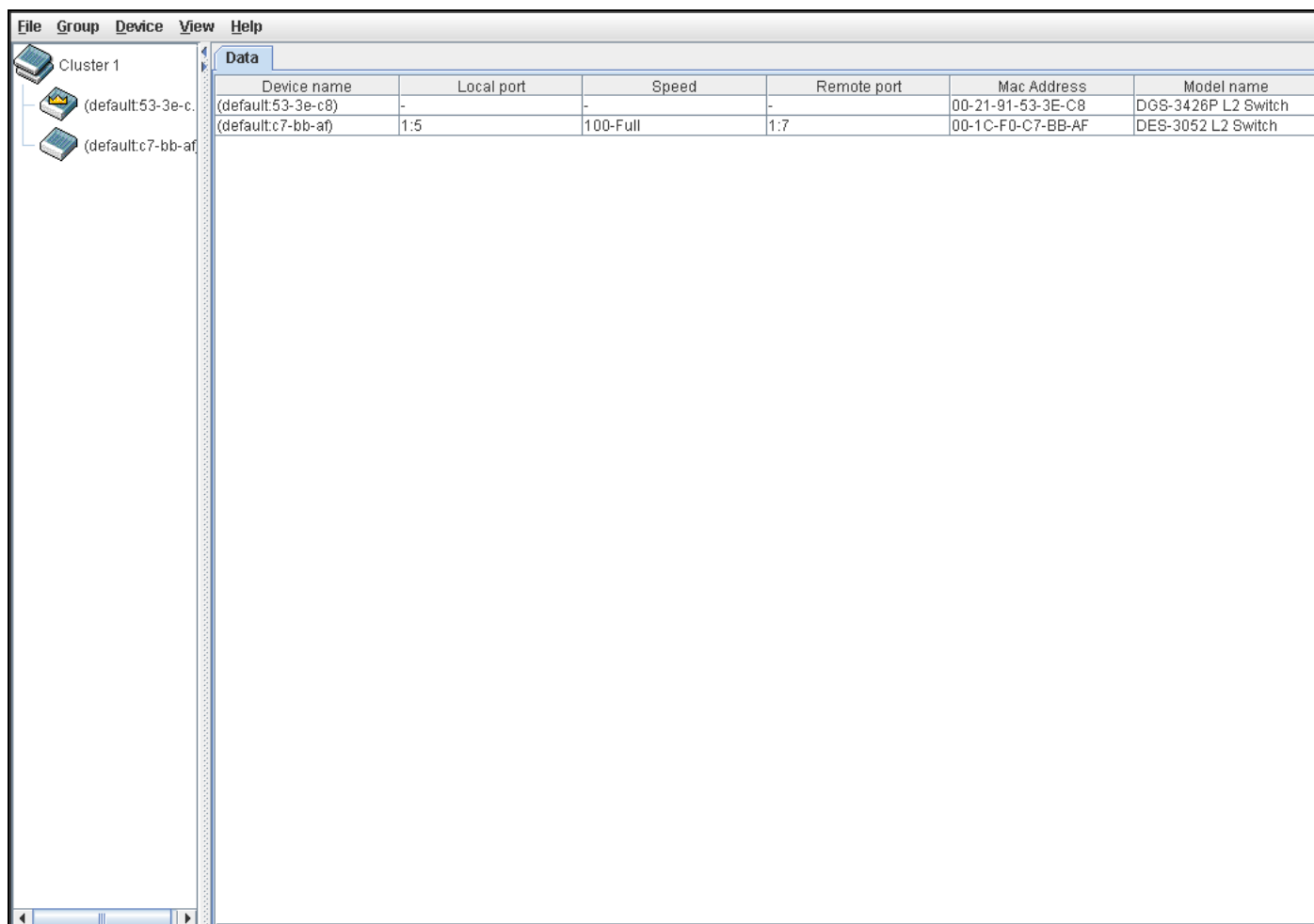


Figure 2 - 145 Single IP Management window - Tree View

The Tree View window holds the following information under the Data tab:

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no device is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Local Port	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Speed	Displays the connection speed between the CS and the MS or CaS.
Remote Port	Displays the number of the physical port on the MS or CaS to which the CS is connected. The CS will have no entry in this field.
MAC Address	Displays the MAC Address of the corresponding Switch.
Model Name	Displays the full Model Name of the corresponding Switch.

To view the **Topology Map**, click the **View** menu in the toolbar and then Topology, which will produce the following screen. The **Topology View** will refresh itself periodically (20 seconds by default).

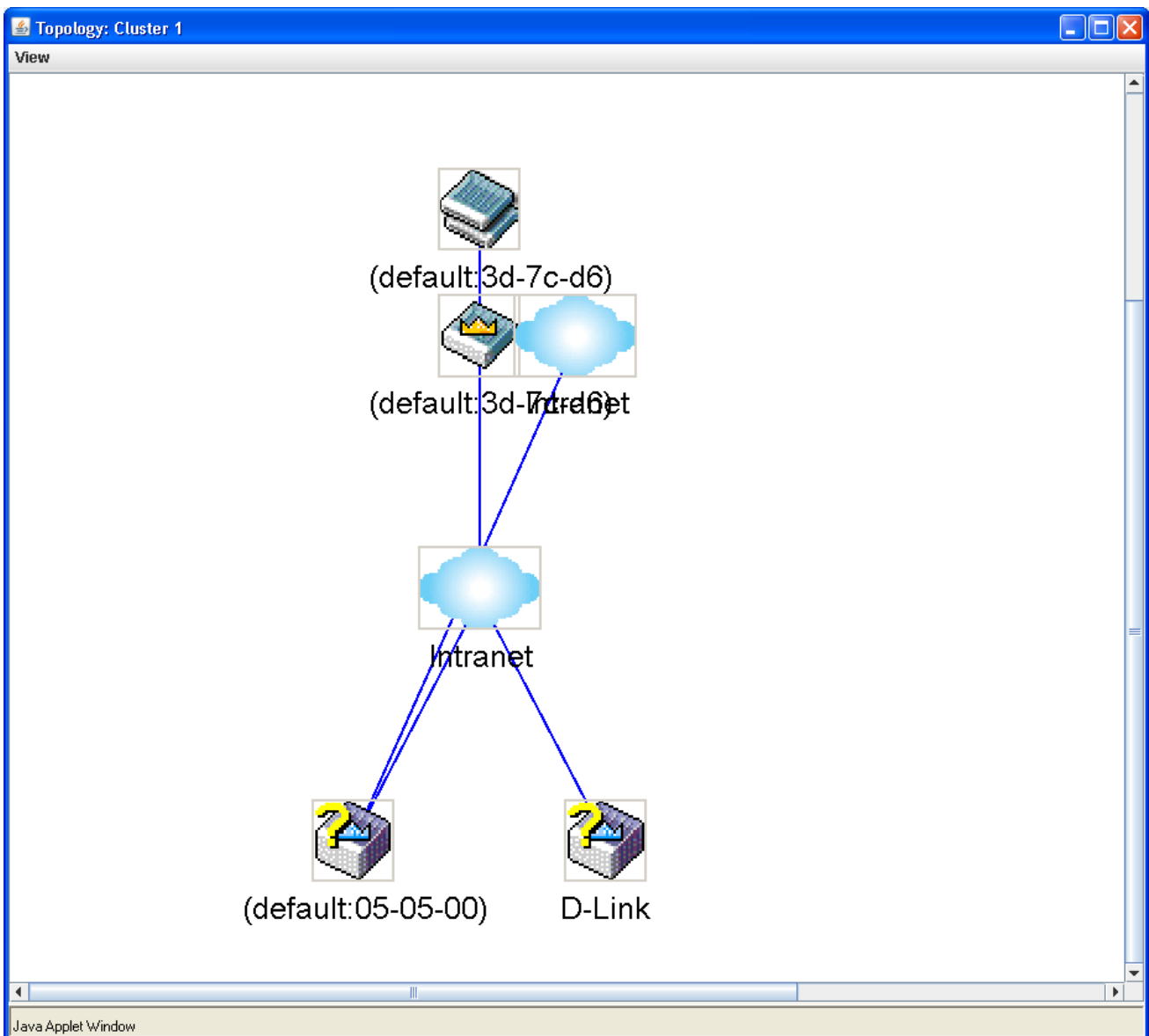













Figure 2 - 146 Topology view

This screen will display how the devices within the Single IP Management Group connect to other groups and devices. Possible icons in this screen are as follows:

Icon	Description
	Group
	Layer 2 commander switch
	Layer 3 commander switch
	Commander switch of other group
	Layer 2 member switch.
	Layer 3 member switch
	Member switch of other group
	Layer 2 candidate switch
	Layer 3 candidate switch
	Unknown device
	Non-SIM devices

Tool Tips

In the Topology view window, the mouse plays an important role in configuration and in viewing device information. Setting the mouse cursor over a specific device in the topology window (tool tip) will display the same information about a specific device as the Tree view does. See the window below for an example.

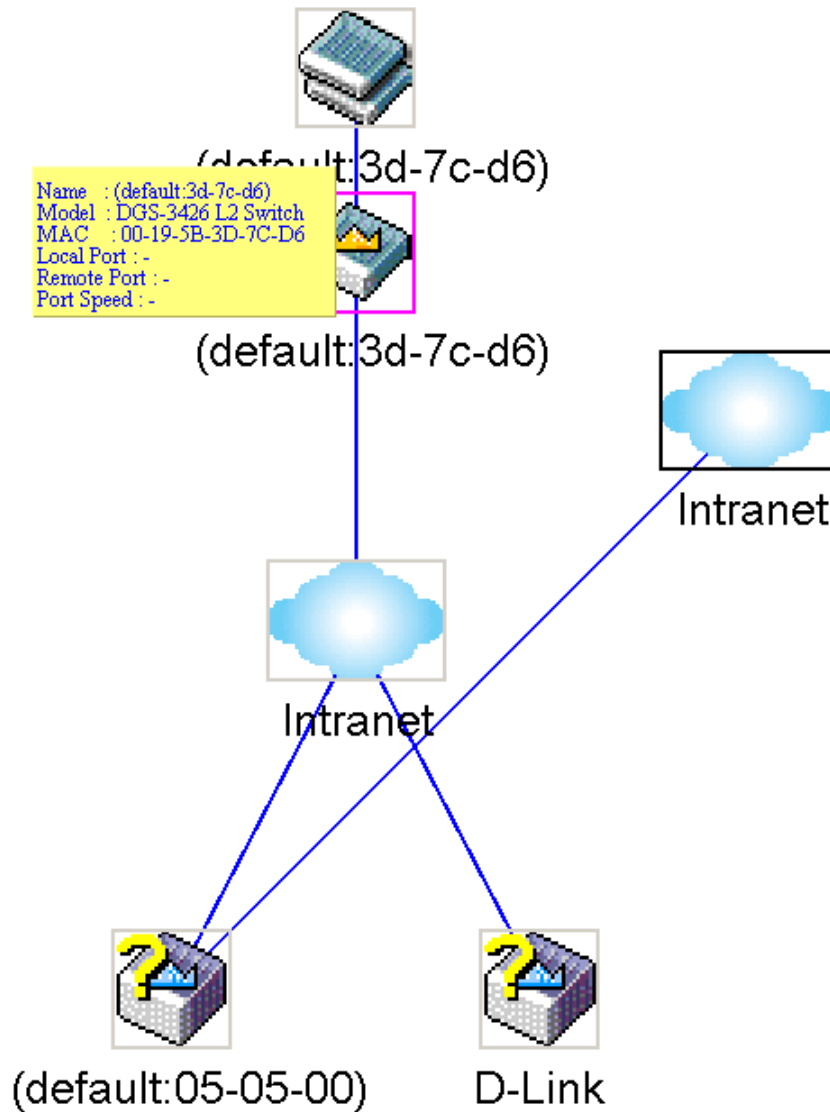


Figure 2 - 147 Device Information Utilizing the Tool Tip

Setting the mouse cursor over a line between two devices will display the connection speed between the two devices, as shown below.

Right-click

Right-clicking on a device will allow the user to perform various functions, depending on the role of the Switch in the SIM group and the icon associated with it.

Group Icon

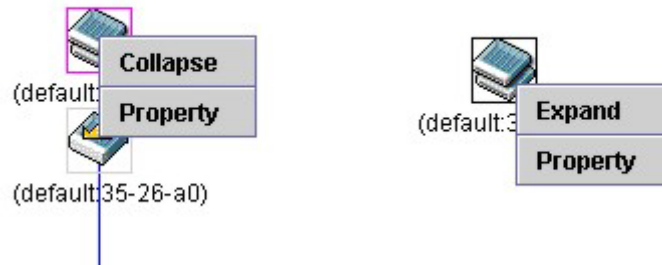


Figure 2 - 149 Right-clicking a Group Icon

The following options may appear for the user to configure:

- **Collapse** - to collapse the group that will be represented by a single icon.
- **Expand** - to expand the SIM group, in detail.
- **Property** - to pop up a window to display the group information.

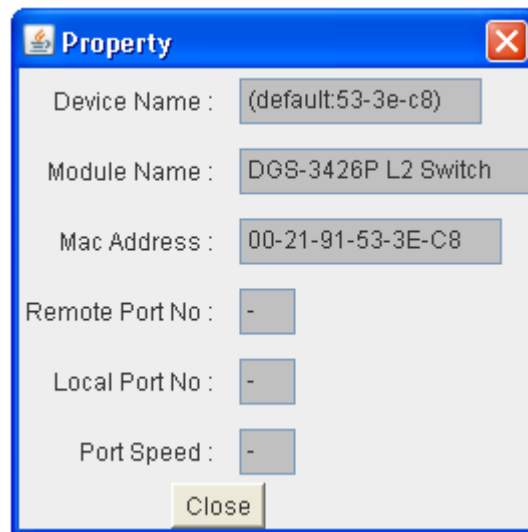


Figure 2 - 150 Property window

Parameter	Description
Device Name	This field will display the Device Name of the switches in the SIM group configured by the user. If no Device Name is configured by the name, it will be given the name default and tagged with the last six digits of the MAC Address to identify it.
Module Name	Displays the full module name of the switch that was right-clicked.
MAC Address	Displays the MAC Address of the corresponding Switch.
Remote Port No.	Displays the number of the physical port on the MS or CaS that the CS is connected to. The CS will have no entry in this field.
Local Port No.	Displays the number of the physical port on the CS that the MS or CaS is connected to. The CS will have no entry in this field.
Port Speed	Displays the connection speed between the CS and the MS or CaS

Commander Switch Icon

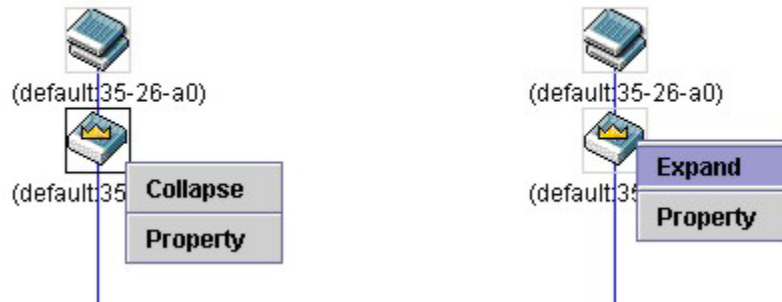


Figure 2 - 151 Right-clicking a Commander Icon

The following options may appear for the user to configure:

- **Collapse** – to collapse the group that will be represented by a single icon.
- **Expand** – to expand the SIM group, in detail.
- **Property** – to pop up a window to display the group information.

Member Switch Icon

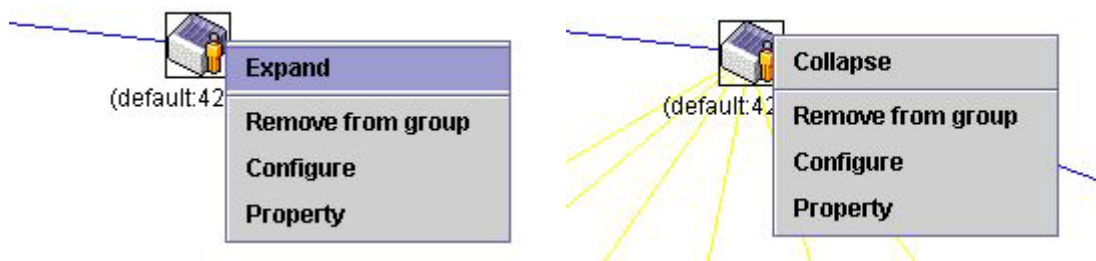


Figure 2 - 152 Right-clicking a Member icon

The following options may appear for the user to configure:

- **Collapse** – to collapse the group that will be represented by a single icon.
- **Expand** – to expand the SIM group, in detail.
- **Remove from group** – remove a member from a group.
- **Configure** – launch the web management to configure the Switch.
- **Property** – to pop up a window to display the device information.

Candidate Switch Icon

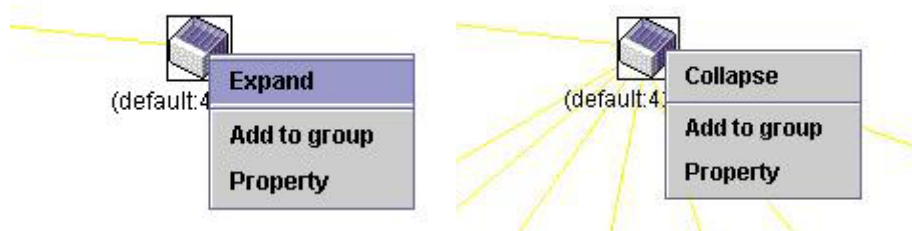


Figure 2 - 153 Right-clicking a Candidate icon

The following options may appear for the user to configure:

- **Collapse** – to collapse the group that will be represented by a single icon.
- **Expand** – to expand the SIM group, in detail.
- **Add to group** – add a candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the window.

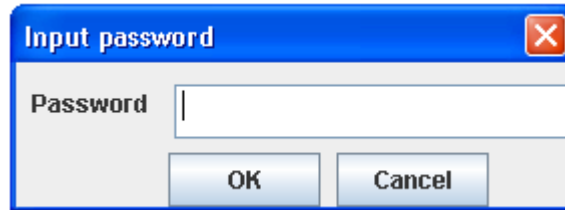


Figure 2 - 154 Input password dialog

- **Property** – to pop up a window to display the device information.

Menu Bar

The **Single IP Management** window contains a menu bar for device configurations, as seen below.



Figure 2 - 155 Menu Bar of the Topology View

The five menus on the menu bar are as follows.

File

- **Print Setup** – will view the image to be printed.
- **Print Topology** – will print the topology map.
- **Preference** – will set display properties, such as polling interval, and the views to open at SIM startup.

Group

- **Add to group** – add a candidate to a group. Clicking this option will reveal the following screen for the user to enter a password for authentication from the Candidate Switch before being added to the SIM group. Click **OK** to enter the password or **Cancel** to exit the window.

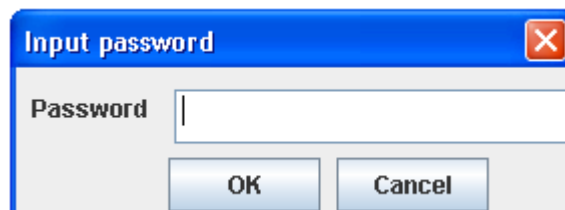


Figure 2 - 156 Input password dialog

- **Remove from Group** - Remove an MS from the group.

Device

- **Configure** - will open the Web manager for the specific device.

View

- **Refresh** - update the views with the latest status.
- **Topology** - display the Topology view.

Help

- **About** - Will display the SIM information, including the current SIM version.



Figure 2 - 157 About window

Firmware Upgrade

This window is used to upgrade firmware from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by Port (port on the CS where the MS resides), MAC Address, Model Name and Version. To specify a certain Switch for firmware download, click its corresponding check box under the Port heading. To update the firmware, enter the Server IP Address where the firmware resides and enter the Path/File name of the firmware. Click **Download** to initiate the file transfer.

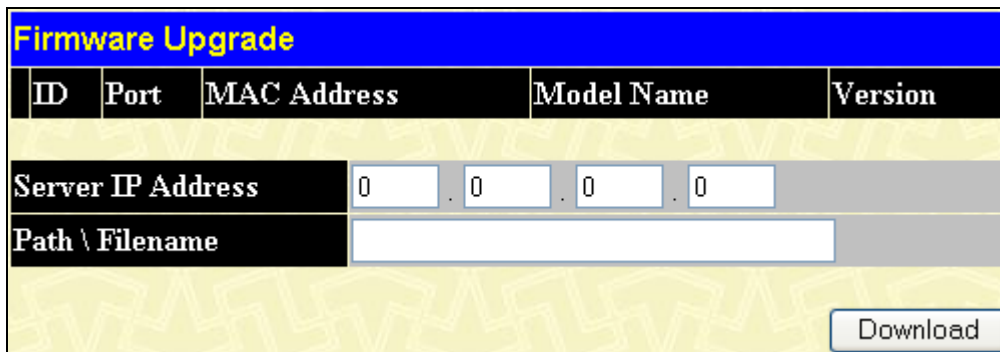


Figure 2 - 158 Firmware Upgrade window

Configuration Backup/Restore

This window is used to upgrade configuration files from the Commander Switch to the Member Switch. Member Switches will be listed in the table and will be specified by Port (port on the CS where the MS resides), MAC Address, Model Name and Version. To specify a certain Switch for upgrading configuration files, click its corresponding radio button under the Port heading. To update the configuration file, enter the Server IP Address where the firmware resides and enter the Path/File name of the firmware. Click **Download** to initiate the file transfer.

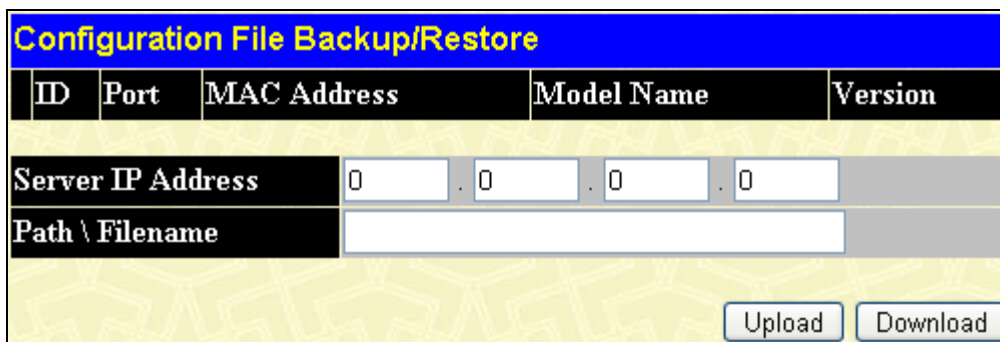


Figure 2 - 159 Configuration File Backup/Restore window

Upload Log

The following window is used to upload log files from SIM member switches to a specified PC. To upload a log file, enter the IP address of the SIM member switch and then enter the path on your PC to which to save this file. Click **Upload** to initiate the file transfer.

To view this window, click **Single IP Management > Upload Log File**, as shown below.

Figure 2 - 160 Upload Log File window

RIP

The Routing Information Protocol is a distance-vector routing protocol. There are two types of network devices running RIP - active and passive. Active devices advertise their routes to others through RIP messages, while passive devices listen to these messages. Both active and passive routers update their routing tables based upon RIP messages that active routers exchange. Only routers can run RIP in the active mode.

Every 30 seconds, a router running RIP broadcasts a routing update containing a set of pairs of network addresses and a distance (represented by the number of hops or routers between the advertising router and the remote network). So, the vector is the network address and the distance is measured by the number of routers between the local router and the remote network.

RIP measures distance by an integer count of the number of hops from one network to another. A router is one hop from a directly connected network, two hops from a network that can be reached through a router, etc. The more routers between a source and a destination, the greater the RIP distance (or hop count).

There are a few rules to the routing table update process that help to improve performance and stability. A router will not replace a route with a newly learned one if the new route has the same hop count (sometimes referred to as 'cost'). So learned routes are retained until a new route with a lower hop count is learned.

When learned routes are entered into the routing table, a timer is started. This timer is restarted every time this route is advertised. If the route is not advertised for a period of time (usually 180 seconds), the route is removed from the routing table.

RIP does not have an explicit method to detect routing loops. Many RIP implementations include an authorization mechanism (a password) to prevent a router from learning erroneous routes from unauthorized routers.

To maximize stability, the hop count RIP uses to measure distance must have a low maximum value. Infinity (that is, the network is unreachable) is defined as 16 hops. In other words, if a network is more than 16 routers from the source, the local router will consider the network unreachable.

RIP can also be slow to converge (to remove inconsistent, unreachable or looped routes from the routing table) because RIP messages propagate relatively slowly through a network.

Slow convergence can be solved by using split horizon update, where a router does not propagate information about a route back to the interface on which it was received. This reduces the probability of forming transient routing loops.

Hold down can be used to force a router to ignore new route updates for a period of time (usually 60 seconds) after a new route update has been received. This allows all routers on the network to receive the message.

A router can 'poison reverse' a route by adding an infinite (16) hop count to a route's advertisement. This is usually used in conjunction with triggered updates, which force a router to send an immediate broadcast when an update of an unreachable network is received.

RIP Version 1 Message Format

There are two types of RIP messages: routing information messages and information requests. Both types use the same format.

The Command field specifies an operation according the following table:

Command	Meaning
1	Request for partial or full routing information
2	Response containing network-distance pairs from sender's routing table
3	Turn on trace mode (obsolete)
4	Turn off trace mode (obsolete)
5	Reserved for Sun Microsystem's internal use
9	Update Request
10	Update Response
11	Update Acknowledgement

RIP Command Codes

The field VERSION contains the protocol version number (1 in this case), and is used by the receiver to verify which version of RIP the packet was sent.

RIP 1 Message

RIP is not limited to TCP/IP. Its address format can support up to 14 octets (when using IP, the remaining 10 octets must be zeros). Other network protocol suites can be specified in the Family of Source Network field (IP has a value of 2). This will determine how the address field is interpreted.

RIP specifies that the IP address, 0.0.0.0, denotes a default route.

The distances, measured in router hops are entered in the Distance to Source Network, and Distance to Destination Network fields.

RIP 1 Route Interpretation

RIP was designed to be used with classed address schemes, and does not include an explicit subnet mask. An extension to version 1 does allow routers to exchange subnetted addresses, but only if the subnet mask used by the network is the same as the subnet mask used by the address. This means the RIP version 1 cannot be used to propagate classless addresses.

Routers running RIP version 1 must send different update messages for each IP interface to which it is connected. Interfaces that use the same subnet mask as the router's network can contain subnetted routes, other interfaces cannot. The router will then advertise only a single route to the network.

RIP Version 2 Extensions

RIP version 2 includes an explicit subnet mask entry, so RIP version 2 can be used to propagate variable length subnet addresses or CIDR classless addresses. RIP version 2 also adds an explicit next hop entry, which speeds convergence and helps prevent the formation of routing loops.

RIP2 Message Format

The message format used with RIP2 is an extension of the RIP1 format:

RIP version 2 also adds a 16-bit route tag that is retained and sent with router updates. It can be used to identify the origin of the route.

Because the version number in RIP2 occupies the same octet as in RIP1, both versions of the protocols can be used on a given router simultaneously without interference.

RIP

RIP Global Settings

To setup RIP for the IP interfaces configured on the Switch, the user must first globally enable RIP and then configure RIP settings for the individual IP interfaces.

To globally enable RIP on the Switch, click **Administration > RIP > RIP > RIP Global Settings**, as shown below.

Figure 2 - 161 RIP Global Settings window

To enable RIP, simply use the pull-down menu, select *Enabled* and click **Apply**.

RIP Interface Settings

RIP settings are configured for each IP interface on the Switch. This window appears in table form listing settings for IP interfaces currently on the Switch. To configure RIP settings for an individual interface, click on the hyperlinked Interface Name.

To view this window, click **Administration > RIP > RIP > RIP Interface Settings**, as shown below.

Total Entries:1					
RIP Interface Settings					
Interface Name	IP Address	TX Mode	RX Mode	Auth.	State
System	10.90.90.90	Disabled	Disabled	Disabled	Disabled

Figure 2 - 162 RIP Interface Settings window

Click the hyperlinked name of the interface to configure the settings for RIP, which will give access to the following window:

Figure 2 - 163 RIP Interface Settings - Edit window

The following RIP interface settings can be applied to each IP interface:

Parameter	Description
Interface Name	The name of the IP interface on which RIP is to be setup. This interface must be previously configured on the Switch.

IP Address	The IP address corresponding to the Interface Name showing in the field above.
TX Mode	Toggle among <i>Disabled</i> , <i>V1 Only</i> , <i>V1 Compatible</i> , and <i>V2 Only</i> . This entry specifies which version of the RIP protocol will be used to transmit RIP packets. <i>Disabled</i> prevents the transmission of RIP packets.
RX Mode	Toggle among <i>Disabled</i> , <i>V1 Only</i> , <i>V2 Only</i> , and <i>V1 or V2</i> . This entry specifies which version of the RIP protocol will be used to interpret received RIP packets. <i>Disabled</i> prevents the reception of RIP packets.
Authentication	Toggle between <i>Disabled</i> and <i>Enabled</i> to specify that routers on the network should use the Password above to authenticate router table exchanges.
Password	A password to be used to authenticate communication between routers on the network.
State	Toggle between <i>Disabled</i> and <i>Enabled</i> to disable or enable this RIP interface on the switch.
Interface Metric	A read only field that denotes the Metric value of the current IP Interface setting.

Click **Apply** to implement the changes. To return to the RIP Interface Settings window, click the [Show All RIP Interface Entries](#) link.

RIPng

The Switch supports Routing Information Protocol next generation (RIPng). RIPng is a routing protocol that exchanges routing information used to compute routes and is intended for IPv6-based networks.

RIPng Global Settings

This window allows users to set up RIPng.

To view this window, click **Administration > RIP > RIPng > RIPng Global Settings**, as shown below.

RIPng Global Settings	
Global State	Disabled
Method	Split Horizon
Update Time (5-65535)	30 sec
Expire Time (1-65535)	180 sec
Garbage Collection Time (1-65535)	120 sec
Apply	

Figure 2 - 164 RIPng Global Settings window

The following settings can be configured:

Parameter	Description
Global State	Enable or disable RIPng globally. The default setting is <i>Disabled</i> .
Method	Choose from <i>No Horizon</i> , <i>Split Horizon</i> , and <i>Poison Reverse</i> . <i>No Horizon</i> – Configured to not use any horizon. <i>Split Horizon</i> – Configured to use basic split horizon. This is the default setting. <i>Poison Reverse</i> – Configured to use split horizon with poison reverse.
Update Time (5-65535)	Enter the value (in seconds) of the update timer.

Expire Time (1-65535)	Enter the value (in seconds) of the expire time.
Garbage Collection Time (1-65535)	Enter the value (in seconds) of the garbage-collection timer.

Click **Apply** to implement changes made.

RIPng Interface Settings

This window allows users to configure RIPng interface settings.

To globally enable RIP ng on the Switch, click **Administration > RIP > RIPng > RIPng Interface Settings**, as shown below.

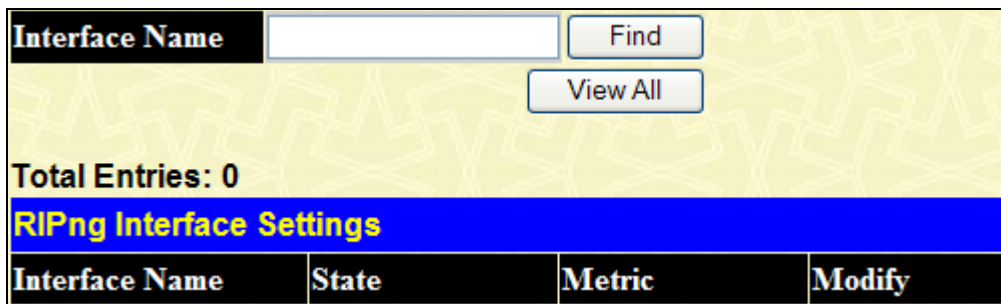


Figure 2 - 165 RIPng Interface Settings window

To modify an entry, click the corresponding **Modify** button to see the window, as shown below.



Figure 2 - 166 RIPng Interface Settings - Edit window

The following settings can be configured:

Parameter	Description
Interface Name	The name of the interface for the RIPng configuration.
State	Enable or disable the RIPng state on the specific IP interface. If the state is <i>Disabled</i> , then RIPng packets will not be transmitted or received by the interface. The default setting is <i>Disabled</i> .
Metric	Enter the cost value of an interface. The RIPng route that was learned from the interface will add this value as a new route metric. The default value is <i>1</i> .

Click **Apply** to implement changes made.

IP Tunnel Settings

The Switch supports IP tunneling. The idea behind this feature is to be able to integrate IPv6 into and coexist with existing IPv4 networks. It is expected that IPv4 and IPv6 hosts will need to coexist for a substantial time during the steady migration from IPv4 to IPv6, and the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start. This IPv6 tunneling mechanism is one of D-Link's strategies for solving the transition from IPv4 to IPv6.

To configure the settings, click **Administration > IP Tunnel Settings**, as shown below.

The screenshot shows the 'IP Tunnel Settings' window. At the top left is an 'Add' button. Below it is a search section with 'Interface Name' and a text input field, followed by 'Find' and 'View All' buttons. Below the search section, it says 'Total Entries: 1'. The main content is a table with the following data:

Tunnel Interface	Interface Admin State	Tunnel Mode	IPv6 Address	Tunnel Source	Tunnel Destination	Modify	Delete
index	Enabled	Unknown	Unknown	Unknown	Unknown	Modify	X

Figure 2 - 167 IPng Tunnel Settings window

To remove an entry, click the corresponding button. To Add a new name of the interface, click **Add** to see the window, as shown below.

The screenshot shows the 'IP Tunnel Settings - Add' window. It has a blue header with the title. Below the header is a form with 'Interface Name' and a text input field. To the right of the input field is an 'Apply' button. At the bottom left, there is a blue link that says 'Show All IP Tunnel Entries'.

Figure 2 - 168 IPng Tunnel Settings - Add window

Enter the Interface Name in the field and click **Apply**. To return to the IP Tunnel Settings window, click the [Show All IP Tunnel Entries](#) link.

To configure a tunnel interface, click the corresponding **Modify** button to see the window below.

The screenshot shows the 'IP Tunnel Settings - Edit' window. It has a blue header with the title. Below the header is a form with the following fields:

- Interface Name:** A text input field containing 'index'.
- Interface Admin State:** A dropdown menu with 'Enabled' selected.
- Mode:** A dropdown menu with 'Manual' selected.
- IPv6 Address/Prefix Length:** A text input field with a hint 'e.g.: 2233::2/64' to its right.
- Source IP Address:** A text input field.
- Destination IP Address:** A text input field.

At the bottom right of the form is an 'Apply' button. At the bottom left, there is a blue link that says 'Show All IP Tunnel Entries'.

Figure 2 - 169 IPng Tunnel Settings - Edit window

The following parameters can be configured or viewed:

Parameter	Description
Interface Name	This is the IPv6 tunnel interface name.
Interface Admin State	Enable or disable IP tunneling.
Mode	<p>Select from <i>Manual</i>, <i>6to4</i>, or <i>ISATAP</i>.</p> <p><i>Manual</i> is used to configure an existing IPv6 tunnel as an IPv6 manual tunnel on the Switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not, will depend on the current mode. IPv6 Manual tunnels are simple point-to-point tunnels that can be used within a site or between sites</p> <p><i>6to4</i> is used to configure an existing IPv6 tunnel as an IPv6 6to4 tunnel on the Switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not will depend on the current mode. A maximum of one IPv6 6to4 tunnel can exist on the system. IPv6 6to4 tunnels are point-to-multipoint tunnels that can be used to connect isolated IPv6 sites. Each IPv6 site has at least one connection to a shared IPv4 network and this IPv4 network could be the global Internet or a corporate backbone. The key requirement is that each site has a globally unique IPv4 address, which is used to construct a 48-bit globally unique 6to4 IPv6 prefix (It starts with the prefix 2002::/16).</p> <p><i>ISATAP</i> is used to configure an existing IPv6 tunnel as an IPv6 ISATAP tunnel on the Switch. If this tunnel has previously been configured in another mode, the tunnel's information will still exist in the database. However, whether the tunnel's former information is invalid or not will depend on the current mode. IPv6 ISATAP tunnels are point-to-multipoint tunnels that can be used to connect systems within a site. An IPv6 ISATAP address is a well-defined unicast address that includes a 64-bit unicast IPv6 prefix (it can be link local or global prefixes), a 32-bit value 0000:5EFE and a 32-bit tunnel source IPv4 address.</p>
IPv6 Address/Prefix Length	Enter the IPv6 address assigned to this IPv6 tunnel interface. IPv6 processing would be enabled on this IPv6 tunnel interface when an IPv6 address is configured. This IPv6 address is not connected with tunnel source or destination IPv4 address.
Source IP Address	Enter the source IPv4 address of this IPv6 tunnel interface. It is used as the source address for packets in this IPv6 tunnel.
Destination IP Address	Enter the destination IPv4 address of this IPv6 tunnel interface. It is used as the destination address for packets in this IPv6 tunnel. It is not required for 6to4 and ISATAP tunnels.

Click **Apply** to implement the changes. To return to the IP Tunnel Settings window, click the [Show All IP Tunnel Entries](#) link.

L2 Features

VLANs

Trunking

IGMP Snooping

MLD Snooping

Loop-back Detection Global Settings

Spanning Tree

Forwarding & Filtering

LLDP

Q-in-Q

ERPS

DULD Settings

NLB Multicast FDB Settings

The following section will aid the user in configuring security functions for the Switch. The Switch includes various functions for VLAN, Trunking, IGMP Snooping, MLD Snooping, Loopback Detection Global Settings, Spanning Tree, Forwarding & Filtering, LLDP and Q-in-Q all discussed in detail in the following section.

VLANs

VLAN Description

A Virtual Local Area Network (VLAN) is a network topology configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. VLANs also logically segment the network into different broadcast domains so that packets are forwarded only between ports within the VLAN. Typically, a VLAN corresponds to a particular subnet, although not necessarily.

VLANs can enhance performance by conserving bandwidth, and improve security by limiting traffic to specific domains.

A VLAN is a collection of end nodes grouped by logic instead of physical location. End nodes that frequently communicate with each other are assigned to the same VLAN, regardless of where they are physically on the network. Logically, a VLAN can be equated to a broadcast domain, because broadcast packets are forwarded to only members of the VLAN on which the broadcast was initiated.

Notes about VLANs on the DGS-3400 Series

No matter what basis is used to uniquely identify end nodes and assign these nodes VLAN membership, packets cannot cross VLANs without a network device performing a routing function between the VLANs.

The xStack® DGS-3400 Series supports IEEE 802.1Q VLANs and Port-based VLANs. The port untagging function can be used to remove the 802.1Q tag from packet headers to maintain compatibility with devices that are tag-unaware.

The Switch's default is to assign all ports to a single 802.1Q VLAN named "default."

The "default" VLAN has a VID = 1.

The member ports of Port-based VLANs may overlap, if desired.

IEEE 802.1Q VLANs

Some relevant terms:

Tagging – The act of putting 802.1Q VLAN information into the header of a packet.

Untagging – The act of stripping 802.1Q VLAN information out of the packet header.

Ingress port – A port on a switch where packets are flowing into the Switch and VLAN decisions must be made.

Egress port – A port on a switch where packets are flowing out of the Switch, either to another switch or to an end station, and tagging decisions must be made.

IEEE 802.1Q (tagged) VLANs are implemented on the Switch. 802.1Q VLANs require tagging, which enables them to span the entire network (assuming all switches on the network are IEEE 802.1Q-compliant).

VLANs allow a network to be segmented in order to reduce the size of broadcast domains. All packets entering a VLAN will only be forwarded to the stations (over IEEE 802.1Q enabled switches) that are members of that VLAN, and this includes broadcast, multicast and unicast packets from unknown sources.

VLANs can also provide a level of security to your network. IEEE 802.1Q VLANs will only deliver packets between stations that are members of the VLAN.

Any port can be configured as either tagging or untagging. The untagging feature of IEEE 802.1Q VLANs allows VLANs to work with legacy switches that don't recognize VLAN tags in packet headers. The tagging feature allows VLANs to span multiple 802.1Q-compliant switches through a single physical connection and allows Spanning Tree to be enabled on all ports and work normally.

The IEEE 802.1Q standard restricts the forwarding of untagged packets to the VLAN the receiving port is a member of.

The main characteristics of IEEE 802.1Q are as follows:

- Assigns packets to VLANs by filtering.
- Assumes the presence of a single global spanning tree.
- Uses an explicit tagging scheme with one-level tagging.
- 802.1Q VLAN Packet Forwarding
- Packet forwarding decisions are made based upon the following three types of rules:
 - Ingress rules – rules relevant to the classification of received frames belonging to a VLAN.
 - Forwarding rules between ports – decides whether to filter or forward the packet.
 - Egress rules – determines if the packet must be sent tagged or untagged.

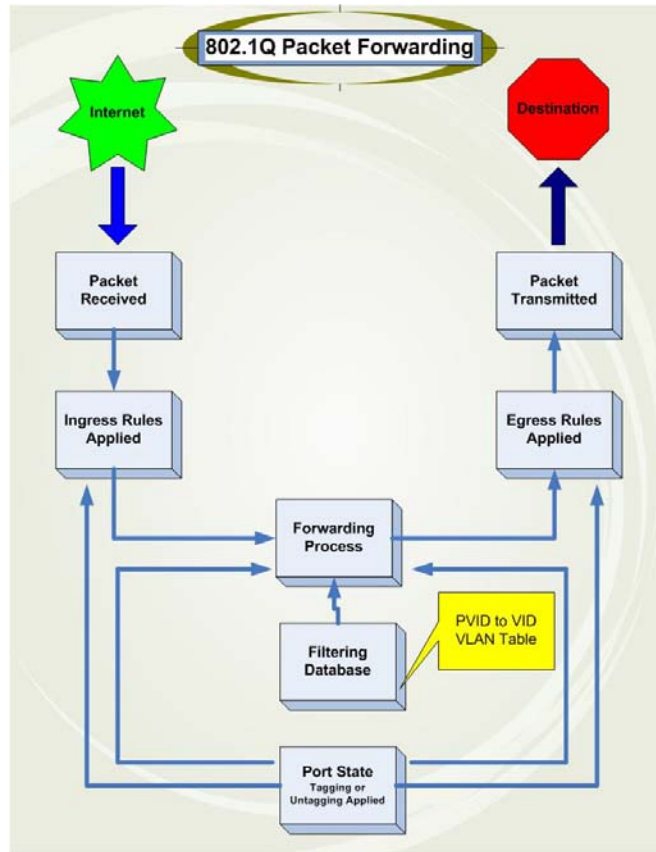


Figure 3 - 1 IEEE 802.1Q Packet Forwarding

802.1Q VLAN Tags

The figure below shows the 802.1Q VLAN tag. There are four additional octets inserted after the source MAC address. Their presence is indicated by a value of 0x8100 in the EtherType field. When a packet's EtherType field is equal to 0x8100, the packet carries the IEEE 802.1Q/802.1p tag. The tag is contained in the following two octets and consists of 3 bits of user priority, 1 bit of Canonical Format Identifier (CFI - used for encapsulating Token Ring packets so they can be carried across Ethernet backbones), and 12 bits of VLAN ID (VID). The 3 bits of user priority are used by 802.1p. The VID is the VLAN identifier and is used by the 802.1Q standard. Because the VID is 12 bits long, 4094 unique VLANs can be identified.

The tag is inserted into the packet header making the entire packet longer by 4 octets. All of the information originally contained in the packet is retained.

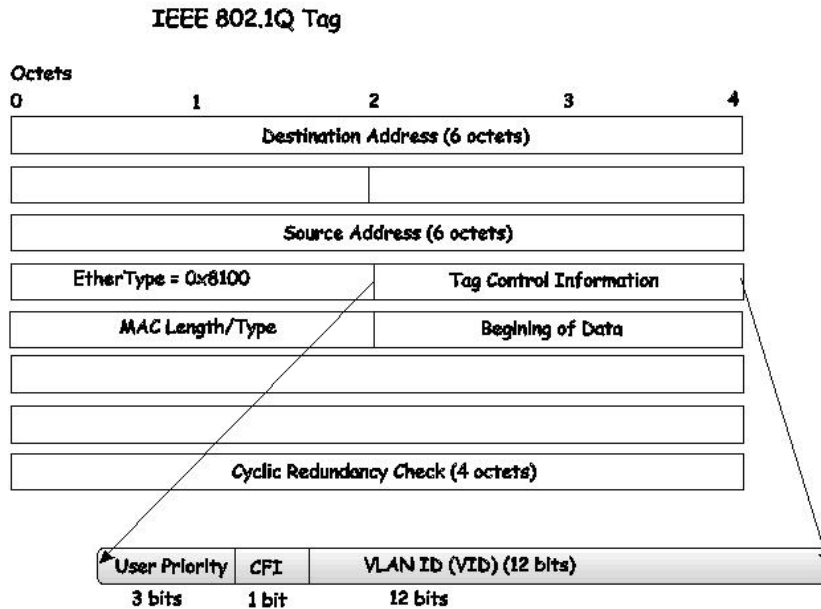


Figure 3 - 2 IEEE 802.1Q Tag

The EtherType and VLAN ID are inserted after the MAC source address, but before the original EtherType/Length or Logical Link Control. Because the packet is now a bit longer than it was originally, the Cyclic Redundancy Check (CRC) must be recalculated.

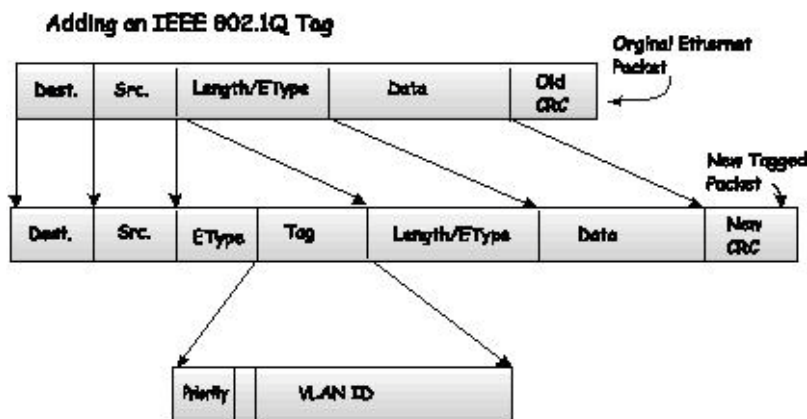


Figure 3 - 3 Adding an IEEE 802.1Q Tag

Port VLAN ID

Packets that are tagged (are carrying the 802.1Q VID information) can be transmitted from one 802.1Q compliant network device to another with the VLAN information intact. This allows 802.1Q VLANs to span network devices (and indeed, the entire network, if all network devices are 802.1Q compliant).

Unfortunately, not all network devices are 802.1Q compliant. These devices are referred to as tag-unaware. 802.1Q devices are referred to as tag-aware.

Prior to the adoption of 802.1Q VLANs, port-based and MAC-based VLANs were in common use. These VLANs relied upon a Port VLAN ID (PVID) to forward packets. A packet received on a given port would be assigned that port's PVID and then be forwarded to the port that corresponded to the packet's destination address (found in the Switch's forwarding table). If the PVID of the port that received the packet is different from the PVID of the port that is to transmit the packet, the Switch will drop the packet.

Within the Switch, different PVIDs mean different VLANs (remember that two VLANs cannot communicate without an external router). So, VLAN identification based upon the PVIDs cannot create VLANs that extend outside a given switch (or switch stack).

Every physical port on a switch has a PVID. 802.1Q ports are also assigned a PVID, for use within the Switch. If no VLANs are defined on the Switch, all ports are then assigned to a default VLAN with a PVID equal to 1. Untagged packets are assigned the PVID of the port on which they were received. Forwarding decisions are based upon this PVID, in so far as VLANs are con-

cerned. Tagged packets are forwarded according to the VID contained within the tag. Tagged packets are also assigned a PVID, but the PVID is not used to make packet-forwarding decisions, the VID is.

Tag-aware switches must keep a table to relate PVIDs within the Switch to VIDs on the network. The Switch will compare the VID of a packet to be transmitted to the VID of the port that is to transmit the packet. If the two VIDs are different, the Switch will drop the packet. Because of the existence of the PVID for untagged packets and the VID for tagged packets, tag-aware and tag-unaware network devices can coexist on the same network.

A switch port can have only one PVID, but can have as many VIDs as the Switch has memory in its VLAN table to store them.

Because some devices on a network may be tag-unaware, a decision must be made at each port on a tag-aware device before packets are transmitted - should the packet to be transmitted have a tag or not? If the transmitting port is connected to a tag-unaware device, the packet should be untagged. If the transmitting port is connected to a tag-aware device, the packet should be tagged.

Tagging and Untagging

Every port on an 802.1Q compliant switch can be configured as tagging or untagging.

Ports with tagging enabled will put the VID number, priority and other VLAN information into the header of all packets that flow into and out of it. If a packet has previously been tagged, the port will not alter the packet, thus keeping the VLAN information intact. Other 802.1Q compliant devices on the network to make packet-forwarding decisions can then use the VLAN information in the tag.

Ports with untagging enabled will strip the 802.1Q tag from all packets that flow into and out of those ports. If the packet doesn't have an 802.1Q VLAN tag, the port will not alter the packet. Thus, all packets received by and forwarded by an untagging port will have no 802.1Q VLAN information. (Remember that the PVID is only used internally within the Switch). Untagging is used to send packets from an 802.1Q-compliant network device to a non-compliant network device.

Ingress Filtering

A port on a switch where packets are flowing into the Switch and VLAN decisions must be made is referred to as an ingress port. If ingress filtering is enabled for a port, the Switch will examine the VLAN information in the packet header (if present) and decide whether or not to forward the packet.

If the packet is tagged with VLAN information, the ingress port will first determine if the ingress port itself is a member of the tagged VLAN. If it is not, the packet will be dropped. If the ingress port is a member of the 802.1Q VLAN, the Switch then determines if the destination port is a member of the 802.1Q VLAN. If it is not, the packet is dropped. If the destination port is a member of the 802.1Q VLAN, the packet is forwarded and the destination port transmits it to its attached network segment.

If the packet is not tagged with VLAN information, the ingress port will tag the packet with its own PVID as a VID (if the port is a tagging port). The switch then determines if the destination port is a member of the same VLAN (has the same VID) as the ingress port. If it does not, the packet is dropped. If it has the same VID, the packet is forwarded and the destination port transmits it on its attached network segment.

This process is referred to as ingress filtering and is used to conserve bandwidth within the Switch by dropping packets that are not on the same VLAN as the ingress port at the point of reception. This eliminates the subsequent processing of packets that will just be dropped by the destination port.

Default VLANs

The Switch initially configures one VLAN, VID = 1, called "default." The factory default setting assigns all ports on the Switch to the "default." As new VLANs are configured in Port-based mode, their respective member ports are removed from the "default."

Packets cannot cross VLANs. If a member of one VLAN wants to connect to another VLAN, the link must be through an external router.



NOTE: If no VLANs are configured on the Switch, then all packets will be forwarded to any destination port. Packets with unknown destination addresses will be flooded to all ports. Broadcast and multicast packets will also be flooded to all ports.

An example is presented below:

VLAN Name	VID	Switch Ports
-----------	-----	--------------

System (default)	1	5, 6, 7, 8, 21, 22, 23, 24
Engineering	2	9, 10, 11, 12
Marketing	3	13, 14, 15, 16
Finance	4	17, 18, 19, 20
Sales	5	1, 2, 3, 4

Table 3 - 1 VLAN Example – Assigned Ports

Port-based VLANs

Port-based VLANs limit traffic that flows into and out of switch ports. Thus, all devices connected to a port are members of the VLAN(s) the port belongs to, whether there is a single computer directly connected to a switch, or an entire department.

On port-based VLANs, NICs do not need to be able to identify 802.1Q tags in packet headers. NICs send and receive normal Ethernet packets. If the packet's destination lies on the same segment, communications take place using normal Ethernet protocols. Even though this is always the case, when the destination for a packet lies on another switch port, VLAN considerations come into play to decide if the packet gets dropped by the Switch or delivered.

VLAN Segmentation

Take for example a packet that is transmitted by a machine on Port 1 that is a member of VLAN 2. If the destination lies on another port (found through a normal forwarding table lookup), the Switch then looks to see if the other port (Port 10) is a member of VLAN 2 (and can therefore receive VLAN 2 packets). If Port 10 is not a member of VLAN 2, then the packet will be dropped by the Switch and will not reach its destination. If Port 10 is a member of VLAN 2, the packet will go through. This selective forwarding feature based on VLAN criteria is how VLANs segment networks. The key point being that Port 1 will only transmit on VLAN 2.

VLAN and Trunk Groups

The members of a trunk group have the same VLAN setting. Any VLAN setting on the members of a trunk group will apply to the other member ports.



NOTE: In order to use VLAN segmentation in conjunction with port trunk groups, first set the port trunk group(s), and then configure the VLAN settings. To change the port trunk grouping with VLANs already in place it is unnecessary to reconfigure the VLAN settings after changing the port trunk group settings. VLAN settings will automatically change in conjunction with the change of the port trunk group settings.

Protocol VLANs

The xStack® DGS -3400 Switch Series incorporates the idea of protocol-based VLANs. This standard, defined by the IEEE 802.1v standard maps packets to protocol-defined VLANs by examining the type octet within the packet header to discover the type of protocol associated with it. After assessing the protocol, the Switch will forward the packets to all ports within the protocol-assigned VLAN. This feature will benefit the administrator by better balancing load sharing and enhancing traffic classification. The Switch supports fourteen pre-defined protocols for configuration. The user may also choose a protocol that is not one of the fourteen defined protocols by properly configuring the *userDefined* protocol VLAN. The supported protocols for the protocol VLAN function on this switch include IP, IPX, DEC LAT, SNAP, NetBIOS, AppleTalk, XNS, SNA, IPv6, RARP and VINES.


Static VLAN Entry

This window is used to create static VLAN entries on the Switch.

To view this window, click **L2 Features > VLAN > Static VLAN Entries**, as shown below.

Add					
Total Entries: 1					
Current Static VLAN Entries					
VID	VLAN Name	Ports	Advertisement	Modify	Delete
1	default	1:1-1:24	Enabled	Modify	X

Figure 3 - 4 Current Static VLAN Entries window

The **Current Static VLAN Entries** window lists all previously configured VLANs by VLAN ID and VLAN Name. To delete an existing 802.1Q VLAN, click the corresponding  button under the Delete heading.

To create a new 802.1Q VLAN, click the **Add** button in the Current Static VLAN Entries window. A new window will appear, as shown below, to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new window.

Static VLAN																									
Unit	VID	VLAN Name																							Advertisement
1																									Disabled
Port Settings		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
None		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Egress		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Forbidden		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port Settings		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Tag		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Egress		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Forbidden		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Apply

[Show All Static VLAN Entries](#)

Figure 3 - 5 Current Static VLAN Entries - Add window

Click **Apply** to implement the changes. To return to the Current Static VLAN Entries window, click the [Show All Static VLAN Entries](#) link.

To change an existing 802.1Q VLAN entry, click the **Modify** button of the corresponding entry in the Current Static VLAN Entries window. A new menu will appear to configure the port settings and to assign a unique name and number to the new VLAN. See the table below for a description of the parameters in the new menu.



NOTE: The Switch supports up to 4k static VLAN entries.

Static VLAN																									
Unit	VID	VLAN Name																							Advertisement
1	1	default																							Enabled
Port Settings		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
Tag		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
None		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Egress		<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
Forbidden		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Port Settings		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Tag		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Egress		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Forbidden		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
<input type="button" value="Apply"/>																									
Show All Static VLAN Entries																									

Figure 3 - 6 Static VLAN window – Edit window

The following parameters can be configured or viewed:

Parameter	Description
Unit	Select the switch in the switch stack for which to configure VLANs.
VID	Allows the entry of a VLAN ID in the Add window, or displays the VLAN ID of an existing VLAN in the Modify window. VLANs can be identified by either the VID or the VLAN name.
VLAN Name	Allows the entry of a name for the new VLAN in the Add window, or for editing the VLAN name in the Modify window.
Advertisement	Enabling this function will allow the Switch to send out GVRP packets to outside sources, notifying that they may join the existing VLAN.
Port Settings	Allows an individual port to be specified as member of a VLAN.
Tag	Specifies the port as either 802.1Q tagging or 802.1Q untagged. Checking the box will designate the port as Tagged.
None	Allows an individual port to be specified as a non-VLAN member.
Egress	Select this to specify the port as a static member of the VLAN. Egress member ports are ports that will be transmitting traffic for the VLAN. These ports can be either tagged or untagged.
Forbidden	Select this to specify the port as not being a member of the VLAN and that the port is forbidden from becoming a member of the VLAN dynamically.

Click **Apply** to implement the changes. To return to the Current Static VLAN Entries window, click the [Show All Static VLAN Entries](#) link.

VLAN Trunk

This window is used to configure VLAN trunk settings.

To view this window, click **L2 Features > VLAN > VLAN Trunk**, as shown below.

Figure 3 - 7 VLAN Trunk Global Settings window

The following parameters can be configured:

Parameter	Description
VLAN Trunk Status	Use the pull-down menu to enable or disable VLAN trunk global status.
State	Use the pull-down menu to enable or disable VLAN trunk port state.
Member Ports	Enter the ports for VLAN trunk. Tick the All Ports check box to select all ports.

Click **Apply** to implement the changes.

GVRP Settings

The **GVRP Settings** window allows the user to determine whether the Switch will share its VLAN configuration information with other GARP VLAN Registration Protocol (GVRP) enabled switches. In addition, Ingress Checking can be used to limit traffic by filtering incoming packets whose PVID does not match the PVID of the port. Results can be seen in the table under the configuration settings, as seen below.

To view this window, click **L2 Features > VLAN > GVRP Settings**, as shown on the right:

GVRP Settings							
Unit	From	To	GVRP	Ingress Check	Acceptable Frame Type	PVID	Apply
1	Port 1	Port 1	Disabled	Enabled	Admit All		Apply

GVRP Table				
Port	PVID	GVRP	Ingress Check	Acceptable Frame Type
1	1	Disabled	Enabled	All Frames
2	1	Disabled	Enabled	All Frames
3	1	Disabled	Enabled	All Frames
4	1	Disabled	Enabled	All Frames
5	1	Disabled	Enabled	All Frames
6	1	Disabled	Enabled	All Frames
7	1	Disabled	Enabled	All Frames
8	1	Disabled	Enabled	All Frames
9	1	Disabled	Enabled	All Frames
10	1	Disabled	Enabled	All Frames
11	1	Disabled	Enabled	All Frames
12	1	Disabled	Enabled	All Frames
13	1	Disabled	Enabled	All Frames
14	1	Disabled	Enabled	All Frames
15	1	Disabled	Enabled	All Frames
16	1	Disabled	Enabled	All Frames
17	1	Disabled	Enabled	All Frames
18	1	Disabled	Enabled	All Frames
19	1	Disabled	Enabled	All Frames
20	1	Disabled	Enabled	All Frames
21	1	Disabled	Enabled	All Frames
22	1	Disabled	Enabled	All Frames
23	1	Disabled	Enabled	All Frames
24	1	Disabled	Enabled	All Frames

Figure 3 - 8 GVRP Settings window

The following fields can be configured:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From / To	These two fields allow the range of ports that will be included in the Port-based VLAN created using the 802.1Q Port Settings window, to be specified.
GVRP	The GARP VLAN Registration Protocol (GVRP) enables the port to dynamically become a member of a VLAN. GVRP is <i>Disabled</i> by default.
Ingress Check	This field can be toggled using the space bar between <i>Enabled</i> and <i>Disabled</i> . <i>Enabled</i> enables the port to compare the VID tag of an incoming packet with the PVID number assigned to the port. If the two are different, the port filters (drops) the packet. <i>Disabled</i> disables ingress filtering. Ingress Checking is <i>Enabled</i> by default.
Acceptable Frame Type	This field denotes the type of frame that will be accepted by the port. The user may choose between <i>Tagged Only</i> , which means only VLAN tagged frames will be accepted, and <i>Admit All</i> , which mean both tagged and untagged frames will be accepted. <i>Admit All</i> is enabled by default.
PVID	The read-only field in the 802.1Q Port Table shows the current PVID assignment for each port, which may be manually assigned to a VLAN when created in the 802.1Q Port Settings table. The Switch's default is to assign all ports to the default VLAN with a VID of 1. The PVID is used by the port to tag outgoing, untagged packets, and to make filtering decisions about incoming packets. If the port is specified to accept only tagged frames - as tagging, and an untagged packet is forwarded to the port for transmission, the port will add an 802.1Q tag using the PVID to write the VID in the tag. When the packet arrives at its destination, the receiving device will use the PVID to

make VLAN forwarding decisions. If the port receives a packet, and Ingress filtering is enabled, the port will compare the VID of the incoming packet to its PVID. If the two are unequal, the port will drop the packet. If the two are equal, the port will receive the packet.

Click **Apply** to implement the changes.

Double VLANs

Double or Q-in-Q VLANs allow network providers to expand their VLAN configurations to place customer VLANs within a larger inclusive VLAN, which adds a new layer to the VLAN configuration. This lets large ISP's create L2 Virtual Private Networks and also create transparent LANs for their customers, which will connect two or more customer LAN points without over-complicating configurations on the client's side. Not only will over-complication be avoided, but also now the administrator has over 4000 VLANs in which over 4000 VLANs can be placed, therefore greatly expanding the VLAN network and enabling greater support of customers utilizing multiple VLANs on the network.

Double VLANs are basically VLAN tags placed within existing IEEE 802.1Q VLANs which we will call SPVIDs (Service Provider VLAN IDs). These VLANs are marked by a TPID (Tagged Protocol ID), configured in hex form to be encapsulated within the VLAN tag of the packet. This identifies the packet as double-tagged and segregates it from other VLANs on the network, therefore creating a hierarchy of VLANs within a single packet.

Here is an example Double VLAN tagged packet.

Destination Address	Source Address	SPVLAN (TPID + Service Provider VLAN Tag)	802.1Q CEVLAN Tag (TPID + Customer VLAN Tag)	Ether Type	Payload
---------------------	----------------	---	--	------------	---------

Consider the example below:

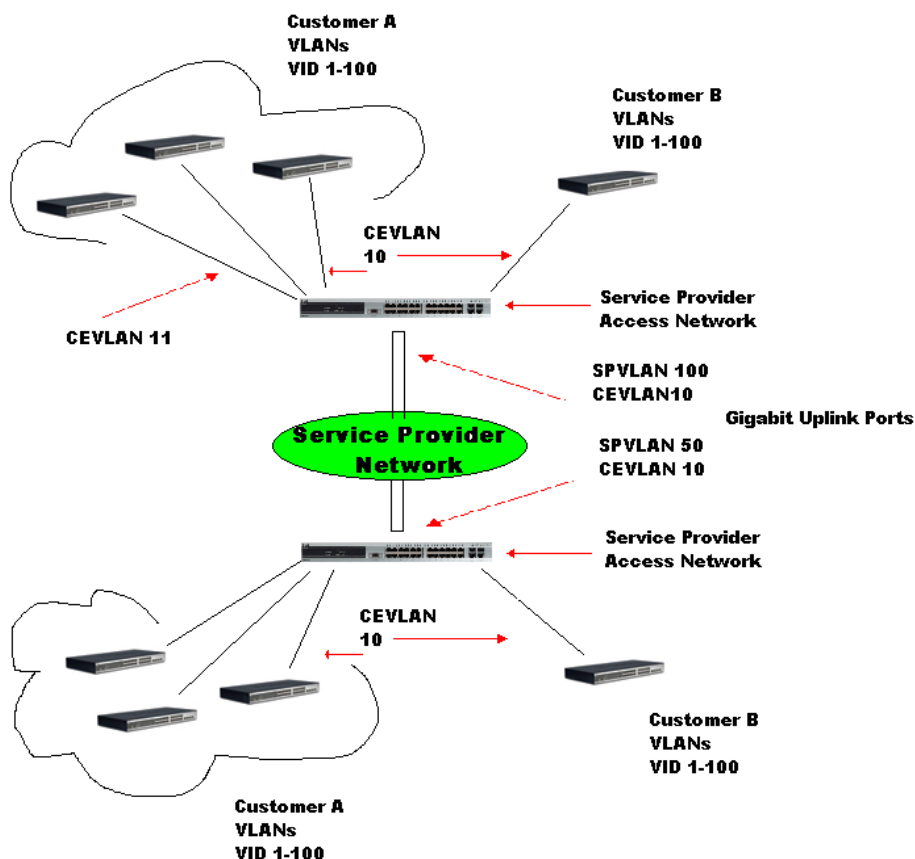


Figure 3 - 9 Double VLAN Example

In this example, the Service Provider Access Network switch (Provider edge switch) is the device creating and configuring Double VLANs. Both CEVLANs (Customer VLANs) 10 and 11, are tagged with the SPVID 100 on the Service Provider Access Network and therefore belong to one VLAN on the Service Provider's network, thus being a member of two VLANs. In this way,

the Customer can retain its normal VLAN and the Service Provider can congregate multiple Customer VLANs within one SP-VLAN, thus greatly regulating traffic and routing on the Service Provider switch. This information is then routed to the Service Provider's main network and regarded there as one VLAN, with one set of protocols and one routing behavior.

Regulations for Double VLANs

Some rules and regulations apply with the implementation of the Double VLAN procedure.

1. All ports must be configured for the SPVID and its corresponding TPID on the Service Provider's edge switch.
2. All ports must be configured as Access Ports or Uplink ports. Access ports can only be Ethernet ports while Uplink ports must be Gigabit ports.
3. Provider Edge switches must allow frames of at least 1522 bytes or more, due to the addition of the SPVID tag.
4. Access Ports must be an un-tagged port of the service provider VLANs. Uplink Ports must be a tagged port of the service provider VLANs.
5. The switch cannot have both double and normal VLANs co-existing. Once the change of VLAN is made, all Access Control lists are cleared and must be reconfigured.
6. Once Double VLANs are enabled, GVRP must be disabled.
7. All packets sent from the CPU to the Access ports must be untagged.
8. The following functions will not operate when the switch is in Double VLAN mode:
 - Guest VLANs
 - Web-based Access Control
 - IP Multicast Routing
 - GVRP
 - All Regular 802.1Q VLAN functions

Double VLAN Settings

This window is used to enable or disable the double VLAN State settings.

To view this window, click **L2 Features > VLAN > Double VLAN**, as shown below.

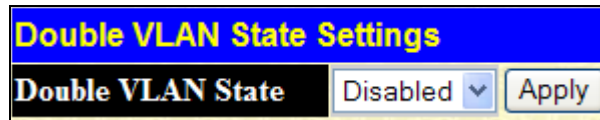


Figure 3 - 10 Double VLAN State Settings window

Choose *Enabled* using the pull-down menu and click **Apply**. The user will be prompted with the following warning window. Click **OK** to continue.

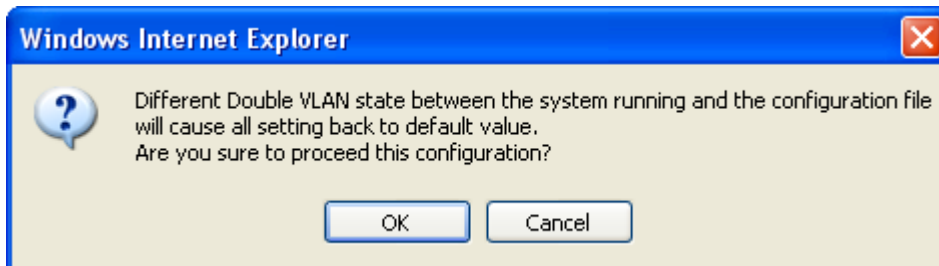


Figure 3 - 11 Alert window

After being prompted with a success message, the user will be presented with this window to configure for Double VLANs.



Figure 3 - 12 Double VLAN State Settings window

Parameters shown in the previous window are explained below:

Parameter	Description
Double VLAN State	Use the pull-down menu to enable or disable the Double VLAN function on this Switch. Enabling the Double VLAN will return all previous VLAN configurations to the factory default settings and remove Static VLAN configurations from the GUI.
SPVID	The VLAN ID number of this potential Service Provider VLAN.
VLAN Name	The name of the VLAN on the Switch.
TPID	The tagged protocol ID of the corresponding VLAN that will be used in identification of this potential Double VLAN, written in hex form.

The user may view configurations for a Double VLAN by clicking its corresponding **View** button, which will display the following read-only window.

Double VLAN Information	
SPVID	1
VLAN Name	default
TPID	0x8100
Uplink Ports	
Access Ports	1:1-1:24
Unknown Ports	
Show Double VLAN Entries	

Figure 3 - 13 Double VLAN State Settings - View window

Parameters shown in the previous window are explained below:

Parameter	Description
SPVID	The VLAN ID number of this potential Service Provider VLAN.
VLAN Name	The name of the VLAN on the Switch.
TPID	The tagged protocol ID of the corresponding VLAN that will be used in identification of this potential Double VLAN, written in hex form.
Uplink Ports	These ports are set as uplink ports on the Switch. Uplink ports are for connecting Switch VLANs to the Service Provider VLANs on a remote source.
Access Ports	These are the ports that are set as access ports on the Switch. Access ports are for connecting Switch VLANs to customer VLANs.
Unknown Ports	These are the ports that are a part of the VLAN but have yet to be defined as Access or Uplink ports.

To return to the Double VLAN State Settings window, click the [Show Double VLAN Entries](#) link.

To create a Double VLAN, click the **Add** button, revealing the following window for the user to configure.

Double VLAN Creation	
VLAN Name	<input type="text"/>
SPVID (1-4094)	<input type="text"/>
TPID (0x0-0xffff)	<input type="text" value="0x8100"/>
<input type="button" value="Apply"/>	
Show Double VLAN Entries	

Figure 3 - 14 Double VLAN State Settings - Add window

To create a Double VLAN, enter the following parameters and click **Apply**.

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as a Double VLAN.
SPVID	Enter the VID for the Service Provider VLAN with an integer between 1 and 4094.
TPID	Enter the TPID in hex form to aid in packet identification of the Service Provider VLAN.

Click **Apply** to implement the changes. To return to the Double VLAN State Settings window, click the [Show Double VLAN Entries](#) link.

To configure the parameters for a previously created Service Provider VLAN, click the **Modify** button of the corresponding SPVID in the Double VLAN State Settings window. The following window will appear for the user to configure.

Figure 3 - 15 Double VLAN State Settings – Modify window

The following parameters can be configured:

Parameter	Description
VLAN Name	The name of the pre-configured VLAN name to be configured.
TPID (0x0-0xffff)	The tagged protocol ID. Enter the new TPID in hex form to aid in packet identification of the Service Provider VLAN.
Operation	Allows one of the following three acts to be performed: <i>Add ports</i> – Will allow users to add ports to this Service Provider VLAN using the Port List field below. <i>Delete ports</i> – Will allow users to remove ports from the Service Provider VLAN configured, using the Port List field below. <i>Config TPID</i> – Will allow users to configure the Tagged Protocol ID of the Service Provider VLAN, in hex form.
Port Type	Allows the user to choose the type of port being utilized by the Service Provider VLAN. The user may choose: <i>Access</i> – Access ports are for connecting Switch VLANs to customer VLANs. <i>Uplink</i> – Uplink ports are for connecting Switch VLANs to the Provider VLANs on a remote source.
Port List	Use the From and To fields to set a list of ports to be placed in, or removed from, the Service Provider VLAN. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.

Click **Apply** to implement the changes. To return to the Double VLAN State Settings window, click the [Show Double VLAN Entries](#) link.

PVID Auto Assign

This window allows the user to enable or disable the PVID Auto Assign feature on the Switch.

To view this window, click **L2 Features > VLAN > PVID Auto Assign**, as shown below.

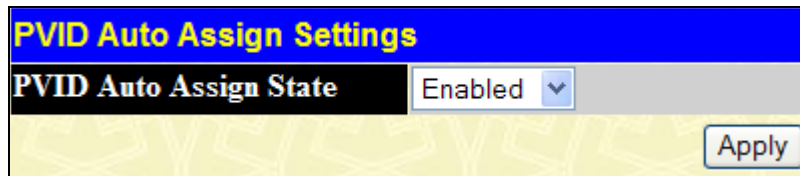


Figure 3 - 16 PVID Auto Assign Settings window

When *Enabled*, PVID will be automatically assigned when adding a port to a VLAN as an untagged member port. Click **Apply** to implement the change.

MAC-based VLAN Settings

This table is used to create new MAC-based VLAN entries and search, edit and delete existing entries.

To view this window click **L2 Features > VLAN > MAC-based VLAN Settings**, as shown below.

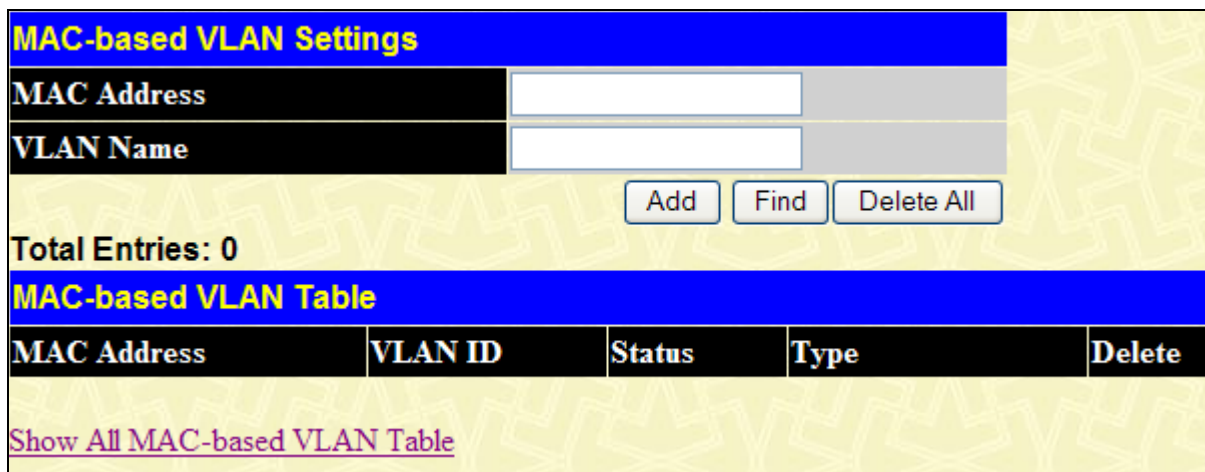


Figure 3 - 17 MAC-based VLAN Settings window

The following fields can be set:

Parameter	Description
MAC Address	Specify the MAC address to be reauthenticated by entering it into the MAC Address field.
VLAN Name	Enter the VLAN name of a previously configured VLAN.

Click **Find**, **Add** or **Delete All** for changes to take effect. To see all MAC-based VLAN entries, click the [Show All MAC-based VLAN Table](#) link.

Protocol VLAN

Protocol VLAN groups can be created on the Switch. The purpose of these Protocol VLAN groups is to identify ingress untagged packets and quickly and accurately send them to their destination. Ingress untagged packets can be identified by a protocol value in the packet header, which has been stated here by the user. Once identified, these packets can be tagged with the appropriate tags for VLAN and priority and then relayed to their destination.

The following is a list of protocol values for some common protocols.

Protocol	Type Header in Hexadecimal Form
IP over Ethernet	0x0800
IPX 802.3	0xFFFF
IPX 802.2	0xE0E0
IPX SNAP	0x8137
IPX over Ethernet2	0x8137
decLAT	0x6004
SNA 802.2	0x0404
netBios	0xF0F0
XNS	0x0600
VINES	0x0BAD
IPV6	0x86DD
AppleTalk	0x809B
RARP	0x8035
SNA over Ethernet2	0x80D5

Table 3 - 2 Protocol VLAN and the corresponding protocol value

To achieve this goal, users must first properly set the type of protocol, along with the identifying value located in the packet header and apply it to a protocol group, which is identified by an ID number. Once the group has been created and configured, then users must add it to a port or set of ports using the **Protocol VLAN Port Settings** window, and configure the appropriate VLAN and priority tags for these untagged packets. When these actions are completed and saved to the switch, then the ingress and untagged packets can be appropriately dealt with and forwarded through the switch.

Protocol VLAN Group Settings

This window is used to begin the Protocol Group VLAN configurations.

To view this window, click **L2 Features > VLAN > Protocol VLAN > Protocol VLAN Group Settings**, as shown below.

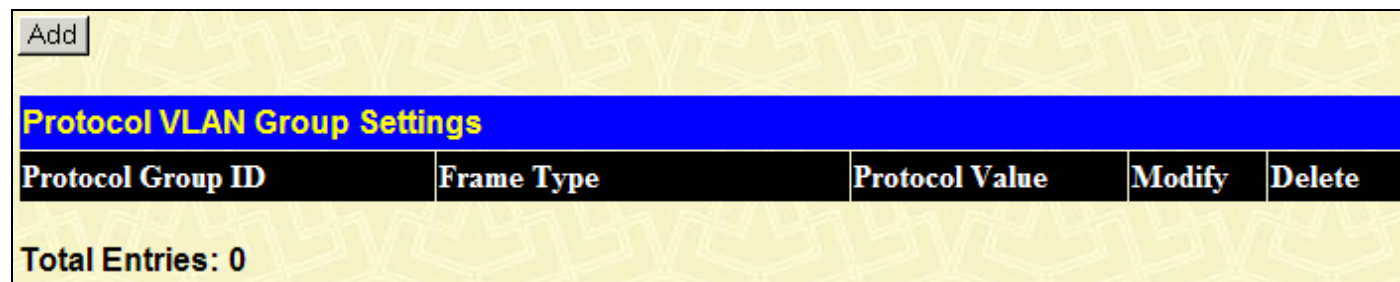


Figure 3 - 18 Protocol VLAN Group Settings window

Click the **Add** button to reveal the following window for the user to configure:

Figure 3 - 19 Protocol VLAN Group - Add window

The Add and Modify windows of the **Protocol VLAN Group** hold the following fields to be configured:

Parameter	Description
Group ID (1-16)	Enter an integer from 1 to 16 to identify the protocol VLAN group being created here. For the Modify window, this field will display the Protocol Group ID number of the group being configured.
Action	Use the pull-down menu to add or delete the protocol to this group. This protocol is identified using the following Protocol field.
Protocol	Use the pull-down menu to select the frame type to be added or deleted from this profile. The frame type indicates the frame format. The user has three choices for frame type: <ul style="list-style-type: none"> • <i>Ethernet II</i> – Choose this parameter if you wish this protocol group to employ the Ethernet II frame type. In this frame type, the protocol is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following Protocol Value. • <i>IEEE802.3 SNAP</i> – Choose this parameter if you wish this protocol group to employ the Sub Network Access Protocol (SNAP) frame type. For this frame type, the protocol is identified by the 16-bit (2 octet) IEEE802.3 type field in the packet header, which is to be stated using the following Protocol Value. • <i>IEEE802.3 LLC</i> – Choose this parameter if you wish this protocol group to employ the Link Logical Control (LLC) frame type. For this frame type, the protocol is identified by the 2-octet IEEE802.3 Link Service Access Point (LSAP) pair field in the packet header, which is to be stated using the following Protocol Value. The first octet defines the Destination Service Access Point value and the second octet is the Source Service Access Point (SSAP) value.
Protocol Value	Enter the corresponding protocol value of the protocol identified in the previous field. This value must be stated in a hexadecimal form.

Click **Apply** to implement changes made. To return to the Protocol VLAN Group Settings window, click the [Show All Protocol VLAN Group Entries](#) link.

Protocol VLAN Port Settings

The following window is used to add a Protocol VLAN Group profile to a port or list of ports and adjust the tags for incoming untagged packets before being relayed through the Switch.

To view this window, click **L2 Features > VLAN > Protocol VLAN > Protocol VLAN Port Settings**, as shown below.

Figure 3 - 20 Protocol VLAN Port Settings window

The following fields may be configured:

Parameter	Description
Port List	Use this parameter to assign ports to a Protocol VLAN Group or remove them from the Protocol VLAN Group. Ticking the Select All Ports check box will configure this Protocol VLAN Group to all ports on the switch.
Action	Use the pull-down menu to add or delete the following Group ID to or from the ports selected in the previous field.
Group ID (1-16)	Enter the ID number of the Protocol VLAN Group for which to add or remove from the selected ports. Ticking the Select All Groups check box will apply all Protocol VLAN groups to the ports listed in the Port List field.
VLAN ID / VLAN Name	Use this field to add a VLAN to be associated with this configuration. Select the correct radio button if you are using a VLAN Name or a VID (VLAN ID).

Click **Apply** to implement changes made. The Protocol VLAN Port Table in the bottom half of the window will display correctly configured ports to Protocol Group configurations, along with associated VLANs and priorities. Users may use the Port List Search in the middle of the window to display configurations based on ports on the switch. Clicking the [Show All Protocol VLAN Port Table Entries](#) link will display all Protocol VLAN Port Table entries.

Subnet VLAN

Subnet VLAN is used to assign VID for untagged or priority-tagged frame based on source IPv4 or IPv6 address.

If the ingress frame is untagged or priority-tagged frame, the source IPv4 address or the upper 64 bits of the IPv6 source address of the frame will be used as a key to lookup the subnet VLAN table. If there is a matched entry, the VID of the frame will be picked up from the matched entry. If the frame is untagged, the priority will be picked up from it too. For priority-tagged packet, its priority will not change.

Subnet VLAN can support to make an IP address mapping to any existent static VLAN. But it can't support to make a same IP address mapping to more than one VLAN.

The VLAN classification precedence is configurable on each port. The default value is MAC-based VLAN classification precedence.

Note:

1. If the IP address of the received untagged packet is match two entries in the table. The longest-prefix match order is used.
2. For make the subnet VLAN can work well, must add the ingress port into the VLAN member ports.
3. The subnet VLAN maybe affects the authorization protocol, such as 802.1x, WAC, JWAC, MAC access control and Compound authentication. Because the authorized port l will be assigned to target VLAN and set its PVID to target VLAN ID, if subnet VLAN takes effect, the ingress packets on this port maybe not are classified to target VLAN.

Subnet VLAN Settings

This window is used to add, modify or delete subnet VLAN entries

To view this window, click **L2 Features > VLAN > Subnet VLAN > Subnet VLAN Settings**, as shown below.

Action	VLAN	Network Address	Priority
Add ▾	VLAN Name ▾	IPv4 Address ▾	0 ▾

Total Entries: 0 View All Delete All

IP Address/Subnet Mask	VLAN	Priority	Delete
------------------------	------	----------	--------

Figure 3 - 21 Subnet VLAN Settings window

The following fields may be configured:

Parameter	Description
Action	Use the pull-down menu to add, delete or find the subnet VLAN.
VLAN	Use the pull-down menu to select VLAN name or VID to enter in the field next to it.
Network Address	Use the pull-down menu to select IPv4 or IPv6 address to enter in the field next to it.
Priority	Use the pull-down menu to select priority 0 to 7.

Click the **Apply** button to implement the changes. Click **View All** to see all the entries. Click **Delete All** to remove all entries.

VLAN Precedence Settings

This window is used to configure VLAN classification precedence on each port. With VLAN classification precedence, you can specify the order of MAC-based VLAN classification and subnet VLAN classification.

To view this window, click **L2 Features > VLAN > Subnet VLAN > VLAN Precedence Settings**, as shown below.

VLAN Precedence Settings				
Unit	From	To	VLAN Precedence	Apply
1	Port 1	Port 1	MAC-based VLAN	Apply

VLAN Precedence Table	
Port	VLAN Precedence
1	MAC-based VLAN
2	MAC-based VLAN
3	MAC-based VLAN
4	MAC-based VLAN
5	MAC-based VLAN
6	MAC-based VLAN
7	MAC-based VLAN
8	MAC-based VLAN
9	MAC-based VLAN
10	MAC-based VLAN
11	MAC-based VLAN
12	MAC-based VLAN
13	MAC-based VLAN
14	MAC-based VLAN
15	MAC-based VLAN
16	MAC-based VLAN
17	MAC-based VLAN
18	MAC-based VLAN
19	MAC-based VLAN
20	MAC-based VLAN
21	MAC-based VLAN
22	MAC-based VLAN
23	MAC-based VLAN
24	MAC-based VLAN

Figure 3 - 22 VLAN Precedence Settings window

The following fields may be configured:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From / To	These two fields allow the range of ports that will be included in the VLAN precedence.
VLAN Precedence	Use the pull-down menu to select the VLAN precedence as MAC-based VLAN or Subnet VLAN.

Click **Apply** to implement the changes.

Trunking

Understanding Port Trunk Groups

Port trunk groups are used to combine a number of ports together to make a single high-bandwidth data pipeline. DGS-3400 Series supports up to 32 port trunk groups with 2 to 8 ports in each group. A potential bit rate of 8000 Mbps can be achieved.

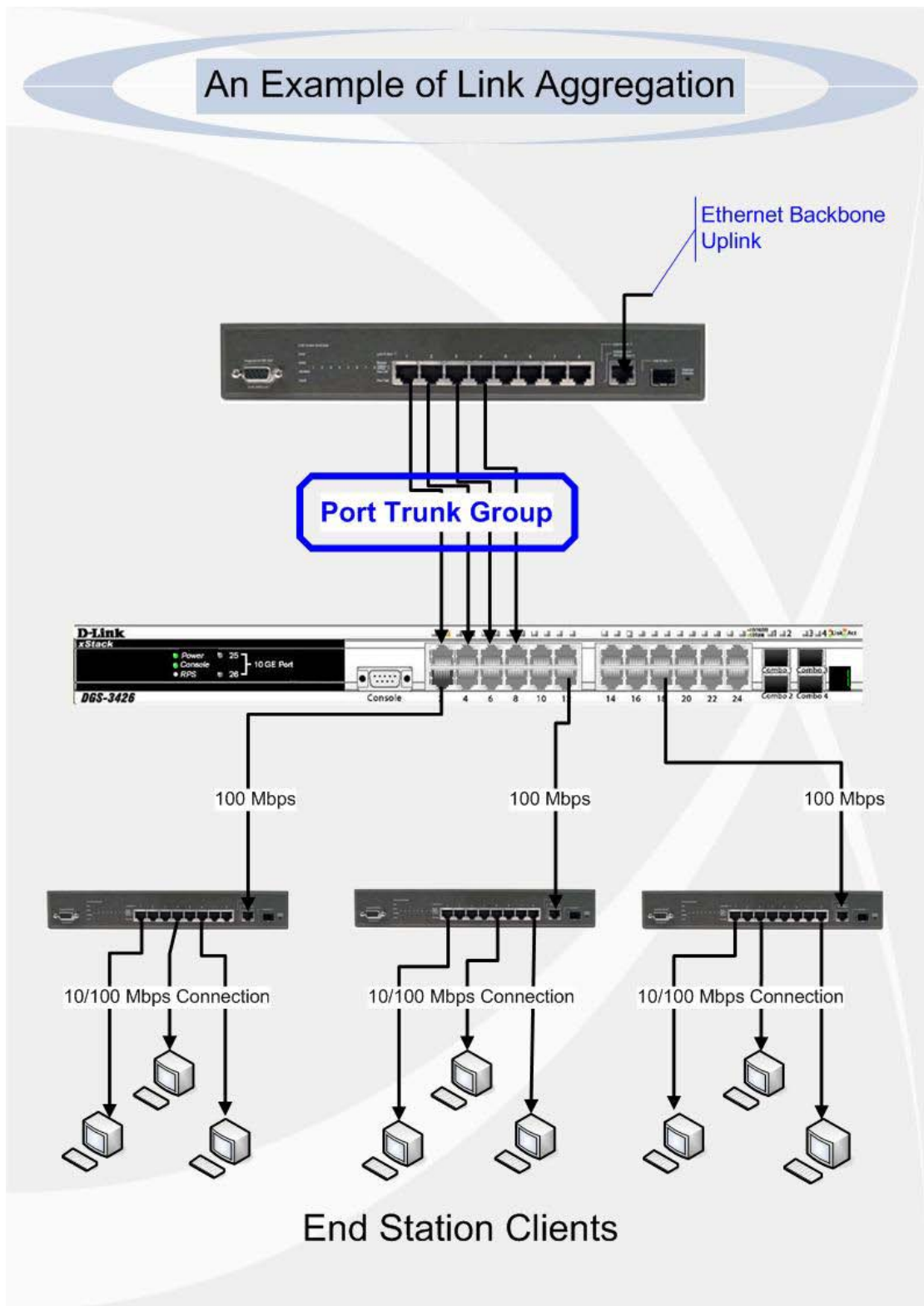


Figure 3 - 23 Example of Port Trunk Group

The Switch treats all ports in a trunk group as a single port. Data transmitted to a specific host (destination address) will always be transmitted over the same port in a trunk group. This allows packets in a data stream to arrive in the same order they were sent.



NOTE: If any ports within the trunk group become disconnected, packets intended for the disconnected port will be load shared among the other linked ports of the link aggregation group.



NOTE: Trunking may be done across switches in the switch stack without any limitations.

Link aggregation allows several ports to be grouped together and to act as a single link. This gives a bandwidth that is a multiple of a single link's bandwidth.

Link aggregation is most commonly used to link a bandwidth intensive network device or devices, such as a server, to the backbone of a network.

The Switch allows the creation of up to 32 link aggregation groups, each group consisting of 2 to 8 links (ports). The (optional) Gigabit ports can only belong to a single link aggregation group. All of the ports in the group must be members of the same VLAN, and their STP status, static multicast, traffic control; traffic segmentation and 802.1p default priority configurations must be identical. Port locking, port mirroring and 802.1X must not be enabled on the trunk group. Further, the LACP aggregated links must all be of the same speed and should be configured as full duplex.

The Master Port of the group is to be configured by the user, and all configuration options, including the VLAN configuration that can be applied to the Master Port, are applied to the entire link aggregation group.

Load balancing is automatically applied to the ports in the aggregated group, and a link failure within the group causes the network traffic to be directed to the remaining links in the group.

The Spanning Tree Protocol will treat a link aggregation group as a single link, on the switch level. On the port level, the STP will use the port parameters of the Master Port in the calculation of port cost and in determining the state of the link aggregation group. If two redundant link aggregation groups are configured on the Switch, STP will block one entire group; in the same way STP will block a single port that has a redundant link.

Link Aggregation

This table is used to configure port trunking on the switch.

To view this window, click **L2 Features > Trunking > Link Aggregation**, as shown below.

<input type="button" value="Add"/>				
Total Entries: 1				
Link Aggregation Group Entries				
Group ID	State	Ports	Modify	Delete
2	Disabled	1:1, 1:3	<input type="button" value="Modify"/>	<input type="button" value="X"/>

Figure 3 - 24 Link Aggregation Group Entries window

To delete a port trunk group, click the corresponding under the Delete heading in the Link Aggregation Group Entries table.

To add port trunk groups, click the **Add** button to display the window shown as below.

Link Aggregation Group Configuration																										
Group ID	<input type="text"/>																									
Type	LACP ▾																									
State	Disabled ▾																									
Master Port	1 ▾ Port 1 ▾																									
Unit	1 ▾																									
Member Ports	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	-	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	-
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Flooding Port	X																									
<input type="button" value="Apply"/>																										
<p>Note(1): It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Link Aggregation Group Entries</p>																										

Figure 3 - 25 Link Aggregation Group Entries - Add window

To edit a port trunk group, click the corresponding **Modify** button to see the window shown as below.

Link Aggregation Group Configuration																										
Group ID	2																									
Type	LACP																									
State	Disabled																									
Master Port	1 Port 1																									
Unit	1																									
Member Ports	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	-	
	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	-
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Active Ports	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	-	
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	-
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Flooding Port	X																									
<input type="button" value="Apply"/>																										
<p>Note(1): It is only valid to set up at most 8 member ports of any one trunk group and a port can be a member of only one trunk group at a time.</p> <p>Show All Link Aggregation Group Entries</p>																										

Figure 3 - 26 Link Aggregation Group Entries - Edit window

The user-changeable parameters are as follows:

Parameter	Description
Group ID	Select an ID number for the group, between 1 and 32.
Type	This pull-down menu allows users to select between <i>Static</i> and <i>LACP</i> (Link Aggregation Control Protocol). LACP allows for the automatic detection of links in a Port Trunking Group.
State	Trunk groups can be toggled between <i>Enabled</i> and <i>Disabled</i> . This is used to turn a port trunking group on or off. This is useful for diagnostics, to quickly isolate a bandwidth intensive network device or to have an absolute backup aggregation group that is not under automatic control.
Master Port	Choose the Master Port for the trunk group using the pull-down menu.
Unit	Select the switch in the switch stack to be modified.
Member Ports	Choose the members of a trunked group. Up to eight ports per group can be assigned to a group.
Active Port	Shows the port that is currently forwarding packets.
Flooding Port	A trunking group must designate one port to allow transmission of broadcasts, multicasts and

unknown unicasts.

After setting the previous parameters, click **Apply** to allow your changes to be implemented. Successfully created trunk groups will be show in the Link Aggregation Group Entries window. To return to the Link Aggregation Group Entries window, click the [Show All Link Aggregation Group Entries](#) link.



NOTE: To configure the Algorithm for Link Aggregation, please refer back to the DGS-3400 Web Management Tool and select the Link Aggregation Algorithm located on that web page. The description for this function may be found in the explanation for the Device Information window located earlier in this manual.

LACP Port Settings

The **LACP Port Settings** window is used in conjunction with the **Link Aggregation** window to create port trunking groups on the Switch. Using the following window, the user may set which ports will be active and passive in processing and sending LACP control frames.

To view this window, click **L2 Features > Trunking > LACP Port Settings**, as shown below.

LACP Port Settings				
Unit	From	To	Mode	Apply
1	Port 1	Port 1	Active	Apply
LACP Port Information-Unit 1				
Port	Mode			
1	Passive			
2	Passive			
3	Passive			
4	Passive			
5	Passive			
6	Passive			
7	Passive			
8	Passive			
9	Passive			
10	Passive			
11	Passive			
12	Passive			
13	Passive			
14	Passive			
15	Passive			
16	Passive			
17	Passive			
18	Passive			
19	Passive			
20	Passive			
21	Passive			
22	Passive			
23	Passive			
24	Passive			

Figure 3 - 27 LACP Port Settings window

The user may set the following parameters:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From / To	A consecutive group of ports may be configured starting with the selected port.
Mode	<i>Active</i> – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed

dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP.

Passive – LACP ports that are designated as passive cannot initially send LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, one end of the connection must have “active” LACP ports (see above).

After setting the previous parameters, click **Apply** to allow your changes to be implemented. The LACP Port Information table on the LACP Port Settings window displays which ports are active and passive.

IGMP Snooping

Internet Group Management Protocol (IGMP) snooping allows the Switch to recognize IGMP queries and reports sent between network stations or devices and an IGMP host. When enabled for IGMP snooping, the Switch can open or close a port to a specific device based on IGMP messages passing through the Switch.

In order to use IGMP Snooping it must first be enabled for the entire Switch (see the **Device Information** window that opens when clicking the **Web Management Tool** at the top of the Web Manager menu in the left pane). Users may then fine-tune the settings for each VLAN using the **IGMP Snooping Settings** folder under **L2 Features**. When enabled for IGMP snooping, the Switch can open or close a port to a specific multicast group member based on IGMP messages sent from the device to the IGMP host or vice versa. The Switch monitors IGMP messages and discontinues forwarding multicast packets when there are no longer hosts requesting that they continue.

IGMP Snooping Settings

This window is used to *Enable, Disable or Modify* the IGMP Snooping Settings on the Switch.

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Settings**, as shown below.

IGMP Multicast Router Only Settings					
IGMP Multicast Router Only				Disabled ▾	Apply
IGMP Snooping Data Driven Learning Settings					
Data Driven Max Learning Entry Value (1-960)				56	Apply
Total Entries: 1					
IGMP Snooping Settings					
VID	VLAN Name	State	Querier State	Modify	
1	default	Disabled	Disabled	Modify	

Figure 3 - 28 IGMP Multicast Router Only Settings window

The following parameters can be configured:

Parameter	Description
IGMP Multicast Router Only	Use the pull-down menu to enable or disable the IGMP multicast router.
IGMP Snooping Data Driven Learning Settings (1-960)	Enter a value between 1 and 960 for data driven max learning entry.

Click **Apply** to implement the changes.

Click the corresponding **Modify** button in the IGMP Snooping Settings table to open the window, as shown below.

IGMP Snooping Settings - Edit	
VID	<input type="text" value="1"/>
VLAN Name	<input type="text" value="default"/>
Query Interval (1-65535)	<input type="text" value="125"/> sec
Max Response Time (1-25)	<input type="text" value="10"/> sec
Robustness Variable (1-255)	<input type="text" value="2"/>
Last Member Query Interval (1-25)	<input type="text" value="1"/> sec
Version (1-3)	<input type="text" value="3"/>
Host Timeout (1-16711450)	<input type="text" value="260"/> sec
Router Timeout (1-16711450)	<input type="text" value="260"/> sec
Leave Timer (1-6375)	<input type="text" value="2"/> sec
Querier State	Disabled <input type="button" value="v"/>
Querier Router Behavior	Non-Querier
State	Disabled <input type="button" value="v"/>
Fast Leave	Disabled <input type="button" value="v"/>
Report Suppression	Disabled <input type="button" value="v"/>
Data Driven Learning State	Enabled <input type="button" value="v"/>
Data Driven Learning Aged Out	Disabled <input type="button" value="v"/>
Data Driven Group Expiry Time (1-65535)	<input type="text" value="260"/> sec
<input type="button" value="Apply"/>	
Show All IGMP Snooping Entries	

Figure 3 - 29 IGMP Snooping Settings – Edit window

The following parameters may be viewed or modified:

Parameter	Description
VID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to modify the IGMP Snooping Settings for.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting IGMP queries. Entries between 1 and 65535 seconds are allowed. Default = 125.
Max Response Time (1-25)	This determines the maximum amount of time in seconds allowed before sending an IGMP response report. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = 10.
Robustness Variable (1-255)	Adjust this variable according to expected packet loss. If packet loss on the VLAN is expected to be high, the Robustness Variable should be increased to accommodate increased packet loss. This entry field allows an entry of 1 to 255. Default = 2.
Last Member Query Interval	This field specifies the maximum amount of time between group-specific query

(1- 25)	messages, including those sent in response to leave group messages. Default = 1.
Version (1-3)	Configure the IGMP version of the query packet which will be sent by the router.
Host Timeout (1-16711450 sec)	This is the maximum amount of time in seconds allowed for a host to continue membership in a multicast group without the Switch receiving a host membership report. Default = 260.
Route Timeout (1-16711450 sec)	This is the maximum amount of time in seconds a route is kept in the forwarding table without receiving a membership report. Default = 260.
Leave Timer (1-6375 sec)	This specifies the maximum amount of time in seconds between the Switch receiving a leave group message from a host, and the Switch issuing a group membership query. If no response to the membership query is received before the Leave Timer expires, the (multicast) forwarding entry for that host is deleted. The default setting is 2 seconds.
Querier State	Choose <i>Enabled</i> to enable transmitting IGMP Query packets or <i>Disabled</i> to disable. The default is <i>Disabled</i> .
Querier Router Behavior	This read-only field describes the current querier state of the Switch, whether Querier, which will send out Multicast Listener Query Messages to links, or Non-Querier, which will not send out Multicast Listener Query Messages.
State	Select <i>Enabled</i> to implement IGMP Snooping. This field is <i>Disabled</i> by default.
Fast Leave	The Fast Leave option may be <i>Enabled</i> or <i>Disabled</i> (default). This allows an interface to be pruned without sending group-specific queries.
Report Suppression	This parameter allows the user to enable the Report Suppression function. When IGMP report suppression is <i>Enabled</i> , the Switch sends the first IGMP report from all hosts for a group to all the multicast routers. The Switch does not send the remaining IGMP reports for the group to the multicast routers. If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the Switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the Switch forwards all IGMPv3 reports for a group to the multicast devices. The default is <i>Disabled</i> .
Receive Query Count	The field appears when selecting State as <i>Enabled</i> . This is used to show the number of IGMP query packets DUT received from specified VLAN when the IGMP snooping is enabled.
Send Query Count	The field appears when selecting State as <i>Enabled</i> . This is used to show the number of IGMP query packets DUT sent from specified VLAN when the IGMP snooping is enabled.
Data Driven Learning State	Select <i>Enabled</i> or <i>Disabled</i> for data driven learning status.
Data Driven Learning Aged Out	Use the pull-down menu to enable or disable the aging out of the entry.
Data Driven Group Expiry Time (1-65535)	Specify the data driven group lifetime in seconds. This parameter is valid only when Data Driven Learning Aged Out is <i>Enabled</i> .

Click **Apply** to implement the new settings. Click the [Show All IGMP Snooping Entries](#) link to return to the IGMP Snooping Settings window.

Router Port Settings

A static router port is a port that has a multicast router attached to it. Generally, this router would have a connection to a WAN or to the Internet. Establishing a router port will allow multicast packets coming from the router to be propagated through the network, as well as allowing multicast messages (IGMP) coming from the network to be propagated to the router.

A router port has the following behavior:

- All IGMP Report packets will be forwarded to the router port.

- IGMP queries (from the router port) will be flooded to all ports.

All UDP multicast packets will be forwarded to the router port. Because routers do not send IGMP reports or implement IGMP snooping, a multicast router connected to the router port of a Layer 3 switch would not be able to receive UDP data streams unless the UDP multicast packets were all forwarded to the router port.

A router port will be dynamically configured when IGMP query packets, RIPv2 multicast, DVMRP multicast or PIM-DM multicast packets are detected flowing into a port.

To view this window click **L2 Features > IGMP Snooping > Router Port Settings**, as shown below.

Total Entries: 1		
Router Port Settings		
VID	VLAN Name	Modify
1	default	Modify

Figure 3 - 30 Router Port Settings window

This window displays all of the current entries to the Switch's static router port table. To modify an entry, click the **Modify** button. This will open the **Router Port** window, as shown below.

Router Port																										
VID	1																									
VLAN Name	default																									
Unit	1 ▾																									
Member Ports																										
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	-	
None	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	-
Static	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	-
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	-
Port	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Static	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Forbidden	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Apply																										
Show All Router Port Entries																										

Figure 3 - 31 Router Port Settings - Edit window

The following parameters can be set:

Parameter	Description
VID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN where the multicast router is attached.
VLAN Name	This is the name of the VLAN where the multicast router is attached.
Unit	Select the switch in the switch stack to be modified.
Member Ports	Ports on the Switch that will have a multicast router attached to them. There are three options for which to configure these ports:

	<p><i>None</i> – Click this option to not set these ports as router ports</p> <p><i>Static</i> – Click this option to designate a range of ports as being connected to a multicast-enabled router. This command will ensure that all packets with this router as its destination will reach the multicast-enabled router.</p> <p><i>Forbidden</i> – Click this option to designate a port or range of ports as being forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets</p>
--	--

Click **Apply** to implement the new settings. Click the [Show All Router Port Entries](#) link to return to the router Port Settings window.

IGMP Snooping Static Group Settings

This table is used to configure the current IGMP snooping static group information on the Switch.

To view this window, click **L2 Features > IGMP Snooping > IGMP Snooping Static Group Settings**, as shown below.

Figure 3 - 32 IGMP Snooping Static Group Settings window

The following parameters can be configured:

Parameter	Description
VID	The list of the VLAN IDs for which to create IGMP snooping static group information.
VLAN Name	The name of the VLAN for which to create IGMP snooping static group information.
IP Address	The static group address for which to create IGMP snooping static group information.

To search for an entry enter the appropriate information and click **Find**. To display all current entries on the Switch click **View All**. To add a new entry, click **Add**, and the following window will be displayed.

Figure 3 - 33 IGMP Snooping Static Group - Add window

To modify an entry, click the corresponding **Modify** button, and the following window will be displayed.

Figure 3 - 34 IGMP Static Group Modify window

The following fields can be configured or viewed:

Parameter	Description
VID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN the user wishes to add.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN the user wishes to add.
IP Address	The static group address for which to create IGMP snooping static group information.
Port List	The ports that will belong to this group.
Action	Specifies to Add or Delete the IGMP Static group entry.

Click **Apply** to implement the changes. To return to the IGMP Snooping Static Group Settings window, click the [Show All IGMP Snooping Static Group Entries](#) link.

ISM VLAN Settings

In a switching environment, multiple VLANs may exist. Every time a multicast query passes through the Switch, the switch must forward separate different copies of the data to each VLAN on the system, which, in turn, increases data traffic and may clog up the traffic path. To lighten the traffic load, multicast VLANs may be incorporated. These multicast VLANs will allow the Switch to forward this multicast traffic as one copy to recipients of the multicast VLAN, instead of multiple copies.

Regardless of other normal VLANs that are incorporated on the Switch, users may add any ports to the multicast VLAN where they wish multicast traffic to be sent. Users are to set up a source port, where the multicast traffic is entering the switch, and then set the ports where the incoming multicast traffic is to be sent. The source port cannot be a recipient port and if configured to do so, will cause error messages to be produced by the switch. Once properly configured, the stream of multicast data will be relayed to the receiver ports in a much more timely and reliable fashion.

Restrictions and Provisos

The Multicast VLAN feature of this switch does have some restrictions and limitations, such as:

1. Multicast VLANs can only be implemented on edge switches.
2. Member ports and source ports can be used in multiple ISM VLANs. But member ports and source ports cannot be the same port in a specific ISM VLAN.
3. The Multicast VLAN is exclusive with normal 802.1q VLANs, which means that VLAN IDs (VIDs) and VLAN Names of 802.1q VLANs and ISM VLANs cannot be the same. Once a VID or VLAN Name is chosen for any VLAN, it cannot be used for any other VLAN.
4. The normal display of configured VLANs will not display configured Multicast VLANs.
5. Once an ISM VLAN is enabled, the corresponding IGMP snooping state of this VLAN will also be enabled. Users cannot disable the IGMP feature for an enabled ISM VLAN.
6. User can configure 16 ranges of multicast groups, no upper limitation of each range.
7. Router ports cannot be deleted if they are the source ports for ISM VLANs.

The following windows will allow users to create and configure multicast VLANs for the switch.

To view this windows, click **L2 Features > IGMP Snooping > ISM VLAN Settings**, as shown below.

VID	VLAN Name	Replace Source IP	State	Remap Priority	Modify	Group List	Delete
2	DG	0.0.0.0	Disabled	None	Modify	Modify	X

Total Entries: 1

Figure 3 - 35 IGMP Snooping Multicast VLAN Table window

The previous window displays the settings for previously created Multicast VLANs.

To create a new Multicast VLAN, click the **Add** button in the top left-hand corner of the screen, which will produce the following window to be configured.

IGMP Snooping Multicast VLAN Settings

VLAN Name:

VID (2-4094):

Remap Priority (0-7): None Replace Priority

[Show IGMP Snooping Multicast VLAN Entries](#)

Figure 3 - 36 IGMP Snooping Multicast VLAN Table - Add window

The following fields can be configured or viewed:

Parameter	Description
VLAN Name	Enter a name for the ISM VLAN into the field.

VID (2-4094)	Enter a VLAN ID between 2 and 4094.
Remap Priority (0-7)	Enter a value between 0 and 7. The remap priority is associated with the data traffic to be forwarded on the multicast VLAN. Tick the None check box to use the packet's original priority.

Click **Apply** to implement the changes. To return to the IGMP Snooping Multicast VLAN Table window, click the [Show IGMP Snooping Multicast VLAN Entries](#) link.

To edit multicast VLAN in the IGMP Snooping Multicast VLAN Table window, click the corresponding **Modify** button of the corresponding ISM VLAN you wish to modify.

IGMP Snooping Multicast VLAN Settings

VLAN Name	<input type="text" value="DG"/>
VID (2-4094)	<input type="text" value="2"/>
State	<input type="button" value="Disabled"/> ▾
Member Port	<input type="text"/>
Tagged Member Ports	<input type="text"/>
Source Port	<input checked="" type="radio"/> <input type="text"/>
Untagged Source Port	<input type="radio"/> <input type="text"/>
Replace Source IP	<input type="text" value="0.0.0.0"/>
Remap Priority (0-7)	<input checked="" type="checkbox"/> None <input type="checkbox"/> Replace Priority

[Show IGMP Snooping Multicast VLAN Entries](#)

Figure 3 - 37 IGMP Snooping Multicast VLAN Table - Edit window

Both the Add and Modify **IGMP Snooping Multicast VLAN Settings** windows have the following configurable fields:

Parameter	Description
VLAN Name	Enter the name of the new Multicast VLAN to be created. This name can be up to 32 characters in length. This field will display the pre-created name of a Multicast VLAN in the Modify window.
VID (2-4094)	Add or edit the corresponding VLAN ID of the Multicast VLAN. Users may enter a value between 2 and 4094.
State	Use the pull-down menu to enable or disable the selected Multicast VLAN.
Member Port	Enter a port or list of ports to be added to the Multicast VLAN. Member ports will become the untagged members of the multicast VLAN.
Tagged Member Ports	Enter a port or list of ports to be added to the Multicast VLAN as a tagged member port.
Source Port	Enter a port or list of ports to be added to the Multicast VLAN. Source ports will become the untagged members of the multicast VLAN.
Untagged Source Port	Click the radio button and enter a port or list of ports to be added to the .multicast VLAN. Source ports will become the untagged members of the multicast VLAN.

Replace Source IP	This field is used to replace the source IP address of incoming packets sent by the host before being forwarded to the source port.
Remap Priority (0-7)	Enter a value between 0 and 7. The remap priority is associated with the data traffic to be forwarded on the multicast VLAN. Tick the None check box to use the packet's original priority.

Click **Apply** to implement the settings. To return to the IGMP Snooping Multicast VLAN Table window, click the [Show IGMP Snooping Multicast VLAN Entries](#) link.

To configure the new Multicast VLAN Group List, click the corresponding **Modify** button in the IGMP Snooping Multicast VLAN Table which will reveal the following window to be configured.

IGMP Snooping Multicast VLAN Group List Settings

VLAN Name	From	To
DG	0.0.0.0	0.0.0.0

IGMP Snooping Multicast VLAN Group List

No.	VLAN Name	VLAN ID	From	To	Delete
1	DG	2			

[Show IGMP Snooping Multicast VLAN Entries](#)

Figure 3 - 38 IGMP Snooping Multicast VLAN Group List Settings

Enter an existing VLAN Name and range and click **Add**. To remove all entries click the **Remove All** button. To return to the IGMP Snooping Multicast VLAN Table window, click the [Show IGMP Snooping Multicast VLAN Entries](#) link.

Limited IP Multicast Address Range Settings

This window allows the user to specify which multicast address(es) reports are to be received on specified ports on the Switch. This function, also known as IGMP Filtering, will therefore limit the number of reports received and the number of multicast groups configured on the Switch. The user may set an IP address or range of IP addresses to accept reports (Permit) or deny reports (Deny) coming into the specified switch ports.

To view this window, click **L2 Features > IGMP Snooping > Limited Multicast Address Range Settings**, as shown below.

To configure Limited IP Multicast Range:

Choose the port or sequential range of ports using the From/To port pull-down menus.

Use the remaining pull-down menus to configure the parameters described below:

Limited Multicast Address Range									
Unit	From	To	From	To	Access	State	Apply	Delete	Delete All
1	Port 1	Port 1	224.0.0.0	239.255.255.255	Permit	Enabled	Apply	Delete	Delete All

Limited IP Multicast Address Range Port Table				
Port	From	To	State	Access
1:1			Disabled	None
1:2			Disabled	None
1:3			Disabled	None
1:4			Disabled	None
1:5			Disabled	None
1:6			Disabled	None
1:7			Disabled	None
1:8			Disabled	None
1:9			Disabled	None
1:10			Disabled	None
1:11			Disabled	None
1:12			Disabled	None
1:13			Disabled	None
1:14			Disabled	None
1:15			Disabled	None
1:16			Disabled	None
1:17			Disabled	None
1:18			Disabled	None
1:19			Disabled	None
1:20			Disabled	None
1:21			Disabled	None
1:22			Disabled	None
1:23			Disabled	None
1:24			Disabled	None

Total Entries: 0

Figure 3 - 39 Limited IP Multicast Address Range window

The following parameters can be configured:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From / To	Enter the port range for which to begin the Limited IP Multicast Range configuration. Enter the multicast IP range of addresses.
Access	Toggle the Access field to either <i>Permit</i> or <i>Deny</i> to limit or grant access to a specified range of Multicast addresses on a particular port or range of ports.
State	Toggle the State field to either <i>Enabled</i> or <i>Disabled</i> for a given port or group of ports where access is to be either permitted or denied.

Click **Apply** to implement the new settings on the Switch. Click **Delete** to remove the configured range from the settings. Click **Delete All** to delete all Limited IP Multicast settings.

MLD Snooping

Multicast Listener Discovery (MLD) Snooping is an IPv6 function used similarly to IGMP snooping in IPv4. It is used to discover ports on a VLAN that are requesting multicast data. Instead of flooding all ports on a selected VLAN with multicast traffic, MLD snooping will only forward multicast data to ports that wish to receive this data through the use of queries and reports produced by the requesting ports and the source of the multicast traffic.

MLD snooping is accomplished through the examination of the layer 3 part of an MLD control packet transferred between end nodes and a MLD router. When the Switch discovers that this route is requesting multicast traffic, it adds the port directly attached to it into the correct IPv6 multicast table, and begins the process of forwarding multicast traffic to that port. This entry in the multicast routing table records the port, the VLAN ID and the associated multicast IPv6 multicast group address and then considers this port to be a active listening port. The active listening ports are the only ones to receive multicast group data.

MLD Control Messages

Three types of messages are transferred between devices using MLD snooping. These three messages are all defined by three ICMPv6 packet headers, labeled 130, 131 and 132.

1. **Multicast Listener Query** – Similar to the IGMPv2 Host Membership Query for IPv4, and labeled as 130 in the ICMPv6 packet header, this message is sent by the router to ask if any link is requesting multicast data. There are two types of MLD query messages emitted by the router. The General Query is used to advertise all multicast addresses that are ready to send multicast data to all listening ports, and the Multicast Specific query, which advertises a specific multicast address that is also ready. These two types of messages are distinguished by a multicast destination address located in the IPv6 header and a multicast address in the Multicast Listener Query Message.
2. **Multicast Listener Report** – Comparable to the Host Membership Report in IGMPv2, and labeled as 131 in the ICMP packet header, this message is sent by the listening port to the Switch stating that it is interested in receiving multicast data from a multicast address in response to the Multicast Listener Query message.
3. **Multicast Listener Done** – Akin to the Leave Group Message in IGMPv2, and labeled as 132 in the ICMPv6 packet header, this message is sent by the multicast listening port stating that it is no longer interested in receiving multicast data from a specific multicast group address, therefore stating that it is “done” with the multicast data from this address. Once this message is received by the Switch, it will no longer forward multicast traffic from a specific multicast group address to this listening port.

MLD Snooping Settings

This window is used to *Enable* or *Disable* the MLD Multicast Router and configure the settings for MLD snooping.

To view this window, click **L2 Features > MLD Snooping > MLD Snooping Settings**, as shown below.

MLD Multicast Router Only Settings				
MLD Multicast Router Only		Disabled ▼		
Apply				
MLD Snooping Data Driven Learning Settings				
Data Driven Max Learning Entry Value (1-511)		56		
Apply				
Total Entries: 1				
MLD Snooping Settings				
VID	VLAN Name	State	Querier State	Modify
1	default	Disabled	Disabled	Modify

Figure 3 - 40 MLD Multicast Router Only Settings window

The following parameters can be configured:

Parameter	Description
MLD Multicast Router Only	Use the pull-down menu to enable or disable the MLD multicast router.
MLD Snooping Data Driven Learning Settings (1-511)	Enter a value between 1 and 511 for data driven max learning entry.

Click **Apply** to implement the changes.

Click the corresponding **Modify** button in the MLD Snooping Settings table to open the window, as shown below.

MLD Snooping Settings - Edit	
VID	1
VLAN Name	default
Query Interval (1-65535)	125 sec
Max Response Time (1-25)	10 sec
Robustness Variable (1-255)	2
Last Listener Query Interval (1-25)	1 sec
Version (1-2)	2
Node Timeout (1-16711450)	260 sec
Router Timeout (1-16711450)	260 sec
Done Timer (1-6375)	2 sec
Querier State	Disabled
Querier Router Behavior	Non-Querier
State	Disabled
Fast Done	Disabled
Data Driven Learning State	Enabled
Data Driven Learning Aged Out	Disabled
Data Driven Group Expiry Time (1-65535)	260 sec
<input type="button" value="Apply"/>	
Show All MLD Snooping Entries	

Figure 3 - 41 MLD Snooping Settings – Edit window

The following parameters may be viewed or modified:

Parameter	Description
VID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN for which to modify the MLD Snooping Settings.
VLAN Name	This is the VLAN Name that, along with the VLAN ID, identifies the VLAN for which to modify the MLD Snooping Settings.
Query Interval (1-65535)	The Query Interval field is used to set the time (in seconds) between transmitting MLD queries. Entries between 1 and 65535 seconds are allowed. Default = 125.
Max Response Time (1-25)	This determines the maximum amount of time in seconds allowed to wait for a

	response for MLD port listeners. The Max Response Time field allows an entry between 1 and 25 (seconds). Default = 10.
Robustness Variable (1-255)	Provides fine-tuning to allow for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If the packet loss rate in a subnet is expected to be high, the user may wish to increase this interval.
Last Listener Query Interval (1-25)	The maximum amount of time to be set between group-specific query messages. This interval may be reduced to lower the amount of time it takes a router to detect the loss of a last listener group. The user may set this interval between 1 and 25 seconds with a default setting of 1 second.
Version (1-2)	Configure the MLD version of the query packet which will be sent by the router.
Node Timeout (1-16711450)	Specifies the link node timeout, in seconds. After this timer expires, this node will no longer be considered as listening node. Default setting is 260 seconds.
Router Timeout (1-16711450)	Specifies the maximum amount of time a router can remain in the Switch's routing table as a listening node of a multicast group without the Switch receiving a node listener report. Default setting is 260 seconds.
Done Timer (1-6375)	Specifies the maximum amount of time a router can remain in the Switch after receiving a done message from the group without receiving a node listener report. Default setting is 2 seconds.
Querier State	Choose <i>Enabled</i> to enable transmitting MLD Snooping Query packets or <i>Disabled</i> to disable. The default is <i>Disabled</i> .
Querier Router Behavior	This read-only field describes the current querier state of the Switch, whether Querier, which will send out Multicast Listener Query Messages to links, or Non-Querier, which will not send out Multicast Listener Query Messages.
State	Used to enable or disable MLD snooping for the specified VLAN. This field is <i>Disabled</i> by default.
Fast Done	This parameter allows the user to enable the <i>fast done</i> function. Enabled, this function will allow members of a multicast group to leave the group immediately when a <i>done</i> message is received by the Switch.
Data Driven Learning State	Select <i>Enabled</i> or <i>Disabled</i> for data driven learning status.
Data Driven Learning Aged Out	Use the pull-down menu to enable or disable the aging out of the entry.
Data Driven Group Expiry Time (1-65535)	Specify the data driven group lifetime in seconds. This parameter is valid only when Data Driven Learning Aged Out is <i>Enabled</i> .

NOTE: The robustness variable of the MLD snooping querier is used in creating the following MLD message intervals:

Group Listener Interval – The amount of time that must pass before a multicast router decides that there are no more listeners present of a group on a network. Calculated as (robustness variable * query interval) + (1 * query interval).

Querier Present Interval – The amount of time that must pass before a multicast router decides that there are no other querier devices present. Calculated as (robustness variable * query interval) + (0.5 * query response interval).

Last Listener Query Count – The amount of group-specific queries sent before the router assumes there are no local listeners in this group. The default value is the value of the robustness variable.



Click **Apply** to implement changes made. Click the [Show All MLD Snooping Entries](#) link to return to the MLD Snooping Settings window.

MLD Router Port Settings

The following window is used to designate a port or range of ports as being connected to multicast enabled routers. When IPv6 routing control packets, such as DVMRP, OSPF or RIP, or MLD Query packets are found in an Ethernet port or specified VLAN, the Switch will set these ports as dynamic router ports. Once set, this will ensure that all packets with a multicast router as its destination will arrive at the multicast-enabled router, regardless of protocol. If the Router's Aging Time expires and no routing control packets or query packets are received by the port, that port will be removed from being a router port.

To view this window, click **L2 Features > MLD Snooping > MLD Router Port Settings**, as shown below.

Total Entries: 1		
MLD Router Port Settings		
VID	VLAN Name	Modify
1	default	<input type="button" value="Modify"/>

Figure 3 - 42 MLD Router Port Settings window

To configure the router ports settings for a specified VLAN, click its corresponding **Modify** button, which will produce the following window for the user to configure.

Router Port																										
VID	1																									
VLAN Name	default																									
Unit	1 <input type="button" value="v"/>																									
Member Ports																										
Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	-	
None	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	-
Static	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	-
Forbidden	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	-
Port	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
None	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Static	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Forbidden	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
<input type="button" value="Apply"/>																										
Show All Router Port Entries																										

Figure 3 - 43 MLD Router Port Settings - Edit window

The following parameters can be set:

Parameter	Description
VID	This is the VLAN ID that, along with the VLAN Name, identifies the VLAN where the MLD multicast router is attached.
VLAN Name	This is the name of the VLAN where the MLD multicast router is attached.
Unit	Select the switch in the switch stack to be modified.
Member Ports	Ports on the Switch that will have a multicast router attached to them. There are four options for

which to configure these ports:

None – Click this option to not set these ports as router ports

Static – Click this option to designate a range of ports as being connected to a multicast-enabled router. This command will ensure that all packets with this router as its destination will reach the multicast-enabled router.

Forbidden – Click this option to designate a port or range of ports as being forbidden from being connected to multicast enabled routers. This ensures that these configured forbidden ports will not send out routing packets

Click **Apply** to implement the new settings.

Loop-back Detection Global Settings

The Loop-back Detection function is used to identify loops occurring between the Switch and a device that is directly connected to it. This process is accomplished by the use of a Configuration Testing Protocol (CTP) packet that is generated by the switch. Users may set the dispatching time interval of the CTP packet and once a CTP packet has returned to the port from where it originated, the loop-back detection function will disable this port until the anomaly has ceased, and the loop-back occurrence will be noted in the Switch's log. Once the loop-back problem has stopped, this port will be automatically recovered in a time period that can also be specified by the user.

To view this window, click **L2 Features > Loopback Detection Global Settings**, as shown on the right:

Loopback Detection Global Settings				
Loopdetect Status	Disabled ▾			
Loopdetect Trap	None ▾			
Interval (1-32767)	10	sec		
Recover Timer (0 or 60-1000000)	60	sec		
Mode	Port Based ▾			
Apply				
Loopback Detection Port Settings				
Unit	From	To	State	Apply
1 ▾	Port 1 ▾	Port 1 ▾	Disabled ▾	Apply
Loopback Detection Port Based Table				
Port	Loopdetect State	Loop Status		
1	Disabled	Normal		
2	Disabled	Normal		
3	Disabled	Normal		
4	Disabled	Normal		
5	Disabled	Normal		
6	Disabled	Normal		
7	Disabled	Normal		
8	Disabled	Normal		
9	Disabled	Normal		
10	Disabled	Normal		
11	Disabled	Normal		
12	Disabled	Normal		
13	Disabled	Normal		
14	Disabled	Normal		
15	Disabled	Normal		
16	Disabled	Normal		
17	Disabled	Normal		
18	Disabled	Normal		
19	Disabled	Normal		
20	Disabled	Normal		
21	Disabled	Normal		
22	Disabled	Normal		
23	Disabled	Normal		
24	Disabled	Normal		

Figure 3 - 44 Loopback Detection Global Settings window

The following fields may be configured:

Parameter	Description
Loopdetect Status	Choose whether to globally enable or disable the Loop-back Detection function by using this pull-down menu.

Loopdetect Trap	<p><i>None</i> – The trap will not be sent in any situation.</p> <p><i>Loop Detected</i> – The trap is sent when the loop condition is detected.</p> <p><i>Loop Cleared</i> – The trap is sent when the loop condition is cleared.</p> <p><i>Both</i> – The trap will be sent for both conditions.</p>
Interval (1-32767)	Enter a time interval, between 1 and 32767 seconds, that CTP packets will be dispatched from loop-back detection-enabled ports. The default setting is 10 seconds.
Recover Timer (0 or 60-1000000)	Enter a time, in seconds that a port will have to wait before being recovered from a loop-back detection shutdown. The user may set a time between 60 and 1000000 seconds with a default setting of 60 seconds. The user may also enter a time of 0, which means that the port can only be recovered manually by the user. This is done by going to the Port Settings window (Administration > Port Configuration) and manually enabling these ports.
Mode	Use the pull-down menu to select <i>Port Based</i> or <i>VLAN Based</i> .
Unit	Select the switch in the switch stack to be modified.
From / To	Choose a port or group of ports that are to be enabled for the loop-back detection function.
State	Use the pull-down menu to enable or disable the loop-back function for the selected ports.

Click **Apply** to implement the changes.

Spanning Tree

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-1998 STP, 802.1D-2004 Rapid STP, and 802.1Q-2005 MSTP. 802.1D-1998 STP will be familiar to most networking professionals. However, since 802.1D-2004 RSTP and 802.1Q-2005 MSTP have been recently introduced to D-Link managed Ethernet switches, a brief introduction to the technology is provided below followed by a description of how to set up 802.1D-1998 STP, 802.1D-2004 RSTP, and 802.1Q-2005 MSTP.

802.1Q-2005 MSTP

Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing any of the three spanning tree protocols (STP, RSTP or MSTP).

This protocol will also tag BDPUs so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. An MSTI ID will classify these instances. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees.

Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

1. A configuration name defined by an alphanumeric string of up to 32 characters (defined in the **MST Configuration Identification** window in the Configuration Name field).
2. A configuration revision number (named here as a Revision Level and found in the **MST Configuration Identification** window) and;
3. A 4094-element table (defined here as a VID List in the **MST Configuration Identification** window), which will associate each of the possible 4094 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

1. The Switch must be set to the MSTP setting (found in the **STP Bridge Global Settings** window in the STP Version field)
2. The correct spanning tree priority for the MSTP instance must be entered (defined here as a Priority in the **MSTI Config Information** window when configuring MSTI ID settings).
3. VLANs that will be shared must be added to the MSTP Instance ID (defined here as a VID List in the **MST Configuration Identification** window when configuring an MSTI ID settings).

802.1D-2004 Rapid Spanning Tree

The Switch implements three versions of the Spanning Tree Protocol, the Multiple Spanning Tree Protocol (MSTP) as defined by the IEEE 802.1Q-2005, the Rapid Spanning Tree Protocol (RSTP) as defined by the IEEE 802.1D-2004 specification and a version compatible with the IEEE 802.1D-1998 STP. RSTP can operate with legacy equipment implementing IEEE 802.1D-1998; however the advantages of using RSTP will be lost.

The IEEE 802.1D-2004 Rapid Spanning Tree Protocol (RSTP) evolved from the 802.1D-1998 STP standard. RSTP was developed in order to overcome some limitations of STP that impede the function of some recent switching innovations, in particular, certain Layer 3 functions that are increasingly handled by Ethernet switches. The basic function and much of the terminology is the same as STP. Most of the settings configured for STP are also used for RSTP. This section introduces some new Spanning Tree concepts and illustrates the main differences between the two protocols.

Port Transition States

An essential difference between the three protocols is in the way ports transition to a forwarding state and in the way this transition relates to the role of the port (forwarding or not forwarding) in the topology. MSTP and RSTP combine the transition states disabled, blocking and listening used in 802.1D-1998 and creates a single state Discarding. In either case, ports do not forward packets. In the STP port transition states disabled, blocking or listening or in the RSTP/MSTP port state discarding, there is no functional difference, the port is not active in the network topology. Table 7-3 below compares how the three protocols differ regarding the port state transition.

All three protocols calculate a stable topology in the same way. Every segment will have a single path to the root bridge. All bridges listen for BPDU packets. However, BPDU packets are sent more frequently - with every Hello packet. BPDU packets are sent even if a BPDU packet was not received. Therefore, each link between bridges is sensitive to the status of the link. Ultimately this difference results in faster detection of failed links, and thus faster topology adjustment. A drawback of 802.1D-1998 is this absence of immediate feedback from adjacent bridges.

802.1Q-2005 MSTP	802.1D-2004 RSTP	802.1D-1998 STP	Forwarding	Learning
Disabled	Disabled	Disabled	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Blocking</i>	No	No
<i>Discarding</i>	<i>Discarding</i>	<i>Listening</i>	No	No
<i>Learning</i>	<i>Learning</i>	<i>Learning</i>	No	Yes
Forwarding	Forwarding	Forwarding	Yes	Yes

Table 3 - 3 Comparing Port States

RSTP is capable of a more rapid transition to a forwarding state - it no longer relies on timer configurations - RSTP compliant bridges are sensitive to feedback from other RSTP compliant bridge links. Ports do not need to wait for the topology to stabilize before transitioning to a forwarding state. In order to allow this rapid transition, the protocol introduces two new variables: the edge port and the point-to-point (P2P) port.

Edge Port

The edge port is a configurable designation used for a port that is directly connected to a segment where a loop cannot be created. An example would be a port connected directly to a single workstation. Ports that are designated as edge ports transition to a forwarding state immediately without going through the listening and learning states. An edge port loses its status if it receives a BPDU packet, immediately becoming a normal spanning tree port.

P2P Port

A P2P port is also capable of rapid transition. P2P ports may be used to connect to other bridges. Under RSTP/MSTP, all ports operating in full-duplex mode are considered to be P2P ports, unless manually overridden through configuration.

802.1D-1998/802.1D-2004/802.1Q-2005 Compatibility

MSTP or RSTP can interoperate with legacy equipment and is capable of automatically adjusting BPDU packets to 802.1D-1998 format when necessary. However, any segment using 802.1D-1998 STP will not benefit from the rapid transition and rapid topology change detection of MSTP or RSTP. The protocol also provides for a variable used for migration in the event that legacy equipment on a segment is updated to use RSTP or MSTP.

The Spanning Tree Protocol (STP) operates on two levels:

1. On the switch level, the settings are globally implemented.
2. On the port level, the settings are implemented on a per-user-defined group of ports basis.

STP Bridge Global Settings

This window is used to configure the STP Bridge Global Settings on the Switch.

To view this window, click **L2 Features > Spanning Tree > STP Bridge Global Settings**, as shown below.

STP Bridge Global Settings	
STP Status	Disabled <input type="button" value="v"/>
STP Version	RSTP <input type="button" value="v"/>
Hello Time (1-10 sec)	2 <input type="text"/>
Max Age (6-40 sec)	20 <input type="text"/>
Forward Delay (4-30 sec)	15 <input type="text"/>
Max Hops (1-40)	20 <input type="text"/>
TX Hold Count (1-10)	6 <input type="text"/>
Forwarding BPDU	Disabled <input type="button" value="v"/>
Loopback Detection	Enabled <input type="button" value="v"/>
LBD Recover Time (0 or 60-1000000)	60 <input type="text"/> sec
NNI BPDU Address	Dot1ad <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 3 - 45 STP Bridge Global Settings window (RSTP - default)

STP Bridge Global Settings	
STP Status	Disabled <input type="button" value="v"/>
STP Version	MSTP <input type="button" value="v"/>
Max Age (6-40 sec)	20 <input type="text"/>
Forward Delay (4-30 sec)	15 <input type="text"/>
Max Hops (1-40)	20 <input type="text"/>
TX Hold Count (1-10)	6 <input type="text"/>
Forwarding BPDU	Disabled <input type="button" value="v"/>
Loopback Detection	Enabled <input type="button" value="v"/>
LBD Recover Time (0 or 60-1000000)	60 <input type="text"/> sec
NNI BPDU Address	Dot1ad <input type="button" value="v"/>
<input type="button" value="Apply"/>	

Figure 3 - 46 STP Bridge Global Settings window (MSTP)

STP Bridge Global Settings	
STP Status	Disabled ▾
STP Version	STP compatible ▾
Hello Time (1-10 sec)	2
Max Age (6-40 sec)	20
Forward Delay (4-30 sec)	15
Max Hops (1-40)	20
TX Hold Count (1-10)	6
Forwarding BPDU	Disabled ▾
Loopback Detection	Enabled ▾
LBD Recover Time (0 or 60-1000000)	60 sec
NNI BPDU Address	Dot1ad ▾
Apply	

Figure 3 - 47 STP Bridge Global Settings window (STP Compatible)

See the table below for descriptions of the STP versions and corresponding setting options.



NOTE: The Hello Time cannot be longer than the Max. Age. Otherwise, a configuration error will occur. Observe the following formulas when setting the above parameters:

Max. Age $\leq 2 \times$ (Forward Delay - 1 second)

Max. Age $\leq 2 \times$ (Hello Time + 1 second)

Configure the following parameters for STP:

Parameter	Description
STP Status	Use the pull-down menu to globally enable or disable STP.
STP Version	Use the pull-down menu to choose the desired version of STP: <i>STP</i> – Select this parameter to set the Spanning Tree Protocol (STP) globally on the switch. <i>RSTP</i> – Select this parameter to set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. <i>MSTP</i> – Select this parameter to set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch.
Hello Time (1 - 10 sec)	The Hello Time can be set from 1 to 10 seconds. If the inputted Hello Time is more than 2, the Hello Time is also 2. This is the interval between two transmissions of BPDU packets sent by the Root Bridge to tell all other switches that it is indeed the Root Bridge. This field will only appear here when STP or RSTP is selected for the STP Version. For MSTP, the Hello Time must be set on a port per port basis. See the MST Port Settings section for further details.
Max Age (6 - 40 sec)	The Max Age may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20.

Forward Delay (4-30 sec)	The Forward Delay can be from 4 to 30 seconds. Any port on the Switch spends this time in the listening state while moving from the blocking state to the forwarding state.
Max Hops (1-40)	Used to set the number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BPDU packet and the information held for the port will age out. The user may set a hop count from 1 to 40. The default is 20. If the Max Hops is less than 6, the Max Hops is 6.
TX Hold Count (1-10)	Used to set the maximum number of Hello packets transmitted per interval. The count can be specified from 1 to 10. The default is 6.
Forwarding BPDU	This field can be <i>Enabled</i> or <i>Disabled</i> . When <i>Enabled</i> , it allows the forwarding of STP BPDU packets from other network devices. The default is <i>Disabled</i> .
Loopback Detection	When enabled, the Switch will temporarily block STP switch-wide when a BPDU packet has looped back. If the Switch detects its own BPDU packet coming back, it signifies a loop on the network – STP is automatically blocked and an alert is sent to the administrator. The default is <i>Enabled</i> .
LBD Recover Time	Time allowed (in seconds) for recovery when an STP Loopback is detected. After the timer has expired the Switch checks for an STP loopback, if no loopback detected, STP is resumed. Entering 0 will disable LBD recovery.
NNI BPDU Address	This field is used to configure the NNI port address. <i>dot1d</i> – Specifies STP’s BPDU MAC address of NNI port using the definition of 802.1d. <i>dot1ad</i> – Specifies STP’s PDU MAC address of NNI port using the definition of 802.1ad.

Click **Apply** to implement the changes.

MST Configuration Identification

The following windows allow the user to configure a MSTI instance on the Switch. These settings will uniquely identify a multiple spanning tree instance set on the Switch. The Switch initially possesses one CIST or Common Internal Spanning Tree of which the user may modify the parameters for but cannot change the MSTI ID for, and cannot be deleted.

To view this window, click **L2 Features > Spanning Tree > MST Configuration Identification**, as shown below.

The screenshot shows a web interface window titled "MST Configuration Identification". At the top left is an "Add" button. Below it is a table with two columns: "Configuration Name" and "Revision Level". The first row shows "00:21:91:53:3E:C8" and "0". Below this is another table with columns "MSTI ID", "VID List", and "Delete". The first row shows "CIST", "1-4094", and a delete icon (X). Below the table is a section titled "MST Configuration Identification Settings". It contains two input fields: "Configuration Name" with the value "00:21:91:53:3E:C8" and "Revision Level (0-65535)" with the value "0". An "Apply" button is located at the bottom right of the settings section.

Figure 3 - 48 MST Configuration Identification window

The window above contains the following information:

Parameter	Description
Configuration Name	A previously configured name set on the Switch to uniquely identify the MSTI (Multiple Spanning Tree Instance). If a configuration name is not set, this field will show the MAC address to the device running MSTP. This field can be set in the STP Bridge Global Settings window.
Revision Level	This value, along with the Configuration Name will identify the MSTP region configured on the Switch.
MSTI ID	This field shows the MSTI IDs currently set on the Switch. This field will always have the CIST MSTI, which may be configured but not deleted. Clicking the hyperlinked name will open a new window for configuring parameters associated with that particular MSTI.
VID List	This field displays the VLAN IDs associated with the specific MSTI.

Click  to remove the entry. Click the **Add** button will reveal the following window to configure:

Figure 3 - 49 MST Configuration Identification - Add window

Configure the following parameters to create a MSTI in the Switch:

Parameter	Description
MSTI ID	Enter a number between 1 and 15 to set a new MSTI on the Switch.
Type	<i>Create</i> is selected to create a new MSTI. No other choices are available for this field when creating a new MSTI.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.

Click **Apply** to implement changes made. Click the [Show MST configuration Table](#) link to return to the MST Configuration Identification window.

To configure the settings for the CIST, click its hyperlinked name in the MST Configuration Identification window, which will reveal the following window to configure:

Figure 3 - 50 MST Configuration Identification – Edit window

The user may configure the following parameters to configure the CIST on the Switch.

Parameter	Description
MSTI ID	The MSTI ID of the CIST is 0 and cannot be altered.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has 2 choices. <i>Add VID</i> – Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. <i>Remove VID</i> – Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094. This field is inoperable when configuring the CIST.

Click **Apply** to implement the changes. Click the [Show MST configuration Table](#) link to return to the MST Configuration Identification window.

To configure the parameters for a previously set MSTI, click its hyperlinked MSTI ID number, which will reveal the following window for configuration.

Figure 3 - 51 MST Configuration Identification – Edit window

The user may configure the following parameters for a MSTI on the Switch.

Parameter	Description
MSTI ID	Displays the MSTI ID previously set by the user.
Type	This field allows the user to choose a desired method for altering the MSTI settings. The user has four choices. <i>Add</i> – Select this parameter to add VIDs to the MSTI ID, in conjunction with the VID List parameter. <i>Remove</i> – Select this parameter to remove VIDs from the MSTI ID, in conjunction with the VID List parameter.
VID List (1-4094)	This field is used to specify the VID range from configured VLANs set on the Switch that the user wishes to add to this MSTI ID. Supported VIDs on the Switch range from ID number 1 to 4094. This parameter can only be utilized if the Type chosen is <i>Add</i> or <i>Remove</i> .

Click **Apply** to implement changes made. Click the [Show MST configuration Table](#) link to return to the MST Configuration Identification window.

MSTP Port Information

This window displays the current MSTP Port Information and can be used to update the port configuration for an MSTI ID. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.

To view this window, click **L2 Features > Spanning Tree > MSTP Port Information**, as shown below.

MSTI	Designated Bridge	Internal PathCost	Prio	Status	Role
0	N/A	200000	128	Disabled	Disabled
4	N/A	200000	128	Disabled	Disabled

Figure 3 - 52 MSTP Port Information window

To view the MSTI settings for a particular port, select the Port number, located in the top left hand corner of the screen and click **Apply**. To modify the settings for a particular MSTI Instance, click its hyperlinked MSTI ID, which will reveal the following window.

Figure 3 - 53 MSTP Port Information – Edit window

The user may configure the following parameters:

Parameter	Description
Instance ID	Displays the MSTI ID of the instance being configured. An entry of 0 in this field denotes the CIST (default MSTI).
Internal Cost (0=Auto)	This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is 0 (auto). There are two options: <i>0 (auto)</i> – Selecting this parameter for the <i>internalCost</i> will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. <i>value 1-200000000</i> – Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower Internal cost represents a quicker transmission.
Priority (0-240)	Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority.

Click **Apply** to implement the changes. Click the [Show MSTP Port Information Table-Port 1 of Unit 1](#) to return to the MSTP Port Information window.

STP Instance Settings

The following window displays MSTIs currently set on the Switch.

To view this window, click **L2 Features > Spanning Tree > STP Instance Settings**, as shown below.

STP Instance Settings			
Instance Type	Instance Status	Instance Priority	Priority
CIST	Disabled	32768(Bridge Priority : 32768, SYS ID Ext : 0)	<input type="button" value="Modify"/>
4	Disabled	32772(Bridge Priority : 32768, SYS ID Ext : 4)	<input type="button" value="Modify"/>

Figure 3 - 54 STP Instance Settings window

The following information is displayed:

Parameter	Description
Instance Type	Displays the instance type(s) currently configured on the Switch. Each instance type is classified by a MSTI ID. CIST refers to the default MSTI configuration set on the Switch.
Instance Status	Displays the current status of the corresponding MSTI ID
Instance Priority	Displays the priority of the corresponding MSTI ID. The lowest priority will be the root bridge.

Click the **Modify** button to change the priority of the MSTI. This will open the **Instance ID Settings** window to configure.

Instance ID Settings	
MSTI ID	<input type="text" value="0"/>
Type	Set Priority Only <input type="button" value="v"/>
Priority (0-61440)	<input type="text"/>
<input type="button" value="Apply"/>	
Show STP Instance Table	

Figure 3 - 55 STP Instance Settings- Edit window

Parameter	Description
MSTI ID	Displays the MSTI ID of the instance being Modified. An entry of 0 in this field denotes the CIST (default MSTI).
Type	The Type field in this window will be permanently set to <i>Set Priority Only</i> .
Priority (0-61440)	Enter the new priority in the Priority field

Click **Apply** to implement the new priority setting.

STP Port Settings

STP can be set up on a port per port basis. In addition to setting Spanning Tree parameters for use on the switch level, the Switch allows for the configuration of groups of ports, each port-group of which will have its own spanning tree, and will require some of its own configuration settings. An STP Group will use the switch-level parameters entered above, with the addition of Port Priority and Port Cost. An STP Group spanning tree works in the same way as the switch-level spanning tree, but the root bridge concept is replaced with a root port concept. A root port is a port of the group that is elected based on port priority and port cost, to be the connection to the network for the group. Redundant links will be blocked, just as redundant links are blocked on the switch level. The STP on the switch level blocks redundant links between switches (and similar network devices). The port level STP will block redundant links within an STP Group.

It is advisable to define an STP Group to correspond to a VLAN group of ports.

To view this window, click **L2 Features > Spanning Tree > STP Port Settings** as shown as below:

STP Port Settings													
Unit	From	To	External Cost (0=Auto)	Hello Time	Migrate	Edge	P2P	State	LBD	BPDU	Restricted Role	Restricted Tcn	Apply
1	Port 1	Port 1	0	0	Yes	True	True	Enabled	Disabled	Enabled	False	False	Apply
STP Port Settings Table-Unit 1													
Port	External Cost	Hello Time	Edge	P2P	Port STP	LBD	BPDU	Restricted Role	Restricted Tcn				
1	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
2	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
3	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
4	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
5	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
6	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
7	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
8	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
9	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
10	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
11	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
12	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
13	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
14	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
15	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
16	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
17	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
18	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
19	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
20	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
21	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
22	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
23	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				
24	Auto/200000	2/2	False/No	Auto/Yes	Enabled	Disabled	Disabled	False	False				

Figure 3 - 56 STP Port Settings window

It is advisable to define an STP Group to correspond to a VLAN group of ports.

The following STP Port Settings fields can be set:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.

From / To	A consecutive group of ports may be configured starting with the selected port.
External Cost (0=Auto)	<p>This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is 0 (auto).</p> <p>0 (auto) – Setting 0 for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000.</p> <p>value 1-200000000 – Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets.</p>
Hello Time	The time interval between transmissions of configuration messages by the designated port, to other devices on the bridged LAN. The user may choose a time between 1 and 10 seconds. The default is 2 seconds. If the inputted Hello Time is greater than 2, the Hello Time is 2. This field is only operable when the Switch is enabled for MSTP.
Migrate	When operating in RSTP mode, selecting yes forces the port that has been selected to transmit RSTP BPDUs.
Edge	Choosing the True parameter designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDUs. If a BPDUs packet is received, it automatically loses edge port status. Choosing the False parameter indicates that the port does not have edge port status.
P2P	Choosing the True parameter indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports, however they are restricted in that a P2P port must operate in full duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of False indicates that the port cannot have p2p status. Auto allows the port to have p2p status whenever possible and operate as if the p2p status were true. If the port cannot maintain this status, (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were false. The default setting for this parameter is true.
State	This drop-down menu allows you to enable or disable STP for the selected group of ports. The default is Enabled.
LBD	Use the pull-down menu to enable or disable the loop-back detection function on the switch for the ports configured above.
BPDUs	Use the pull-down menu to enable or disable the flooding of BPDUs packets when STP is disabled.
Restricted Role	<p>Toggle between <i>True</i> and <i>False</i> to set the restricted role state of the port. The default value is <i>False</i>.</p> <p>If <i>True</i> causes the port not to be selected as the root port for the CIST or any MSTI, even if it has the best spanning tree priority vector, such a port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be <i>False</i> by default. Setting this variable can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.</p>
Restricted Tcn	<p>Toggle between <i>True</i> and <i>False</i> to set the restricted TCN of the port. The default value is <i>False</i>.</p> <p>If <i>True</i> causes the port not to be selected as the root port for the CIST or any MSTI, even if it has the best spanning tree priority vector, such a port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be <i>False</i> by default. Setting this variable can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.</p>

Click **Apply** to implement the changes.

Forwarding & Filtering

This folder contains windows for Unicast Forwarding, Multicast Forwarding and Multicast Filtering Mode.

Unicast Forwarding

This window is used to configure the Unicast Forwarding on the Switch.

To view this window, click **L2 Features > Forwarding & Filtering > Unicast Forwarding**, as shown on the right:

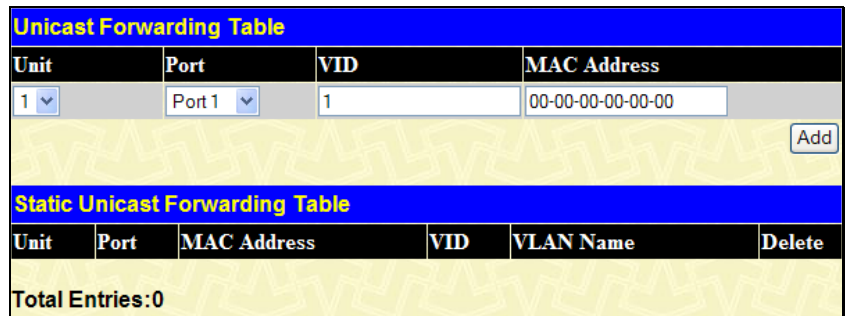



Figure 3 - 57 Setup Static Unicast Forwarding Table window

To add or edit an entry, define the following parameters and then click **Add/Modify**:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
Port	Allows the selection of the port number on which the MAC address entered above resides.
VID	The VLAN ID number of the VLAN on which the above Unicast MAC address resides.
MAC Address	The MAC address to which packets will be statically forwarded. This must be a unicast MAC address.

Click **Add** to implement the changes made. To delete an entry in the Static Unicast Forwarding Table, click the corresponding  under the Delete heading.

Multicast Forwarding

The following window describes how to set up Multicast Forwarding on the Switch.

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Forwarding**, as shown below.

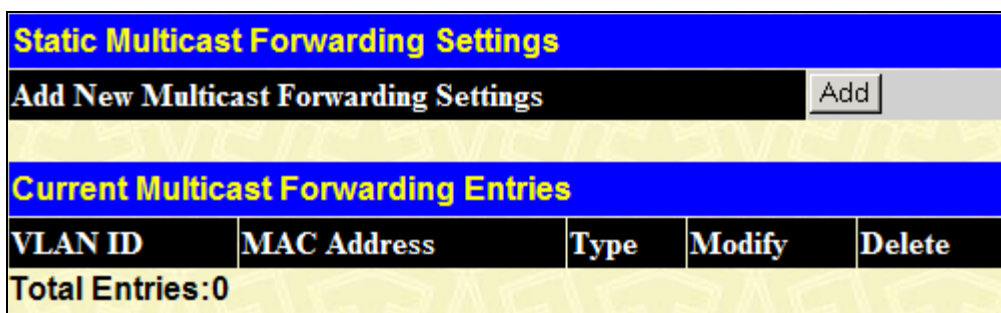



Figure 3 - 58 Static Multicast Forwarding Settings window

The Static Multicast Forwarding Settings window displays all of the entries made into the Switch's static multicast forwarding table. To delete an entry in the Static Multicast Forwarding Table, click the corresponding  under the Delete heading.

Click the **Add** button to open the Setup Static Multicast Forwarding Table window, as shown below.

Figure 3 - 59 Setup Static Multicast Forwarding Table window

The following parameters can be set:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
VID	The VLAN ID of the VLAN the corresponding MAC address belongs to.
Multicast MAC Address	The MAC address of the static source of multicast packets. This must be a multicast MAC address.
Port Settings	<p>Allows the selection of ports that will be members of the static multicast group and ports that are either forbidden from joining dynamically, or that can join the multicast group dynamically, using GMRP. The options are:</p> <p><i>None</i> – No restrictions on the port dynamically joining the multicast group. When None is chosen, the port will not be a member of the Static Multicast Group.</p> <p><i>Egress</i> – The port is a static member of the multicast group.</p>

Click **Apply** to implement the changes made. Click the [Show All Multicast Forwarding Entries](#) link to return to the **Static Multicast Forwarding Settings** window.

Multicast Filtering Mode

This window allows users to configure the Switch to forward or filter the Unregistered Groups per VLAN.

To view this window, click **L2 Features > Forwarding & Filtering > Multicast Filtering Mode**, as shown below.

Figure 3 - 60 Multicast Filtering Mode Settings window

The following parameters can be set:

Parameter	Description
VLAN Name	The VLAN to which the specified filtering action applies. Tick the All check box to apply the action to all VLANs on the Switch.
Filtering Mode	<p>This drop-down menu allows you to select the action the Switch will take when it receives a multicast packet that requires forwarding to a port in the specified VLAN.</p> <ul style="list-style-type: none"> • <i>Forward All Groups</i> – This will instruct the Switch to forward a multicast packet to all multicast groups residing within the range of ports specified above. • <i>Forward Unregistered Groups</i> – This will instruct the Switch to forward a multicast packet whose destination is an unregistered multicast group residing within the range of ports specified above. • <i>Filter Unregistered Groups</i> – This will instruct the Switch to filter any multicast packets whose destination is an unregistered multicast group residing within the range of ports specified above but it will forward the multicast reserved address.

Click **Apply** to implement the changes.

LLDP

The Link Layer Discovery Protocol (LLDP) allows stations attached to an IEEE 802 LAN to advertise, to other stations attached to the same IEEE 802 LAN. The major capabilities provided by this system is that it incorporates the station, the management address or addresses of the entity or entities that provide management of those capabilities, and the identification of the station's point of attachment to the IEEE 802 LAN required by those management entity or entities.

The information distributed via this protocol is stored by its recipients in a standard Management Information Base (MIB), making it possible for the information to be accessed by a Network Management System (NMS) through a management protocol such as the Simple Network Management Protocol (SNMP).

LLDP Global Settings

This window is used to configure the LLDP Global Settings on the Switch. When LLDP is enabled the Switch can start to transmit, receive and process LLDP packets. The specific function of each port will depend on the per port LLDP settings. LLDP Global State is *Disabled* by default.

To view this window, click **L2 Features > LLDP > LLDP Global Settings**, as shown below.

Figure 3 - 61 LLDP Global Settings window

The following parameters can be configured:

Parameter	Description
LLDP Operation State	Used to <i>Enable</i> or <i>Disable</i> LLDP on the Switch.
LLDP Forward Message State	When LLDP is disabled this function controls the LLDP packet forwarding message based on individual ports. If LLDP is enabled on a port it will flood the LLDP packet to all ports that have the same port VLAN and will advertise to other stations attached to the same IEEE 802 LAN.
Message TX Interval (5-32768)	This interval controls how often active ports retransmit advertisements to their neighbors. To change the packet transmission interval, enter a value in seconds (5 to 32768).
Message TX Hold Multiplier (2-10)	This function calculates the Time-to-Live for creating and transmitting the LLDP advertisements to LLDP neighbors by changing the multiplier used by an LLDP Switch. When the Time-to-Live for an advertisement expires the advertised data is then deleted from the neighbor Switch's MIB.
ReInit Delay (1-10)	The LLDP reinitialization delay interval is the minimum time that an LLDP port will wait before reinitializing after receiving an LLDP disable command. To change the LLDP Reinit Delay, enter a value in seconds (1 to 10).
TX Delay (1-8192)	LLDP TX Delay allows the user to change the minimum time delay interval for any LLDP

	port which will delay advertising any successive LLDP advertisements due to change in the LLDP MIB content. To change the LLDP TX Delay, enter a value in seconds (1 to 8192).
Notification Interval (5-3600)	LLDP Notification Interval is used to send notifications to configured SNMP trap receiver(s) when an LLDP change is detected in an advertisement received on the port from an LLDP neighbor. To set the LLDP Notification Interval, enter a value in seconds (5 to 3600).

Click **Apply** to implement the changes.

Basic LLDP Port Settings

This window is used to display the LLDP port settings on the Switch. The ports can be individually configured to send notifications to configured SNMP trap receivers.

To view this window, click **L2 Features > LLDP > Basic LLDP Port Settings**, as shown below.

Basic LLDP Port Settings									
Unit	From	To	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities	Apply
1	Port 1	Port 1	Disabled	TX_Only	Disabled	Disabled	Disabled	Disabled	Apply
Basic LLDP Port Settings Table									
Port ID	Notification State	Admin Status	Port Description	System Name	System Description	System Capabilities			
1	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
2	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
3	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
4	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
5	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
6	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
7	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
8	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
9	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
10	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
11	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
12	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
13	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
14	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
15	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
16	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
17	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
18	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
19	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
20	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
21	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
22	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
23	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			
24	Disabled	TX_and_RX	Disabled	Disabled	Disabled	Disabled			

Figure 3 - 62 Basic LLDP Port Settings window

The following parameters can be set:

Parameter	Description
Unit	Select the unit to configure.
From / To	Use the pull-down menu to select a range of ports to be configured.
Notification State	Use the pull-down menu to <i>Enable</i> or <i>Disable</i> the status of the LLDP notification. This function controls the SNMP trap, however it cannot implement traps on SNMP when the notification is disabled.
Admin Status	This function controls the local LLDP agent and allows it to send and receive LLDP frames on the ports. This option contains <i>TX_Only</i> , <i>RX_Only</i> , <i>TX_and_RX</i> or <i>Disabled</i> . <i>TX_Only</i> – The local LLDP agent can only transmit LLDP frames. <i>RX_Only</i> – The local LLDP agent can only receive LLDP frames. <i>TX_and_RX</i> – The local LLDP agent can both transmit and receive LLDP frames. <i>Disabled</i> – The local LLDP agent can neither transmit nor receive LLDP frames. The default value is <i>TX_and_RX</i> .
Port Description	Used to enable or disable the port description on the Switch.
System Name	Used to enable or disable the system name on the Switch.
System Description	Used to enable or disable the system description on the Switch.
System Capabilities	Used to enable or disable the system capabilities on the Switch.

Click **Apply** to implement the changes.

802.1 Extension LLDP Port Settings

This window is used to configure an individual port or group of ports to exclude one or more of the IEEE 802.1 organizational port VLAN ID TLV data types from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > 802.1 Extension LLDP Port Settings**, as shown below.

802.1 Extension LLDP Port Settings

Unit	1		
From	Port 1		
To	Port 1		
Port VLAN ID	Disabled		
Protocol VLAN ID	VLAN ID	<input type="text"/>	Disabled
VLAN Name	VLAN ID	<input type="text"/>	Disabled
Protocol Identify	EAPOL		Disabled

802.1 Extension LLDP Port Settings Table

Port ID	Port VLAN ID	Enabled Protocol VLAN ID	Enabled VLAN Name	Enabled Protocol Identity
1	Disabled	(None)	(None)	(None)
2	Disabled	(None)	(None)	(None)
3	Disabled	(None)	(None)	(None)
4	Disabled	(None)	(None)	(None)
5	Disabled	(None)	(None)	(None)
6	Disabled	(None)	(None)	(None)
7	Disabled	(None)	(None)	(None)
8	Disabled	(None)	(None)	(None)
9	Disabled	(None)	(None)	(None)
10	Disabled	(None)	(None)	(None)
11	Disabled	(None)	(None)	(None)
12	Disabled	(None)	(None)	(None)
13	Disabled	(None)	(None)	(None)
14	Disabled	(None)	(None)	(None)
15	Disabled	(None)	(None)	(None)
16	Disabled	(None)	(None)	(None)
17	Disabled	(None)	(None)	(None)
18	Disabled	(None)	(None)	(None)
19	Disabled	(None)	(None)	(None)
20	Disabled	(None)	(None)	(None)
21	Disabled	(None)	(None)	(None)
22	Disabled	(None)	(None)	(None)
23	Disabled	(None)	(None)	(None)
24	Disabled	(None)	(None)	(None)

Figure 3 - 63 802.1 Extension LLDP Port Settings window

The following parameters can be set:

Parameter	Description
Unit	Select the unit to configure.
From / To	Use the pull-down menu to select a range of ports to be configured.
Port VLAN ID	Use the drop-down menu to enable or disable the advertised PVID. This TLV optional datatype determines whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port. The default state is <i>Disabled</i> .
Protocol VLAN ID	Use the drop-down menu to enable or disable the advertise Protocol <i>VLAN ID</i> , <i>VLAN Name</i> , or <i>All</i> . This TLV optional data type indicates whether the corresponding Local System's port and protocol VLAN ID instance will be transmitted on the port. If a port is associated with multiple protocol VLANs, those enabled ports and protocol VLAN IDs will be advertised.
VLAN Name	This function indicates whether the System's <i>VLAN ID</i> , <i>VLAN Name</i> or <i>All</i> will be transmitted on the port. The default state is <i>Disabled</i> .
Protocol Identify	Use the drop-down menu to enable or disable the advertise Protocol Identity. Select the protocol you wish to use <i>EAPOL</i> , <i>LACP</i> , <i>GVRP</i> , <i>STP</i> or <i>All</i> . This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.

Click **Apply** to implement the changes.

802.3 Extension LLDP Port Settings

This window is used to configure an individual port or group of ports to exclude one or more IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.

To view this window, click **L2 Features > LLDP > 802.3 Extension LLDP Port Settings**, as shown below.

802.3 Extension LLDP Port Settings

Unit	From	To	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size	Apply
1	Port 1	Port 1	Disabled	Disabled	Disabled	Disabled	Apply

802.3 Extension LLDP Port Settings Table

Port ID	MAC/PHY Configuration/Status	Power Via MDI	Link Aggregation	Maximum Frame Size
1	Disabled	Disabled	Disabled	Disabled
2	Disabled	Disabled	Disabled	Disabled
3	Disabled	Disabled	Disabled	Disabled
4	Disabled	Disabled	Disabled	Disabled
5	Disabled	Disabled	Disabled	Disabled
6	Disabled	Disabled	Disabled	Disabled
7	Disabled	Disabled	Disabled	Disabled
8	Disabled	Disabled	Disabled	Disabled
9	Disabled	Disabled	Disabled	Disabled
10	Disabled	Disabled	Disabled	Disabled
11	Disabled	Disabled	Disabled	Disabled
12	Disabled	Disabled	Disabled	Disabled
13	Disabled	Disabled	Disabled	Disabled
14	Disabled	Disabled	Disabled	Disabled
15	Disabled	Disabled	Disabled	Disabled
16	Disabled	Disabled	Disabled	Disabled
17	Disabled	Disabled	Disabled	Disabled
18	Disabled	Disabled	Disabled	Disabled
19	Disabled	Disabled	Disabled	Disabled
20	Disabled	Disabled	Disabled	Disabled
21	Disabled	Disabled	Disabled	Disabled
22	Disabled	Disabled	Disabled	Disabled
23	Disabled	Disabled	Disabled	Disabled
24	Disabled	Disabled	Disabled	Disabled

Figure 3 - 64 802.3 Extension LLDP Port Settings window

The following parameters can be set:

Parameter	Description
Unit	Select the unit you wish to configure.
From / To	Use the pull-down menu to select a range of ports to be configured.
MAC/PHY Configuration/Status	This function indicates that the LLDP agent should transmit 'MAC/PHY configuration/status TLV'. It is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, if the function is enabled, the auto-negotiated advertised capability, or the operational MAU type. The default state is <i>Disabled</i> .

Power Via MDI	This specifies that the LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is <i>Disabled</i> .
Link Aggregation	The Link Aggregation option indicates that LLDP agents should transmit 'Link Aggregation TLV'. This indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and what is the aggregated port ID. The default state is <i>Disabled</i> .
Maximum Frame Size	The Maximum Frame Size indicates that LLDP agent should transmit 'Maximum-frame-size TLV'. The default state is <i>Disabled</i> .

Click **Apply** to implement the changes.

LLDP Management Address Settings

This window is used to configure the LLDP management address information on the Switch.

To view this window, click **L2 Features > LLDP > LLDP Management Address Settings**, as shown below.

LLDP Management Address Settings						
Unit	From	To	Address Type	Address	Port State	Apply
1	Port 1	Port 1	IPv4 Address		Disabled	Apply

Enabled Management Address Table	
Port ID	Enabled Management Address
1	(None)
2	(None)
3	(None)
4	(None)
5	(None)
6	(None)
7	(None)
8	(None)
9	(None)
10	(None)
11	(None)
12	(None)
13	(None)
14	(None)
15	(None)
16	(None)
17	(None)
18	(None)
19	(None)
20	(None)
21	(None)
22	(None)
23	(None)
24	(None)

Figure 3 - 65 LLDP Management Address Settings window

The following parameters can be set:

Parameter	Description
Unit	Select the unit you wish to configure.
From / To	Use the pull-down menu to select a range of ports to be configured.
Address Type	Use the drop down menu to select either the <i>IPv4</i> or <i>IPv6</i> Address. IPv4/IPv6 is a management IP so the IP information will be sent with the frame when the mgt_addr config is enabled.
Address	Enter the management ip address or the ip address of the entity you wish to advertise to.
Port State	Used to <i>Enable</i> or <i>Disable</i> the Port State for the LLDP Management Address Settings.

Click **Apply** to implement the changes.

LLDP Statistics

LLDP Statistics allows you an overview of neighbor detection activity, LLDP Statistics and the settings for individual ports on the Switch. Use the drop-down menu to check a specific unit the information will be displayed in the lower half of the table.

To view this window, click **L2 Features > LLDP > LLDP Statistics**, as shown below.

LLDP Statistics System							
Last Change Time		4931					
Number of Table Insert		0					
Number of Table Delete		0					
Number of Table Drop		0					
Number of Table Age Out		0					
Unit		1 ▾					
LLDP Statistics Ports							
Port ID	TxPort FramesTotal	RxPortFrames DiscardedTotal	RxPort FramesErrors	RxPort FramesTotal	RxPortTLVs DiscardedTotal	RxPortTLVs UnrecognizedTotal	RxPort AgeoutsTotal
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0
14	0	0	0	0	0	0	0
15	0	0	0	0	0	0	0
16	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0
19	0	0	0	0	0	0	0
20	0	0	0	0	0	0	0
21	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0
24	0	0	0	0	0	0	0

Figure 3 - 66 LLDP Statistics System window

LLDP Management Address Table

The following window is used to set up LLDP management address settings on the Switch.

To view this window, click **L2 Features > LLDP > LLDP Management Address Settings**, as shown below.

Management Address		IPv4 Address ▾	<input type="text"/>	<input type="button" value="Find"/>	
LLDP Management Address Table					
No.	Subtype	Address	IF Type	OID	Advertising Ports
1	IPv4	10.90.90.90	Unknown	1.3.6.1.4.1.171.10.70.7	(None)
Total Entries:1					

Figure 3 - 67 LLDP Management Address window

The following parameters can be set or displayed:

Parameter	Description
Address Type	Use the drop-down menu to toggle between <i>IPV4 Address</i> and <i>IPV6 Address</i> .
Address	Enter the LLDP management address in this field.

Click **Find** to display the entry.

LLDP Local Port Table

LLDP Local Port Table window displays the information on a per port basis currently available for populating outbound LLDP advertisements in the local port brief table shown below.

To view this window, click **L2 Features > LLDP > LLDP Local Port Table**, as shown below.

Unit		1 ▾			
LLDP Local Port Brief Table					
No.	Port ID Subtype	Port ID	Port Description	Normal	Detailed
1	Local	1/1	D-Link DGS-3426P R2.70.B43 Port 1 on Unit 1	View	View
2	Local	1/2	D-Link DGS-3426P R2.70.B43 Port 2 on Unit 1	View	View
3	Local	1/3	D-Link DGS-3426P R2.70.B43 Port 3 on Unit 1	View	View
4	Local	1/4	D-Link DGS-3426P R2.70.B43 Port 4 on Unit 1	View	View
5	Local	1/5	D-Link DGS-3426P R2.70.B43 Port 5 on Unit 1	View	View
6	Local	1/6	D-Link DGS-3426P R2.70.B43 Port 6 on Unit 1	View	View
7	Local	1/7	D-Link DGS-3426P R2.70.B43 Port 7 on Unit 1	View	View
8	Local	1/8	D-Link DGS-3426P R2.70.B43 Port 8 on Unit 1	View	View
9	Local	1/9	D-Link DGS-3426P R2.70.B43 Port 9 on Unit 1	View	View
10	Local	1/10	D-Link DGS-3426P R2.70.B43 Port 10 on Unit 1	View	View
11	Local	1/11	D-Link DGS-3426P R2.70.B43 Port 11 on Unit 1	View	View
12	Local	1/12	D-Link DGS-3426P R2.70.B43 Port 12 on Unit 1	View	View
13	Local	1/13	D-Link DGS-3426P R2.70.B43 Port 13 on Unit 1	View	View
14	Local	1/14	D-Link DGS-3426P R2.70.B43 Port 14 on Unit 1	View	View
15	Local	1/15	D-Link DGS-3426P R2.70.B43 Port 15 on Unit 1	View	View
16	Local	1/16	D-Link DGS-3426P R2.70.B43 Port 16 on Unit 1	View	View
17	Local	1/17	D-Link DGS-3426P R2.70.B43 Port 17 on Unit 1	View	View
18	Local	1/18	D-Link DGS-3426P R2.70.B43 Port 18 on Unit 1	View	View
19	Local	1/19	D-Link DGS-3426P R2.70.B43 Port 19 on Unit 1	View	View
20	Local	1/20	D-Link DGS-3426P R2.70.B43 Port 20 on Unit 1	View	View
21	Local	1/21	D-Link DGS-3426P R2.70.B43 Port 21 on Unit 1	View	View
22	Local	1/22	D-Link DGS-3426P R2.70.B43 Port 22 on Unit 1	View	View
23	Local	1/23	D-Link DGS-3426P R2.70.B43 Port 23 on Unit 1	View	View
24	Local	1/24	D-Link DGS-3426P R2.70.B43 Port 24 on Unit 1	View	View

Figure 3 - 68 LLDP Local Port Brief Table window

To view *Normal* information on a per port basis click the corresponding **View** button, which will display the following window.

LLDP Local Port Normal Table	
No.	1 : 1
Port ID Subtype	Local
Port ID	1/1
Port Description	D-Link DGS-3426P R2.70.B43 Port 1 on Unit 1
Port VLAN ID	1
Management Address Count	1
PPVID Entries Count	0
VLAN Name Entries Count	1
Protocol Identity Entries Count	0
MAC/PHY Configuration/Status	see detailed
Power Via MDI	see detailed
Link Aggregation	see detailed
Maximum Frame Size	1536
Show LLDP Local Port Brief Table Show LLDP Local Port Detailed Table	

Figure 3 - 69 LLDP Local Port Table - View Normal window

To return to the previous window click the [Show LLDP Local Port Brief Table](#) link. To view details of individual parameters, click the hyperlinked [see detailed](#) or [Show LLDP Local Port Detailed Table](#) which will reveal the following window. You may also click the **View** button under Detailed heading in the LLDP Local Port Brief Table window.

LLDP Local Port Detailed Table
Port ID : 1 : 1

Port ID Subtype : Local
Port ID : 1/1
Port Description : D-Link DGS-3426P R2.70.B43 Port 1 on Unit 1
Port PVID : 1
Management Address Count : 1
Subtype : IPv4
Address : 10.90.90.90
IF Type : Unknown
OID : 1.3.6.1.4.1.171.10.70.7
PPVID Entries Count : 0
(None)
VLAN Name Entries Count : 1
Entry 1 :
VLAN ID : 1
VLAN Name : default
Protocol Identity Entries Count : 0
(None)
MAC/PHY Configuration/Status :
Auto-Negotiation Support : Supported
Auto-Negotiation Enabled : Enabled
Auto-Negotiation Advertised Capability : 6c01(hex)
Auto-Negotiation Operational MAU Type : 0000(hex)
Power Via MDI :
Port Class : PSE
PSE MDI Power Support : Supported
PSE MDI Power State : Enabled
PSE Pairs Control Ability : Uncontrollable
MDI PSE Power Pair : 1
MDI PSE Power Class : 4
Link Aggregation :
Aggregation Capability : Aggregated
Aggregation Status : Not Currently In Aggregation
Aggregation Port ID : 0
Maximum Frame Size : 1536
Show LLDP Local Port Brief Table
Show LLDP Local Port Normal Table

Figure 3 - 70 LLDP Local Port Table - View Detailed window

To return to the LLDP Local Port Brief Information window, click the [Show LLDP Local Port Brief Table](#) link. To view the LLDP Local Port Normal Table window, click the [Show LLDP Local Port Normal Table](#) link.

LLDP Remote Port Table

This window displays port information learned from the neighbor. The Switch receives packets from a remote station but is able to store the information as local.

To view this window, click **L2 Features > LLDP > LLDP Remote Port Table**, as shown below.



Figure 3 - 71 LLDP Remote Port Brief Table window

Select the port you wish to view by using the drop-down menu and click **Find**, the information will be displayed in the lower half of the table. To view the settings for an individual port select the port and click [View Normal](#) which will display the following window.

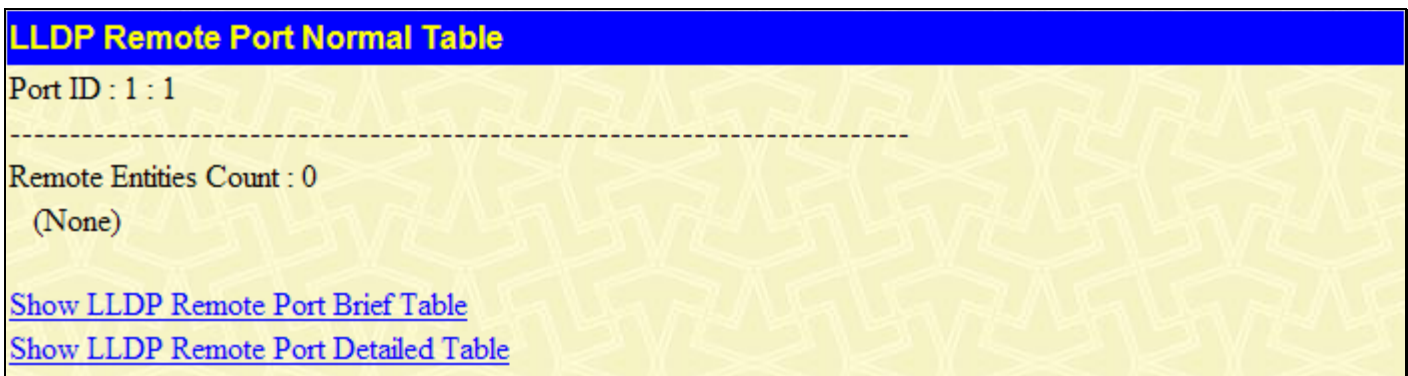


Figure 3 - 72 LLDP Remote Port Table - View Normal window

To return to the LLDP Local Remote Port Brief window, click the [Show LLDP Remote Port Brief Table](#) link.

To view the LLDP Remote Port Detailed Table window, click the [Show LLDP Remote Port Detailed Table](#) link, or select a port and click [View Detailed](#) in the LLDP Remote Port Brief Table window which will display the following window.



Figure 3 - 73 LLDP Remote Port Table - View Detailed window

To return to the LLDP Local Remote Port Brief window, click the [Show LLDP Remote Port Brief Table](#) link. To view the LLDP Remote Port Normal Table window, click the [Show LLDP Remote Port Normal Table](#) link.

Q-in-Q

Q-in-Q is designed for service providers to carry traffic from multiple users across a network. Q-in-Q is used to maintain customer specific VLAN and Layer 2 protocol configurations even when the same VLAN ID is being used by different customers. This is achieved by inserting SP-VLAN tags into the customer's frames when they enter the service provider's network, and then removing the tags when the frames leave the network.

Customers of a service provider may have different or specific requirements regarding their internal VLAN IDs and the number of VLANs that can be supported. Therefore customers in the same service provider network may have VLAN ranges that overlap, which might cause traffic to become mixed up. So assigning a unique range of VLAN IDs to each customer might cause restrictions on some of their configurations requiring intense processing of VLAN mapping tables which may exceed the VLAN mapping limit. Q-in-Q uses a single service provider VLAN (SP-VLAN) for customers who have multiple VLANs. Customer's VLAN IDs are segregated within the service provider's network even when they use the same customer specific VLAN ID. Q-in-Q expands the VLAN space available while preserving the customer's original tagged packets and adding SP-VLAN tags to each new frame.

Q-in-Q Settings

This function allows the user to enable or disable the Q-in-Q function on the Switch.

To view this window click **L2 Features > QinQ > QinQ Settings**, as shown on the right:

The screenshot displays the Q-in-Q Settings window, which is divided into three main sections:

- QinQ Global Settings:** A section with a blue header. It contains a 'QinQ State' dropdown menu set to 'Disabled' and an 'Apply' button.
- QinQ Port Settings:** A section with a blue header. It contains a table with columns: Unit, From, To, Role, Missdrop, TPID (1-FFFF), Use Inner Priority, and Apply. The first row shows Unit: 1, From: Port 1, To: Port 1, Role: NNI, Missdrop: Disabled, TPID: 0x88A8, and Use Inner Priority: Disabled.
- QinQ Port Table:** A table with columns: Port, Role, Missdrop, TPID, and Use Inner Priority. It lists 24 ports, all with a Role of 'Normal', Missdrop of 'Disabled', TPID of '0x8100', and Use Inner Priority of 'Disabled'.

Figure 3 - 74 Q-in-Q Settings window

The following fields can be set:

Parameter	Description
QinQ State	Use the pull down menu to <i>Enable</i> or <i>Disable</i> the Q-in-Q State. When Q-in-Q is <i>Enabled</i> , all network port roles will have NNI ports and their outer TPID set to 0x88a8. All existing static VLANs will run as SP-VLANs. All dynamically learned L2 addresses and all dynamically registered VLAN entries will be cleared, GVRP will be disabled. According 802.1ad, the address 01-80-c2-00-00-08 will be used for STP in the provider's network. So the user shall disable STP first, and then use the new address for STP state machine. The default setting is <i>Disabled</i> .
Unit	Select the unit you wish to configure.
From / To	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
Role	The user can choose between UNI or NNI role. <i>UNI</i> – To select a user-to-network interface which specifies that communication between the specified user and a specified network will occur. <i>NNI</i> – To select a network-to-network interface specifies that communication between two specified networks will occur.
Missdrop	<i>Enable</i> or <i>Disable</i> C-VLAN based on SP-VLAN assignment miss drop. When enabled the tagged packet will be dropped if the VLAN translation look up misses. When disabled the packet will not be dropped if the VLAN translation loop up misses and the packet will be added to an outer VLAN based on MAC/SUBNET/PROTOCOL/PORT based VLAN configuration. This will make the packet a double tagged packet. NOTE: The result will be Transparent Mode behavior.
TPID(0x1-0xffff)	The Outer TPID is used for learning and switching packets. The Outer TPID constructs and inserts the outer tag into the packet based on the VLAN ID.
User Inner Priority	Use the drop-down menu to enable or disable the function. When enabled, the priority of C-tag copies to S-tag.

Click **Apply** to implement the changes.

VLAN Translation Settings

The VLAN translation settings translates the VLAN ID carried in the data packets it receives from private networks into those used in the Service Providers network.

To view this window, click **L2 Features > QinQ > VLAN Translation Settings**, as shown below.

VLAN Translation Settings									
Unit	From	To	CVID List	Action	SVID(1-4094)	Priority	Apply	Find By Ports	Delete All
1	Port 1	Port 1		Add		None	Apply	Find By Ports	Delete All
Total Entries: 0									
VLAN Translation Table									
Unit	Port	CVID	SVID	Action	Priority	Delete			
Show All VLAN Translation Table									

Figure 3 - 75 VLAN Translation Settings window

The following fields can be set:

Parameter	Description
Unit	Select the unit you wish to configure.
From / To	A consecutive group of ports that are part of the VLAN configuration starting with the selected port.
CVID List	The customer VLAN ID List to which the tagged packets will be added.
Action	Specify if you want SPVID packets to be added or replaced.
SVID(1-4094)	This configures the VLAN to join the Service Providers VLAN as a tagged member.
Priority	Select a priority for the VLAN ranging from 0-7. With 7 having the highest priority.

Click **Apply** to create a new entry, click **Find By Ports** to view the current entries by ports and **Delete All** to remove all VLAN Translation entries. To view the VLAN translation table, click the hyperlinked [Show All VLAN Translation Table](#).

ERPS

The Switch supports ITU-T G.8032 Ethernet Ring Protection Switching (ERPS) to provide a reliable mechanism of malfunction recovery in an Ethernet ring topology network.

ERPS Global Settings

This window is used to enable global ERPS function on the Switch. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. The global ERPS function cannot be enabled when any ERPS ring on the device is enabled and the integrity of any ring parameter is not available. For each ring, with the individual ring state enabled and ERPS enabled globally, the following integrity will be checked:

1. The Ring-Automatic Protection Switching (R-APS) VLAN is created.
2. The Ring port is a tagged member port of the R-APS VLAN.
3. The Ring Protection Link (RPL) port is specified if the RPL owner is enabled.

The default state is *Disabled*.

To view this window, click **L2 Features > ERPS > ERPS Global Settings**, as shown below.

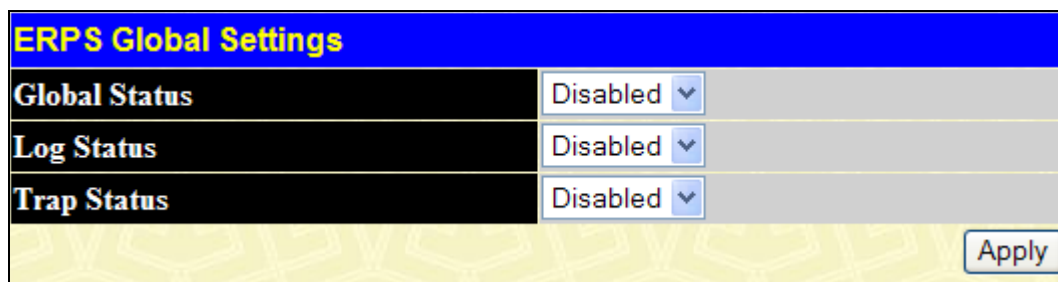


Figure 3 - 76 ERPS Global Settings window

The following fields can be set:

Parameter	Description
Global Status	Enable the global ERPS function on a switch.

Log Status	Enable or disable the log state of ERPS events. The default value is <i>Disabled</i> .
Trap Status	Enable or disable the trap state of ERPS events. The default value is <i>Disabled</i>

Click **Apply** to implement the changes.

ERPS RAPS VLAN Settings

This window allows users to search for and display ERPS RAPS information. Enter an R-APS VLAN ID in the field provided.

To view this window, click **L2 Features > ERPS > ERPS RAPS VLAN Settings**, as shown below.

Add

R-APS VID (1-4094) **Find**
View All

Total Rings: 1

ERPS RAPS VLAN Table

R-APS VID	West Port	East Port	Protected VID List	Modify	Sub Ring Modify	Delete
1	1:1(Forwarding)	1:2(Forwarding)		Modify	Modify	X

Figure 3 - 77 ERPS RAPS VLAN Table window

The following fields can be set:

Parameter	Description
R-APS VID (1-4094)	The R-APS VLAN is the dedicated VLAN for transferring R-APS message. Enter the R-APS VLAN ID between 1 and 4094.

To search for specific VID, enter the VLAN ID in the **R-APS VID (1-4094)** field and click **Find**. To see all the entries, click **View All**.

To add a new entry, click **Add** to see the window shown below.

ERPS RAPS VLAN Settings - Add

R-APS VID (1-4094) **Apply**

[Show All ERPS RAPS VLAN](#)

Figure 3 - 78 ERPS RAPS VLAN Table - Add window

Enter a VLAN ID in the **R-APS VID (1-4094)** field, and click **Apply** to see the entry appears in ERPS RAPS VLAN Table window.

To edit an entry, click **Modify** to see the window shown below.

ERPS RAPS VLAN Settings - Edit		
R-APS VID (1-4094)	<input type="text" value="1"/>	
ERPS State	Disabled <input type="button" value="v"/>	
West	<input checked="" type="radio"/> Port <input type="button" value="v"/> <input type="checkbox"/>	
West Port	<input type="text" value="1:1"/>	Forwarding
East	<input type="radio"/> Port <input type="button" value="v"/> <input type="checkbox"/>	
East Port	<input type="text" value="1:2"/>	Forwarding
RPL Port	<input type="checkbox"/> None <input type="button" value="v"/>	
RPL Owner	Disabled <input type="button" value="v"/>	
Protected VLAN Action	Add <input type="button" value="v"/>	
Protected VIDList	<input type="checkbox"/> <input type="text"/>	
Ring MEL (0-7)	<input type="text" value="1"/>	
Holdoff Time (0-10000)	<input type="text" value="0"/> ms	
Guard Time (10-2000)	<input type="text" value="500"/> ms	
WTR Time (5-12)	<input type="text" value="5"/> min	
Current Ring State	-	

[Show All ERPS RAPS VLAN](#)

Figure 3 - 79 ERPS RAPS VLAN Table - Edit window

The following fields can be set:

Parameter	Description
ERPS State	This is used to configure ring state of the specified ring. When both the global state and the specified ring ERPS state are enabled, the specified ring will be activated. STP and LBD should be disabled on the ring ports before the specified ring is activated. The ring cannot be enabled before the R-APS VLAN is created, and ring ports, RPL port, RPL owner, are configured. Note that these parameters cannot be changed when the ring is activated. The default ring state is <i>Disabled</i> .
West	Click to specify the port as the west ring port. To specify as a Virtual Channel, tick the check and toggle from <i>Port</i> to <i>Virtual Channel</i> .
West Port	If Port is set above, enter the port to be configured.
East	Click to specify the port as the east ring port. To specify as a Virtual Channel, tick the check and toggle from <i>Port</i> to <i>Virtual Channel</i> .
East Port	If Port is set above, enter the port to be configured.
RPL Port	Tick the check box and use the drop-down menu to select <i>West</i> , <i>East</i> , or <i>None</i> . <i>West</i> - Specify the west ring port as the RPL port. <i>East</i> - Specify the east ring port as the RPL port. <i>None</i> - This indicates that there is no RPL port on this node. By default, the node has no RPL

	port.
RPL Owner	Enable or disable the RPL owner. <i>Enabled</i> specifies the device as an RPL owner node. <i>Disabled</i> indicates the node is not an RPL owner. By default, the RPL owner is disabled.
Protected VLAN Action	This is used to configure the VLANs that are protected by the ERPS function. The R-APS VLAN cannot be the protected VLAN. The protected VLAN can be one that has already been created, or it can be used for a VLAN that has not yet been created. Toggle between <i>Add</i> or <i>Delete</i> . <i>Add</i> - This adds VLANs to the protected VLAN group. <i>Delete</i> - This removes VLANs from the protected VLAN group.
Protected VIDList	Tick this check box and enter the VLANs to be added or deleted.
Ring MEL (0-7)	Enter the ring MEL of the R-APS function. The range is from 0 to 7. The default ring MEL is 1.
Holdoff Time (0-10000)	The Holdoff timer is used to filter out intermittent link faults when link failures occur during the protection switching process. When a ring node detects a link failure, it will start the holdoff timer and report the link failure event (R-APS BPDU with SF flag) after the link failure is confirmed within period of time specified. The range is from 0 to 10000 milliseconds. The default holdoff time is 0 milliseconds.
Guard Time (10-2000)	The Guard timer is used to prevent ring nodes from receiving outdated R-APS messages. This timer is used during the protection switching process after the link failure recovers. When the link node detects the recovery of the link, it will report the link failure recovery event (R-APS PDU with NR flag) and start the guard timer. Before the guard timer expires, all received R-APS messages are ignored by this ring node, except in the case where a burst of three R-APS event messages that indicates the topology of a sub-ring has changed and the node needs to flush FDB are received on the node. In this case, the recovered link does not go into a blocking state. The Guard Timer should be greater than the maximum expected forwarding delay for which one R-APS message circles around the ring. The range is from 10 to 2000 milliseconds. The default guard time is 500 milliseconds.
WTR Time (5-12)	The WTR timer is used to prevent frequent operation of the protection switch due to an intermittent defect. This timer is used during the protection switching process when a link failure recovers. It is only used by the RPL owner. When the RPL owner in protection state receives R-APS PDU with an NR flag, it will start the WTR timer. The RPL owner will block the original unblocked RPL port and start to send R-APS PDU with an RB flag after the link recovery is confirmed within this period of time. The range is from 5 to 12 minutes. The default WTR time is 5 minutes.

Click **Apply** to implement changes made.

To edit ERPS RAPS Sub Ring Settings for an ERPS RAPS VLAN Table entry, click the **Modify** button in the Sub Ring Modify column in the ERPS RAPS VLAN Table. The following window will open:

Figure 3 - 80 ERPS RAPS VLAN Table - Edit Sub Ring window

The following fields can be set:

Parameter	Description
Sub-Ring R-APS VLAN Action	Toggle between <i>Add</i> or <i>Delete</i> . <i>Add</i> connects the sub-ring to another ring. <i>Delete</i> disconnects the sub-ring from a connected ring.
Sub-Ring R-APS VLAN	Enter sub-ring R-APS VLAN.
TC Propagation State	This is used to configure the state of topology change propagation for the sub-ring. This setting is applied on the interconnection node.

Click **Apply** to implement changes made.

DULD Settings

The Switch features a D-Link Unidirectional Link Detection (DULD) module. The unidirectional link detection provides a mechanism that can be used to detect unidirectional link for Ethernet switches whose PHYs do not support unidirectional OAM operation. This function is established based on OAM, so OAM should be enabled before starting detection.

To view this window, click **L2 Features > DULD Settings**, as shown below.

DULD Settings						
Unit	From	To	Admin State	Mode	Discovery Time (5-65535 sec)	Apply
1	Port 1	Port 1	Disabled	Normal	5	Apply

DULD Table					
Port	Admin State	Oper Status	Mode	Link Status	Discovery Time
1	Disabled	Disabled	Normal	Unknown	5
2	Disabled	Disabled	Normal	Unknown	5
3	Disabled	Disabled	Normal	Unknown	5
4	Disabled	Disabled	Normal	Unknown	5
5	Disabled	Disabled	Normal	Unknown	5
6	Disabled	Disabled	Normal	Unknown	5
7	Disabled	Disabled	Normal	Unknown	5
8	Disabled	Disabled	Normal	Unknown	5
9	Disabled	Disabled	Normal	Unknown	5
10	Disabled	Disabled	Normal	Unknown	5
11	Disabled	Disabled	Normal	Unknown	5
12	Disabled	Disabled	Normal	Unknown	5
13	Disabled	Disabled	Normal	Unknown	5
14	Disabled	Disabled	Normal	Unknown	5
15	Disabled	Disabled	Normal	Unknown	5
16	Disabled	Disabled	Normal	Unknown	5
17	Disabled	Disabled	Normal	Unknown	5
18	Disabled	Disabled	Normal	Unknown	5
19	Disabled	Disabled	Normal	Unknown	5
20	Disabled	Disabled	Normal	Unknown	5
21	Disabled	Disabled	Normal	Unknown	5
22	Disabled	Disabled	Normal	Unknown	5
23	Disabled	Disabled	Normal	Unknown	5
24	Disabled	Disabled	Normal	Unknown	5

Figure 3 - 81 DULD Settings window

The following fields can be set:

Parameter	Description
Unit	Select the unit you wish to configure.

From / To	Select a range of ports.
Admin State	Enable or disable the administration state. This indicates these ports unidirectional link detection status. The default state is <i>Disabled</i> .
Mode	Toggle between <i>Shutdown</i> and <i>Normal</i> . When <i>Shutdown</i> is selected, if any unidirectional link is detected, this feature will disable the port and log an event. When <i>Normal</i> is selected, this feature will only log an event when a unidirectional link is detected.
Discovery Time (5-65535 sec)	Enter the port neighbor discovery time between 5 and 65535 seconds. If the discovery is timed out, the unidirectional link detection will start. The default discovery time is 5 seconds

Click **Apply** to implement the changes.

NLB Multicast FDB Settings

The Switch supports Network Load Balancing (NLB). This is a MAC forwarding control for supporting the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. The server can work in two different modes – unicast mode and multicast mode. In unicast mode, the client uses a unicast MAC address as the destination MAC to reach the server. In multicast mode, the client uses a multicast MAC address as the destination MAC to reach the server. The destination MAC is the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet. The NLB multicast FDB entry will be mutually exclusive with the L2 multicast entry. At the current time, only multicas mode is supported.

To view this window, click **L2 Features > NLB Multicast FDB Settings**, as shown below.

Add				
Total Entries: 1				
NLB Multicast FDB Table				
MAC Address	VID	Egress Ports	Modify	Delete
01-00-5E-00-00-02	1		Modify	X

Figure 3 - 82 NLB Multicast FDB Table window

To remove an entry from the table, click its corresponding under the Delete heading.

To add a new entry, click **Add** to see the window shown below.

NLB Multicast FDB Settings - Add	
VLAN Name	<input type="radio"/> <input type="text"/>
VID (1-4094)	<input type="radio"/> <input type="text"/>
MAC Address	<input type="text"/>
Apply	
Show All NLB Multicast FDB Entries	

Figure 3 - 83 NLB Multicast FDB Settings - Add window

The following fields can be set:

Parameter	Description
-----------	-------------

VLAN Name	Click the radio button and enter the VLAN of the NLB multicast FDB entry to be created.
VID (1-4094)	Click the radio button and enter the VLAN by the VLAN ID.
MAC Address	Enter the MAC address of the NLB multicast FDB entry to be created.

Click **Apply** to implement the changes. To view the NLB Multicast FDB Table, click the hyperlinked [Show All NLB Multicast FDB Entries](#).

To edit an entry, click the corresponding **Modify** button in the NLB Multicast FDB Table window to see the window shown below.

Figure 3 - 84 NLB Multicast FDB Settings - Edit window

The following fields can be configured or viewed:

Parameter	Description
VLAN Name	Display the VLAN of the NLB multicast FDB entry.
VID (1-4094)	Display the VLAN ID of the NLB multicast FDB entry.
MAC Address	Display the MAC address of the NLB multicast FDB entry.
Ports Action	Use the drop-down menu to add or remove a list of forwarding ports.
Ports	Enter a list of ports to be added or removed.

Click **Apply** to implement the changes.

QoS

802.1p Settings

Bandwidth Control

HOL Prevention Settings

Schedule Settings

QoS

The xStack® DGS-3400 Series supports 802.1p priority queuing Quality of Service. The following section discusses the implementation of QoS (Quality of Service) and benefits of using 802.1p priority queuing.

The Advantages of QoS

QoS is an implementation of the IEEE 802.1p standard that allows network administrators a method of reserving bandwidth for important functions that require a large bandwidth or have a high priority, such as VoIP (voice-over Internet Protocol), web browsing applications, file server applications or video conferencing. Not only can a larger bandwidth be created, but other less critical traffic can be limited, so excessive bandwidth can be saved. The Switch has separate hardware queues on every physical port to which packets from various applications can be mapped to, and, in turn prioritized. View the following map to see how the xStack® DGS-3400 switch series implements basic 802.1p priority queuing.

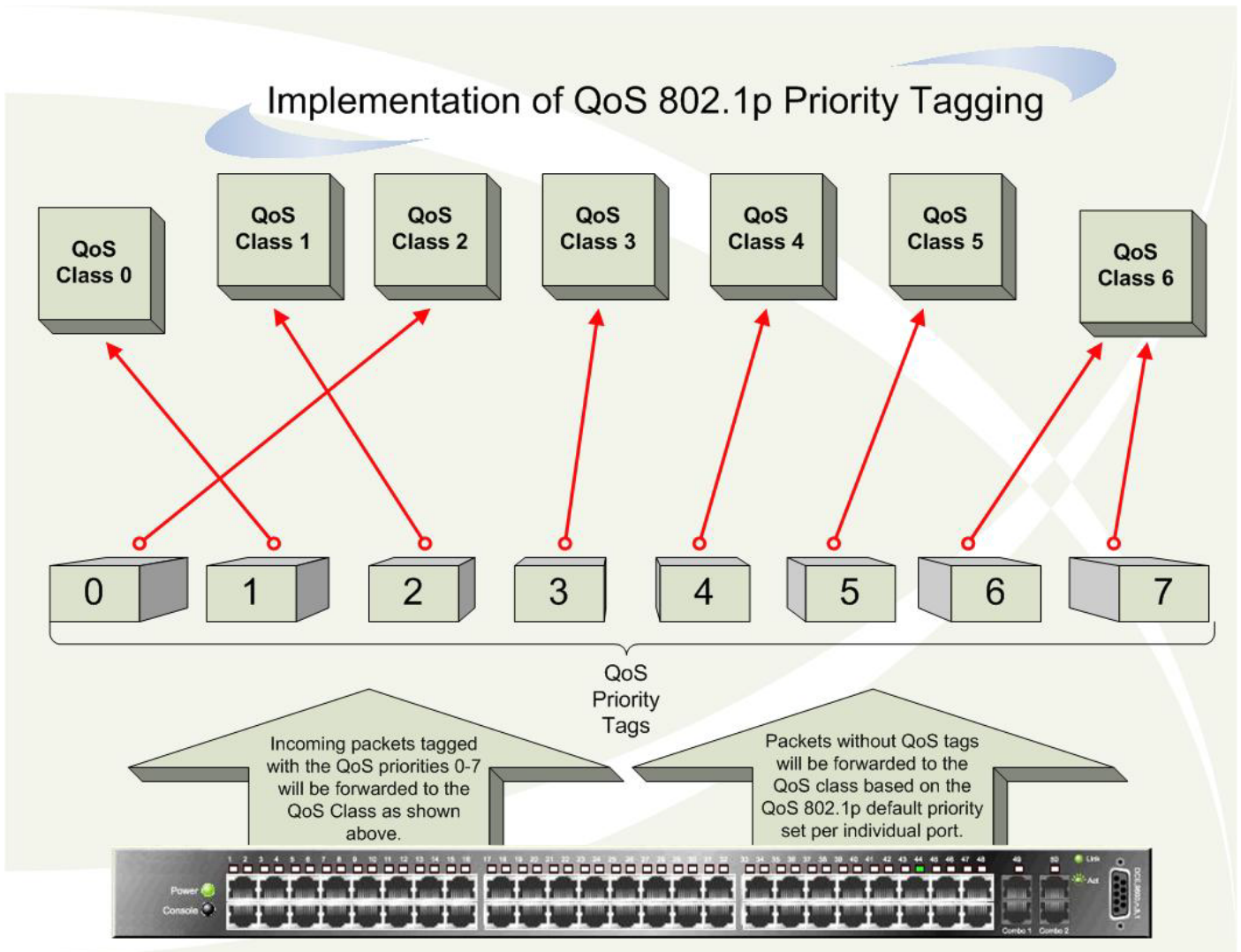


Figure 4 - 1 An Example of the Default QoS Mapping on the Switch

The picture above shows the default priority setting for the Switch. Class-6 has the highest priority of the seven priority classes of service on the Switch. In order to implement QoS, the user is required to instruct the Switch to examine the header of a packet to see if it has the proper identifying tag. Then the user may forward these tagged packets to designated classes of service on the Switch where they will be emptied, based on priority.

For example, let's say a user wishes to have a video conference between two remotely set computers. The administrator can add priority tags to the video packets being sent out, utilizing the Access Profile commands. Then, on the receiving end, the administrator instructs the Switch to examine packets for this tag, acquires the tagged packets and maps them to a class queue on the Switch. Then in turn, the administrator will set a priority for this queue so that will be emptied before any other packet is forwarded. This results in the end user receiving all packets sent as quickly as possible, thus prioritizing the queue and allowing for an uninterrupted stream of packets, which optimizes the use of bandwidth available for the video conference.

Understanding QoS

The xStack® DGS-3400 Series supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 6 (Class 6) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q6 queue.

For strict priority-based scheduling, any packets residing in the higher priority classes of service are transmitted first. Multiple strict priority classes of service are emptied based on their priority tags. Only when these classes are empty, are packets of lower priority transmitted.

For weighted round-robin queuing, the number of packets sent from each priority queue depends upon the assigned weight. For a configuration of 8 CoS queues, A~H, with their respective weight value: 8~1. When each queue has 10 outbound packets, they are sent in the following sequence:

A1, B1, C1, D1, E1, F1, G1, H1,

A2, B2, C2, D2, E2, F2, G2,

A3, B3, C3, D3, E3, F3,

A4, B4, C4, D4, E4,

A5, B5, C5, D5,

A6, B6, C6,

A7, B7,

A8,

A9, B8, C7, D6, E5, F4, G3, H2,

A10, B9, C8, D7, E6, F5, G4

B10, C9, D8, E7, F6,

C10, D9, E8,

D10,

E9, F7, G5, H3,

E10, F8, G6,

F9,

F10, G7, H4,

G8,

G9, H5,

G10, H6 ~ H10

For weighted round-robin queuing, if each CoS queue has the same weight value, then each CoS queue has an equal opportunity to send packets just like round-robin queuing.

For weighted round-robin queuing, if the weight for a CoS is set to 0, then it will continue processing the packets from this CoS until there are no more packets for this CoS. The other CoS queues that have been given a nonzero value, and depending upon the weight, will follow a common weighted round-robin scheme.

Remember that the xStack® DGS-3400 switch series has 7 configurable priority queues (and seven Classes of Service) for each port on the Switch.



NOTICE: The Switch contains eight classes of service for each port on the Switch. One of these classes is reserved for internal use on the Switch and is therefore not configurable. All references in the following section regarding classes of service will refer to only the seven classes of service that may be used and configured by the administrator.

Understanding IEEE 802.1p Priority

Priority tagging is a function defined by the IEEE 802.1p standard designed to provide a means of managing traffic on a network where many different types of data may be transmitted simultaneously. It is intended to alleviate problems associated with the delivery of time critical data over congested networks. The quality of applications that are dependent on such time critical data, such as video conferencing, can be severely and adversely affected by even very small delays in transmission.

Network devices that comply with the IEEE 802.1p standard have the ability to recognize the priority level of data packets. These devices can also assign a priority label or tag to packets. Compliant devices can also strip priority tags from packets. This priority tag determines the packet's degree of expeditiousness and determines the queue to which it will be assigned.

Priority tags are given values from 0 to 7 with 0 being assigned to the lowest priority data and 7 assigned to the highest. The highest priority tag 7 is generally only used for data associated with video or audio applications, which are sensitive to even slight delays, or for data from specified end users whose data transmissions warrant special consideration.

The Switch allows you to further tailor how priority tagged data packets are handled on your network. Using queues to manage priority tagged data allows you to specify its relative priority to suit the needs of your network. There may be circumstances where it would be advantageous to group two or more differently tagged packets into the same queue. Generally, however, it is recommended that the highest priority queue, Queue 7, be reserved for data packets with a priority value of 7. Packets that have not been given any priority value are placed in Queue 0 and thus given the lowest priority for delivery.

Strict mode and weighted round robin system are employed on the Switch to determine the rate at which the queues are emptied of packets. The ratio used for clearing the queues is 4:1. This means that the highest priority queue, Queue 7, will clear 4 packets for every 1 packet cleared from Queue 0.

Remember, the priority queue settings on the Switch are for all ports, and all devices connected to the Switch will be affected. This priority queuing system will be especially beneficial if your network employs switches with the capability of assigning priority tags.

802.1p Settings

802.1p Default Priority Settings

The Switch allows the assignment of a default 802.1p priority to each port on the Switch. The priority tags are numbered from 0, the lowest priority, to 7, the highest priority.

To view this window, click **QoS > 802.1p Settings > 802.1p Default Priority Settings**, as shown below.

802.1p Default Priority Settings

Unit	From	To	Priority	Apply
1 ▾	Port 1 ▾	Port 1 ▾	0 ▾	Apply

802.1p Default Priority Table

Port	Priority	Effective Priority
1	0	0
2	0	0
3	0	0
4	0	0
5	0	0
6	0	0
7	0	0
8	0	0
9	0	0
10	0	0
11	0	0
12	0	0
13	0	0
14	0	0
15	0	0
16	0	0
17	0	0
18	0	0
19	0	0
20	0	0
21	0	0
22	0	0
23	0	0
24	0	0

Figure 4 - 2 802.1p Default Priority window

The following parameters can be configured:

Parameter	Description
Unit	Use the pull-down menu to choose the switch unit from the switch stack.
From / To	Enter a port range by using the pull-down menus in the From and To fields.
Priority	The priority tags are numbered from 0, the lowest priority, to 7, the highest priority. Insert a priority

value, from 0-7 in the Priority field.

Click **Apply** to implement the changes.

802.1p User Priority Settings

The xStack® DGS-3400 Series allows the assignment of a class of service to each of the 802.1p priorities.

To view this window, click **QoS > 802.1p Settings > 802.1p User Priority Settings**, as shown below.

Unit	From	To	Priority	Class ID	Apply
1	Port 1	Port 1	0	Class-0	Apply

Port	Priority	Class ID
1	0	Class-2
1	1	Class-0
1	2	Class-1
1	3	Class-3
1	4	Class-4
1	5	Class-5
1	6	Class-6
1	7	Class-6
2	0	Class-2
2	1	Class-0
2	2	Class-1
2	3	Class-3
2	4	Class-4
2	5	Class-5
2	6	Class-6
2	7	Class-6
3	0	Class-2

Figure 4 - 3 802.1p User Priority window

The following parameters can be configured:

Parameter	Description
Unit	Use the pull-down menu to choose the switch unit from the switch stack.
From / To	Enter a port range by using the pull-down menus in the From and To fields.
Priority	The priority tags are numbered from 0, the lowest priority, to 7, the highest priority. Insert a priority value, from 0-7 in the Priority field.

Class ID	Use the pull-down menu to select the Switch's hardware priority queue. The switch has seven hardware priority queues available.
-----------------	---

Click **Apply** to implement the changes.

Bandwidth Control

The Bandwidth Control section includes Bandwidth Control Settings and Per Queue Bandwidth Control Settings. Bandwidth Control is to limit a port's bandwidth. The RX and TX rate can be configured separately.

Bandwidth Control Settings

The bandwidth control settings are used to place a ceiling on the transmitting and receiving data rates for any selected port.

To view this window, click **QoS > Bandwidth Control > Bandwidth Control Settings**, as shown below.

Bandwidth Control Settings						
Unit	From	To	Type	No Limit	Rate (64-10000000)	Apply
1	Port 1	Port 1	Both	Enabled	Kbit/sec	Apply

Bandwidth Control Table				
Port	RX Rate (Kbit/sec)	TX Rate (Kbit/sec)	Effective RX (Kbit/sec)	Effective TX (Kbit/sec)
1	No Limit	No Limit	No Limit	No Limit
2	No Limit	No Limit	No Limit	No Limit
3	No Limit	No Limit	No Limit	No Limit
4	No Limit	No Limit	No Limit	No Limit
5	No Limit	No Limit	No Limit	No Limit
6	No Limit	No Limit	No Limit	No Limit
7	No Limit	No Limit	No Limit	No Limit
8	No Limit	No Limit	No Limit	No Limit
9	No Limit	No Limit	No Limit	No Limit
10	No Limit	No Limit	No Limit	No Limit
11	No Limit	No Limit	No Limit	No Limit
12	No Limit	No Limit	No Limit	No Limit
13	No Limit	No Limit	No Limit	No Limit
14	No Limit	No Limit	No Limit	No Limit
15	No Limit	No Limit	No Limit	No Limit
16	No Limit	No Limit	No Limit	No Limit
17	No Limit	No Limit	No Limit	No Limit
18	No Limit	No Limit	No Limit	No Limit
19	No Limit	No Limit	No Limit	No Limit
20	No Limit	No Limit	No Limit	No Limit
21	No Limit	No Limit	No Limit	No Limit
22	No Limit	No Limit	No Limit	No Limit
23	No Limit	No Limit	No Limit	No Limit
24	No Limit	No Limit	No Limit	No Limit

Figure 4 - 4 Bandwidth Settings window

The following parameters can be set or are displayed:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From / To	A consecutive group of ports may be configured starting with the selected port.
Type	This drop-down menu allows a selection between <i>RX</i> (receive,) <i>TX</i> (transmit,) and <i>Both</i> . This setting will determine whether the bandwidth ceiling is applied to receiving, transmitting, or both receiving and transmitting packets.
No Limit	This drop-down menu allows the user to specify that the selected port will have no bandwidth limit. <i>Enabled</i> disables the limit.
Rate (64-10000000)	This field allows the input of the data rate that will be the limit for the selected port. The user may choose a rate between 64 and 10000000 units, where each unit is defined a 1Kbit/s.

Effective RX rate	Specifies the limitation of the received data rate.
Effective TX rate	Specifies the limitation of the transmitted data rate.

Click **Apply** to set the bandwidth control for the selected ports. Results of configured Bandwidth Settings will be displayed in the Bandwidth Control Table.

Per Queue Bandwidth Control Settings

This window sets the bandwidth control for each specific queue on specified ports.

To view this window, click **QoS > Bandwidth Control > Per Queue Bandwidth Control Settings**, as shown below.

Per Queue Bandwidth Control Settings						
Unit	From	To	Queue	Min Rate (64-10000000)	Max Rate (64-10000000)	Apply
1	Port 1	Port 1	0	<input type="text"/> Kbit/sec <input checked="" type="checkbox"/> No Limit	<input type="text"/> Kbit/sec <input checked="" type="checkbox"/> No Limit	<input type="button" value="Apply"/>

Queue Bandwidth Control Table			
Port	Queue	Min Rate (Kbit/sec)	Max Rate (Kbit/sec)
1	0	No Limit	No Limit
1	1	No Limit	No Limit
1	2	No Limit	No Limit
1	3	No Limit	No Limit
1	4	No Limit	No Limit
1	5	No Limit	No Limit
1	6	No Limit	No Limit
2	0	No Limit	No Limit
2	1	No Limit	No Limit
2	2	No Limit	No Limit
2	3	No Limit	No Limit
2	4	No Limit	No Limit
2	5	No Limit	No Limit
2	6	No Limit	No Limit
3	0	No Limit	No Limit
3	1	No Limit	No Limit
3	2	No Limit	No Limit
3	3	No Limit	No Limit
3	4	No Limit	No Limit
3	5	No Limit	No Limit
3	6	No Limit	No Limit
4	0	No Limit	No Limit
4	1	No Limit	No Limit

Figure 4 - 5 Per Queue Bandwidth Control Settings window

The following parameters can be set:

Parameter	Description
Unit	Select the switch in the switch stack to be modified.
From / To	A consecutive group of ports may be configured starting with the selected port.
Queue	Use the pull-down menu to select the priority queue from 0 to 6.
Min Rate (64-10000000)	Enter a value between 64 and 10000000 Kbit/sec or tick the No Limit check box to specify the minimum rate of packets to be received.
Max Rate (64-10000000)	Enter a value between 64 and 10000000 Kbit/sec or tick the No Limit check box to specify the maximum rate of packets to be received.

Click **Apply** to implement the changes.

HOL Prevention Settings

This window is used to enable or disable Head of Line (HOL) prevention.

To view the HOL Prevention Settings window, click **QoS > HOL Prevention Settings**, as shown below.

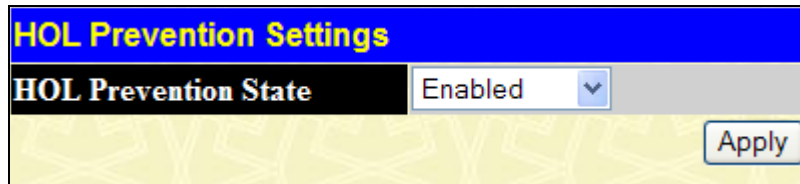


Figure 4 - 6 Per Queue Bandwidth Control Settings window

Use the drop-down menu to enable or disable head of line prevention. The default is *Enabled*. Click **Apply** to implement the change.

Schedule Settings

QoS Output Scheduling Settings

QoS can be customized by changing the output scheduling used for the hardware classes of service in the Switch. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority classes of service is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If choosing to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view this window, click **QoS > Schedule Settings > QoS Output Scheduling Settings**, as shown below.

QoS Output Scheduling Settings					
Unit	From	To	Class ID	Max Pakcet (0-15)	Apply
1	Port 1	Port 1	Class-0		Apply

QoS Output Scheduling Table		
Port	Class ID	Max Packet
1	Class-0	1
1	Class-1	2
1	Class-2	3
1	Class-3	4
1	Class-4	5
1	Class-5	6
1	Class-6	7
2	Class-0	1
2	Class-1	2
2	Class-2	3
2	Class-3	4
2	Class-4	5
2	Class-5	6
2	Class-6	7
3	Class-0	1
3	Class-1	2
3	Class-2	3
3	Class-3	4

Figure 4 - 7 QoS Output Scheduling window

The following values may be assigned to the QoS classes to set the scheduling.

Parameter	Description
Unit	Select the unit to configure.
From / To	A consecutive group of ports may be configured starting with the selected port.
Class ID	Select the class ID from <i>Class-0</i> through <i>Class-6</i> .
Max Packet (0-15)	Specifies the maximum number of packets the above specified hardware priority class of service will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 15 can be specified.

Click **Apply** to implement changes made.



NOTE: Entering a 0 for the Max Packets field in the **QoS Output Scheduling** window above will create a Combination Queue. For more information on implementation of this feature, see the next section, Configuring the Combination Queue.

Configuring the Combination Queue

Utilizing the QoS Output Scheduling window shown above, the xStack® DGS-3400 Series can implement a combination queue for forwarding packets. This combination queue allows for a combination of strict and weight-fair (weighted round-robin, or WRR) scheduling for emptying given classes of service. To set the combination queue, enter a 0 for the Max Packets entry of the corresponding priority classes of service listed in the window above. Priority classes of service that have a 0 in the Max Packet field will forward packets with strict priority scheduling. The remaining classes of service, that do not have a 0 in their Max Packet field, will follow a weighted round-robin method of forwarding packets — as long as the priority classes of service with a 0 in their Max Packet field are empty. When a packet arrives in a priority class with a 0 in its Max Packet field, this class of service will automatically begin forwarding packets until it is empty. Once a priority class of service with a 0 in its Max Packet field is empty, the remaining priority classes of service will reset the WRR cycle of forwarding packets, starting with the highest available priority class of service. Priority classes of service with an equal level of priority and equal entries in their Max Packet field will empty their fields based on hardware priority scheduling. The Max Packet parameter allows the maximum number of packets a given priority class of service can transmit per WRR scheduling cycle to be selected. This provides for a controllable CoS behavior while allowing other classes to empty as well. A value between 0 and 15 packets can be specified per priority class of service to create the combination queue.

QoS Scheduling Mechanism Settings

Changing the output scheduling used for the hardware queues in the Switch can customize QoS. As with any changes to QoS implementation, careful consideration should be given to how network traffic in lower priority queues is affected. Changes in scheduling may result in unacceptable levels of packet loss or significant transmission delay. If the user chooses to customize this setting, it is important to monitor network performance, especially during peak demand, as bottlenecks can quickly develop if the QoS settings are not suitable.

To view the following window, click **QoS > Schedule Settings > QoS Scheduling Mechanism Settings**, as shown below.

QoS Scheduling Mechanism Settings				
Unit	From	To	Mode	Apply
1	Port 1	Port 1	Strict	Apply

QoS Scheduling Mechanism Table	
Port	Mode
1	Strict
2	Strict
3	Strict
4	Strict
5	Strict
6	Strict
7	Strict
8	Strict
9	Strict
10	Strict
11	Strict
12	Strict
13	Strict
14	Strict
15	Strict
16	Strict
17	Strict
18	Strict
19	Strict
20	Strict
21	Strict
22	Strict
23	Strict
24	Strict

Figure 4 - 8 QoS Scheduling Mechanism window

The following parameters can be configured.

Parameter	Description
Unit	Select the unit to configure.
From / To	A consecutive group of ports may be configured starting with the selected port.

Mode	<p>Use the pull-down menu to select one of the following modes.</p> <p><i>Strict</i> - The highest class of service is the first to process traffic. That is, the highest class of service will finish before other queues empty.</p> <p><i>Weight Fair</i> - Use the weighted round-robin (<i>WRR</i>) algorithm to handle packets in an even distribution in priority classes of service.</p>
-------------	---

Click **Apply** to allow changes to take effect.

Section 5

ACL (Access Control List)

Time Range

Access Profile Table

ACL Flow Meter

CPU Interface Filtering

Time Range

This window is used in conjunction with the Access Profile feature to determine a starting point and an ending point, based on days of the week, when an Access Profile configuration will be enabled on the Switch. Once configured here, the time range settings are to be applied to an access profile rule using the **Access Profile Table** window. The user may enter up to 64 time range entries on the Switch.



NOTE: The Time Range commands are based on the time settings of the Switch. Make sure to configure the time for the Switch appropriately for these commands using commands listed in the following chapter, **Time and SNTP Commands**.

To view this window, click **ACL > Time Range**, as shown below.

Time Range Settings

Range Name	<input style="width: 90%;" type="text"/>															
Hours (HH MM SS)	Start Time	00 ▾	00 ▾	00 ▾	End Time	00 ▾	00 ▾	00 ▾								
Weekdays	Mon	<input type="checkbox"/>	Tue	<input type="checkbox"/>	Wed	<input type="checkbox"/>	Thu	<input type="checkbox"/>	Fri	<input type="checkbox"/>	Sat	<input type="checkbox"/>	Sun	<input type="checkbox"/>	Select All Days	<input type="checkbox"/>

Total Entries: 0

Time Range Information

Range Name	Days	Start Time	End Time	Delete

Figure 5 - 1 Time Range Settings window

The user may adjust the following parameters to configure a time range on the Switch:

Parameter	Description
Range Name	Enter a name of no more than 32 alphanumeric characters that will be used to identify this time range on the Switch. This range name will be used in the Access Profile Table window to identify the access profile and associated rule to be enabled during this time range.
Hours (HH MM SS)	This parameter is used to set the time in the day that this time range is to be enabled using the following parameters: <ul style="list-style-type: none"> <i>Start Time</i> – Use this parameter to identify the starting time of the time range, in hours, minutes and seconds, based on the 24-hour time system. <i>End Time</i> – Use this parameter to identify the ending time of the time range, in hours, minutes and seconds, based on the 24-hour time system.
Weekdays	Use the check boxes to select the corresponding days of the week that this time range is to be enabled. Tick the Select All Days check box to configure this time range for every day of the week.

Click **Apply** to implement changes made. Currently configured entries will be displayed in the Time Range Information table in the bottom half of the window shown above.

Access Profile Table

Access profiles allow you to establish criteria to determine whether the Switch will forward packets based on the information contained in each packet's header. These criteria can be specified on a basis of VLAN, MAC address or IP address.

Creating an access profile is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below in two parts.

To view this window, click **ACL > Access Profile Table**, as shown below.

Profile ID	Type	Access Rule	Display	Delete
1	IP	Modify	View	X
2	Ethernet	Modify	View	X
3	Packet Content	Modify	View	X
4	IPv6	Modify	View	X

Figure 5 - 2 Access Profile Table window

To add an entry to the **Access Profile Table** window, click the **Add Profile** button. This will open the **Access Profile Configuration** window, as shown below. There are four **Access Profile Configuration** windows; one for Ethernet (or MAC address-based) profile configuration, one for IP address-based profile configuration, one for Packet Content, and one IPv6. Switch between the four **Access Profile Configuration** windows by using the Type drop-down menu. The window shown below is the **Ethernet Access Profile Configuration** window. To remove all access profiles from this table, click **Clear All**.

Profile ID (1-6)	1
Type	Ethernet
VLAN	<input type="checkbox"/>
Source MAC	<input type="checkbox"/> 00-00-00-00-00-00
Destination MAC	<input type="checkbox"/> 00-00-00-00-00-00
802.1p	<input type="checkbox"/>
Ethernet Type	<input type="checkbox"/>

Apply

[Show All Access Profile Table Entries](#)

Figure 5 - 3 Access Profile Configuration window (Ethernet)

The following parameters can be set, for the Ethernet type:

Parameter	Description
Profile ID (1-6)	Type in a unique identifier number for this profile set. This value can be set from 1 to 6.
Type	Select profile based on Ethernet (MAC Address), IP, Packet Content or IPv6 address. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header. Select <i>Packet Content</i> to instruct the Switch to examine the packet header.
VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
Source MAC	Source MAC Mask – Enter a MAC address mask for the source MAC address.
Destination MAC	Destination MAC Mask – Enter a MAC address mask for the destination MAC address.
802.1p	Selecting this option instructs the Switch to examine the 802.1p priority value of each packet header and use this as the, or part of the criterion for forwarding.
Ethernet Type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click **Apply** to implement the changes.

To view the settings for a created profile, click its corresponding **View** button in the **Access Profile Table** window, revealing the following window:

Access Profile Entry Display	
Profile ID	2
Owner	ACL
Type	Ethernet
VLAN	-----
Source MAC	-----
Destination MAC	-----
802.1p	-----
Ethernet Type	Enabled
Show All Access Profile Table Entries	

Figure 5 - 4 Access Profile Entry Display window (Ethernet)

The window shown below is the **IP Access Profile Configuration** window:

Access Profile Configuration	
Profile ID (1-6)	1
Type	IP
VLAN	<input type="checkbox"/>
Source IP Mask	<input type="checkbox"/> 0.0.0.0
Destination IP Mask	<input type="checkbox"/> 0.0.0.0
DSCP	<input type="checkbox"/>
Protocol	<input type="checkbox"/> ICMP <input type="checkbox"/> type <input type="checkbox"/> code <input type="radio"/> IGMP <input type="checkbox"/> type <input type="radio"/> TCP <input type="checkbox"/> src port mask 0000 <input type="checkbox"/> dst port mask 0000 <input type="checkbox"/> flag bit <input type="checkbox"/> urg <input type="checkbox"/> ack <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> fin <input type="radio"/> UDP <input type="checkbox"/> src port mask 0000 <input type="checkbox"/> dst port mask 0000 <input type="radio"/> Protocol id 00 <input type="checkbox"/> user mask 00000000
<input type="button" value="Apply"/>	
Show All Access Profile Table Entries	

Figure 5 - 5 Access Profile Configuration window (IP)

The following parameters can be set, for IP:

Parameter	Description
Profile ID (1-6)	Type in a unique identifier number for this profile set. This value can be set from 1 to 6.
Type	Select profile based on Ethernet (MAC Address), IP, Packet Content or IPv6 address. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header. Select <i>Packet Content</i> to instruct the Switch to examine the packet header.
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Enter an IP address mask for the source IP address.
Destination IP Mask	Enter an IP address mask for the destination IP address.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines: Select <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header.

- *Type* - Further specify that the access profile will apply an ICMP type value.
- *Code* - Further specify that the access profile will apply an ICMP code value.

Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.

- *Type* - Further specify that the access profile will apply an IGMP type value.

Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask.

- *src port mask* – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter.
- *dst port mask* – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter.
- *flag bit* – The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish).

Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.

- *src port mask* – Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff).
- *dst port mask* – Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff).

protocol id – Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff).

Click **Apply** to implement the changes.

To view the settings for a created profile, click its corresponding **View** button in the **Access Profile Table** window, revealing the following window.

Access Profile Entry Display	
Profile ID	1
Owner	ACL
Type	IP
VLAN	Enabled
Source IP Mask	-----
Destination IP Mask	-----
DSCP	-----
Protocol	
Show All Access Profile Table Entries	

Figure 5 - 6 Access Profile Entry Display window (IP)

The page shown below is the IPv6 configuration window.

Figure 5 - 7 Access Profile Configuration window (IPv6)

The following parameters can be set, for IP:

Parameter	Description
Profile ID (1-6)	Type in a unique identifier number for this profile set. This value can be set from 1 to 6.
Type	Select profile based on Ethernet (MAC Address), IP, Packet Content or IPv6 address. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header. Select <i>Packet Content</i> to instruct the Switch to examine the packet header.
Class	Checking this field will instruct the Switch to examine the <i>class</i> field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
Flow Label	Checking this field will instruct the Switch to examine the <i>flow label</i> field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Mask	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
Destination IPv6 Mask	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. Then the user must specify what protocol(s) to include according to the following guidelines: Select <i>TCP</i> to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires that you specify a source port mask and/or a destination port mask. <ul style="list-style-type: none"> <i>src port mask</i> – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter. <i>dst port mask</i> – Specify a TCP port mask for the destination port in hex form (hex

	<p>0x0-0xffff) which you wish to filter.</p> <p>Select <i>UDP</i> to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.</p> <ul style="list-style-type: none"> • <i>src port mask</i> – Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff). • <i>dst port mask</i> – Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff).
--	--

Click **Apply** to implement the changes.

To view the settings for a created profile, click its corresponding **View** button in the **Access Profile Table** window, revealing the following window.

Access Profile Entry Display	
Profile ID	4
Owner	ACL
Type	IPv6
Class	Enabled
Flow Label	-----
Source IPv6 Mask	-----
Destination IPv6 Mask	-----
Protocol	-----
Show All Access Profile Table Entries	

Figure 5 - 8 Access Profile Entry Display (IPv6)

The window shown below is the Access Profile Configuration window for Packet Content Mask:

Access Profile Configuration	
Profile ID (1-6)	<input type="text" value="1"/>
Type	Packet Content <input type="button" value="v"/>
Offset	<input type="checkbox"/> Chunk 1 (0-31) <input type="text"/> mask <input type="text" value="00000000"/>
	<input type="checkbox"/> Chunk 2 (0-31) <input type="text"/> mask <input type="text" value="00000000"/>
	<input type="checkbox"/> Chunk 3 (0-31) <input type="text"/> mask <input type="text" value="00000000"/>
	<input type="checkbox"/> Chunk 4 (0-31) <input type="text"/> mask <input type="text" value="00000000"/>
<input type="button" value="Apply"/>	
Show All Access Profile Table Entries	

Figure 5 - 9 Access Profile Configuration window (Packet Content Mask)

This window will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the Packet Content Mask:

Parameter	Description																														
Profile ID (1-6)	Type in a unique identifier number for this profile set. This value can be set from 1 to 6.																														
Type	<p>Select profile based on Ethernet (MAC Address), IP address, packet content mask or IPv6. This will change the menu according to the requirements for the type of profile.</p> <ul style="list-style-type: none"> Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 part of each packet header. 																														
Offset	<p>The offset field is used to examine the packet header which is divided up into four “chunks” where each chunk represents 4 bytes. Values within the packet header chunk to be identified are to be marked in hexadecimal form in the “mask” field. The following table will help you identify the bytes in the respective chunks.</p> <table border="1"> <thead> <tr> <th>chunk0</th> <th>chunk1</th> <th>chunk2.....</th> <th>chunk29</th> <th>chunk30</th> <th>chunk31</th> </tr> </thead> <tbody> <tr> <td>b126</td> <td>b2</td> <td>b6</td> <td>b114</td> <td>b118</td> <td>b122</td> </tr> <tr> <td>b127</td> <td>b3</td> <td>b7</td> <td>b115</td> <td>b119</td> <td>b123</td> </tr> <tr> <td>b0</td> <td>b4</td> <td>b8</td> <td>b116</td> <td>b120</td> <td>b124</td> </tr> <tr> <td>b1</td> <td>b5</td> <td>b9</td> <td>b117</td> <td>b121</td> <td>b125</td> </tr> </tbody> </table> <p>Check the box of the chunk, from 1 to 4, you wish to examine and then enter the hexadecimal value in the mask field.</p>	chunk0	chunk1	chunk2.....	chunk29	chunk30	chunk31	b126	b2	b6	b114	b118	b122	b127	b3	b7	b115	b119	b123	b0	b4	b8	b116	b120	b124	b1	b5	b9	b117	b121	b125
chunk0	chunk1	chunk2.....	chunk29	chunk30	chunk31																										
b126	b2	b6	b114	b118	b122																										
b127	b3	b7	b115	b119	b123																										
b0	b4	b8	b116	b120	b124																										
b1	b5	b9	b117	b121	b125																										

Click **Apply** to implement the changes.

To view the settings for a created profile, click its corresponding **View** button in the **Access Profile Table** window, revealing the following window:

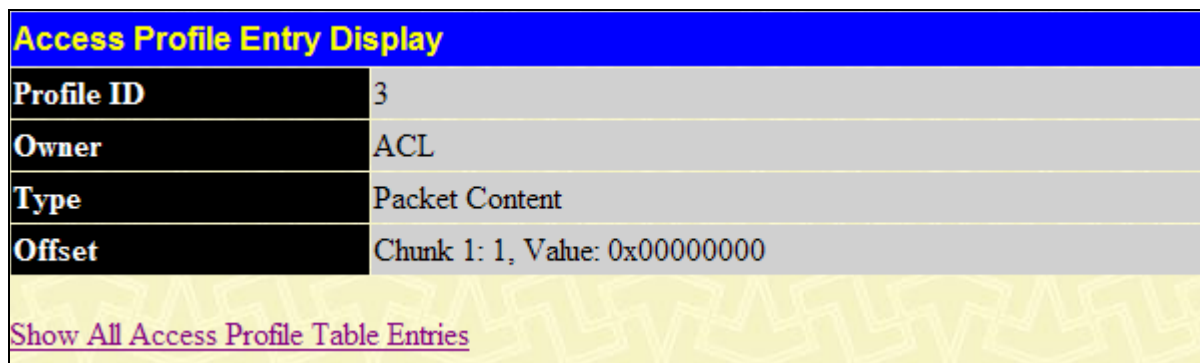


Figure 5 - 10 Access Profile Entry Display window (Packet Content Mask)

To establish the rule for a previously created Access Profile:

To configure the Access Rule for Ethernet, open the **Access Profile Table** window and click **Modify** for an Ethernet entry. This will open the following window:

Add Rule

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	Ethernet	1	View	<input type="button" value="X"/>

Unused Entries: 127

[Show All Access Profile Entries](#)

Figure 5 - 11 Access Rule Table window (Ethernet)

To remove a previously created rule, select it and click the button. To add a new Access Rule, click the **Add Rule** button:

Access Rule Configuration	
Profile ID	2
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Mirror <input type="radio"/> Deny
Access ID (1-128)	1 <input type="checkbox"/> Auto assign <input type="checkbox"/>
Type	Ethernet
Priority (0-7)	<input type="checkbox"/> 0 <input type="checkbox"/> Replace Priority
Replace DSCP (0-63)	<input type="checkbox"/> 0
Group ID (1-4)	
VLAN Name	
Source MAC	
Destination MAC	
802.1p (0-7)	
Ethernet Type (0-FFFF)	
Port	
RX Rate (1-156249)	No Limit <input checked="" type="checkbox"/> 1
Time Range	Range Name <input type="checkbox"/> <input type="button" value="v"/>
Counter	<input type="checkbox"/> State Disabled <input type="button" value="v"/>

[Show All Access Rule Entries](#)

Figure 5 - 12 Access Rule Configuration window (Ethernet)

The following parameters can be configured:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch

	<p>and will be filtered.</p> <p>Select <i>Mirror</i> to specify that packets match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.</p>
Access ID (1-128)	<p>Type in a unique identifier number for this access. This value can be set from 1 to 128.</p> <p>Auto Assign – Checking this field will instruct the Switch to automatically assign an Access ID for the rule being created.</p>
Type	<p>Specifies the type of profile that is being created.</p>
Priority (0-7)	<p>This parameter is to be specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.</p> <p><i>replace priority</i> – Click the corresponding box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.</p> <p>For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.</p>
Replace DSCP (0-63)	<p>Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.</p>
Group ID (1-4)	<p>Enter a mirror group ID.</p>
VLAN Name	<p>Allows the entry of a name for a previously configured VLAN.</p>
Source MAC	<p>Source MAC Address – Enter a MAC Address for the source MAC address.</p>
Destination MAC	<p>Destination MAC Address – Enter a MAC Address mask for the destination MAC address.</p>
802.1p (0-7)	<p>Enter a value from 0-7 to specify that the access profile will apply only to packets with this 802.1p priority value.</p>
Ethernet Type	<p>Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form hex 0x0-0xffff, which means the user may choose any combination of letters and numbers ranging from a-f and from 0-9.</p>
Port	<p>The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the Auto Assign check box MUST be clicked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.</p>
RX Rate (1-156249)	<p>Use this to limit RX bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an RX rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1-156249 or <i>No Limit</i>. The default setting is No Limit.</p>
Time Range	<p>Click the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.</p>
Counter	<p>Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.</p>

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **Access Rule Table** window to view the following window:

Access Rule Display	
Profile ID	2
Access ID	1
Mode	Permit
Type	Ethernet
Priority	-----
Replace DSCP	-----
VLAN Name	default
Source MAC	-----
Destination MAC	-----
802.1p	-----
Ethernet Type	-----
Port	1:2
RX Rate (64Kbps)	No Limit

[Show All Access Rule Entries](#)

Figure 5 - 13 Access Rule Display window (Ethernet)

To configure the Access Rule for IP, open the **Access Profile Table** window and click **Modify** for an IP entry. This will open the following window:

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	IP	1	View	<input type="button" value="X"/>

Unused Entries:127

[Show All Access Profile Entries](#)

Figure 5 - 14 Access Rule Table window (IP)

To create a new rule set for an access profile click the **Add Rule** button. A new window is displayed. To remove a previously created rule, click the corresponding button.

Access Rule Configuration	
Profile ID	1
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Mirror <input type="radio"/> Deny
Access ID (1-128)	1 <input type="checkbox"/> Auto assign <input type="checkbox"/>
Type	IP
Priority (0-7)	<input type="checkbox"/> 0 <input type="checkbox"/> Replace Priority
Replace DSCP (0-63)	<input type="checkbox"/> 0
Group ID (1-4)	
VLAN Name	
Source IP	
Destination IP	
DSCP (0-63)	
Protocol	Protocol id <input type="text"/> user define <input type="text"/>
Port	
RX Rate (1-156249)	No Limit <input checked="" type="checkbox"/> <input type="text"/>
Time Range	Range Name <input type="checkbox"/> <input type="text"/>
Counter	<input type="checkbox"/> State <input type="text"/> Disabled <input type="text"/>

[Show All Access Rule Entries](#)

Figure 5 - 15 Access Rule Configuration window (IP)

Configure the following Access Rule Configuration settings for IP:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> to specify that packets match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from 1 to 128. Auto Assign – Checking this field will instruct the Switch to automatically assign an Access ID for the rule being created.
Type	Specifies the type of profile that is being created.
Priority (0-7)	This parameter is specified if you want to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. <i>Replace priority with</i> – Click the corresponding box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being

	forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Replace DSCP (0-63)	Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.
Group ID (1-4)	Enter a mirror group ID.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address – Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address – Enter an IP Address mask for the destination IP address.
DSCP (0-63)	This field allows the user to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. The user may choose a value between 0 and 63.
Protocol	Specifies that the Switch will examine the Protocol field in each packet and if this field contains the value entered here, apply the appropriate rules. <ul style="list-style-type: none"> • <i>user define</i> – Enter a hexadecimal value in the form <i>0x0-0xfffff</i> that will identify the protocol to be discovered in the packet header.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the Auto Assign check box MUST be clicked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number, and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.
RX Rate	Use this to limit RX bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an RX rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1- 156249 or <i>No Limit</i> . The default setting is No Limit.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **Access Rule Table** window to view the following window:

Access Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	IP
Priority	-----
Replace DSCP	-----
VLAN Name	default
Source IP	-----
Destination IP	-----
DSCP	-----
Protocol	-----
Port	1:3
RX Rate (64Kbps)	No Limit

[Show All Access Rule Entries](#)

Figure 5 - 16 Access Rule Display window (IP)

To configure the Access Rule for IPv6, open the **Access Profile Table** window and click **Modify** for an IPv6 entry. This will open the following window:

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
4	Permit	IPv6	1	View	

Unused Entries:127

[Show All Access Profile Entries](#)

Figure 5 - 17 Access Rule Table (IPv6)

Click **Add Rule** to open the next window to configure the IPv6 entry for an access rule.

Access Rule Configuration	
Profile ID	4
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Mirror <input type="radio"/> Deny
Access ID (1-128)	1 <input type="checkbox"/> Auto assign <input type="checkbox"/>
Type	IPv6
Priority (0-7)	<input type="checkbox"/> <input type="text"/> <input type="checkbox"/> Replace Priority
Group ID (1-4)	<input type="text"/>
Class (0-255)	<input type="text"/>
Flow Label (0-FFFFF)	<input type="text"/>
Source IPv6 Address	<input type="text"/>
Destination IPv6 Address	<input type="text"/>
Port	<input type="text"/>
RX Rate (1-156249)	No Limit <input checked="" type="checkbox"/> <input type="text"/>
Time Range	Range Name <input type="checkbox"/> <input type="text"/>
Counter	<input type="checkbox"/> State Disabled <input type="text"/>

[Show All Access Rule Entries](#)

Figure 5 - 18 Access Rule Configuration window (IPv6)

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> to specify that packets match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.
Access ID (1-128)	Type in a unique identifier number for this access rule. This value can be set from 1 to 128.
Type	Specifies the type of profile that is being created.
Priority (0-7)	This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user. <i>replace priority</i> – Click the corresponding box to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch. For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.
Group ID (1-4)	Enter a mirror group ID.
Class	Entering a value between 0 and 255 will instruct the Switch to examine the class field of the IPv6

	header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field of IPv4.
Flow Label	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by entering the IP address mask, in hex form.
Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by and entering the IP address mask, in hex form.
Port	The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the Auto Assign check box MUST be clicked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The port list is specified by listing the lowest switch number and the beginning port number on that switch, separated by a colon. Then the highest switch number and the highest port number of the range (also separated by a colon) are specified. The beginning and end of the port list range are separated by a dash. For example, 1:3 specifies switch number 1, port 3. 2:4 specifies switch number 2, port 4. 1:3 - 2:4 specifies all of the ports between switch 1, port 3 and switch 2, port 4 – in numerical order. Entering <i>all</i> will denote all ports on the Switch.
RX Rate (1-156249)	Use this to limit RX bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an RX rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1 and 156249, or <i>No Limit</i> . The default setting is <i>No Limit</i> .
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.
Counter	Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **Access Rule Table** window to view the following window:

Access Rule Display	
Profile ID	4
Access ID	1
Mode	Permit
Type	IPv6
Priority	-----
Class	-----
Flow Label	-----
Source IPv6	-----
Destination IPv6	-----
Protocol	-----
Port	1:23
RX Rate (64Kbps)	No Limit

[Show All Access Rule Entries](#)

Figure 5 - 19 Access Rule Display window (IPv6)

The following window is the Access Rule table for Packet Content.

Access Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
3	Permit	Packet Content	1	View	<input type="button" value="X"/>

Unused Entries:127

[Show All Access Profile Entries](#)

Figure 5 - 20 Access Rule Table window (Packet Content Mask)

To remove a previously created rule, select it and click the button. To add a new Access Rule, click the **Add** button:

Access Rule Configuration	
Profile ID	3
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Mirror <input type="radio"/> Deny
Access ID (1-128)	1 <input type="checkbox"/> Auto assign <input type="checkbox"/>
Type	Packet Content
Priority (0-7)	<input type="checkbox"/> <input type="text"/> <input type="checkbox"/> Replace Priority
Group ID (1-4)	<input type="text"/>
Offset	<input type="checkbox"/> Chunk 1 mask <input type="text" value="00000000"/>
	<input type="checkbox"/> Chunk 2 mask <input type="text" value="00000000"/>
	<input type="checkbox"/> Chunk 3 mask <input type="text" value="00000000"/>
	<input type="checkbox"/> Chunk 4 mask <input type="text" value="00000000"/>
Port	<input type="text"/>
RX Rate (1-156249)	No Limit <input checked="" type="checkbox"/> <input type="text" value="1"/>
Time Range	Range Name <input type="checkbox"/> <input type="text"/>
Counter	<input type="checkbox"/> State <input type="text" value="Disabled"/>
Replace DSCP (0-63)	<input type="checkbox"/> <input type="text"/>
<input type="button" value="Apply"/>	
Show All Access Rule Entries	

Figure 5 - 21 Access Rule Configuration window (Packet Content)

To set the Access Rule for the Packet Content Mask, adjust the following parameters and click **Apply**.

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered. Select <i>Mirror</i> to specify that packets that match the access profile are mirrored to a port defined in the Port Mirroring window. Port Mirroring must be enabled and a target port must be set.
Access ID (1-128)	Type in a unique identifier number for this access. This value can be set from 1 to 128. <ul style="list-style-type: none"> Auto Assign – Ticking this check box will instruct the Switch to automatically assign an Access ID for the rule being created.
Type	Specifies the type of profile that is being created.

Priority (0-7)	<p>This parameter is specified to re-write the 802.1p default priority previously set in the Switch, which is used to determine the CoS queue to which packets are forwarded to. Once this field is specified, packets accepted by the Switch that match this priority are forwarded to the CoS queue specified previously by the user.</p> <p>Replace priority with – Tick the corresponding check box if you want to re-write the 802.1p default priority of a packet to the value entered in the Priority field, which meets the criteria specified previously in this command, before forwarding it on to the specified CoS queue. Otherwise, a packet will have its incoming 802.1p user priority re-written to its original value before being forwarded by the Switch.</p> <p>For more information on priority queues, CoS queues and mapping for 802.1p, see the QoS section of this manual.</p>
Group ID (1-4)	Enter a mirror group ID.
Offset	<p>This field will instruct the Switch to mask the packet header beginning with the offset value specified:</p> <ul style="list-style-type: none"> • Chunk 1 – Enter a value in hex form to mask the packet from the beginning of the packet to the first chunk. • Chunk 2 – Enter a value in hex form to mask the packet from the end of the first chunk to the end of the second chunk. • Chunk 3 – Enter a value in hex form to mask the packet from the end of the second chunk to the end of the third chunk. • Chunk 4 – Enter a value in hex form to mask the packet from the end of the third chunk to the end of the fourth chunk.
Port	<p>The Access Rule may be configured on a per-port basis by entering the port number of the switch in the switch stack into this field. When a range of ports is to be configured, the Auto Assign check box MUST be ticked in the Access ID field of this window. If not, the user will be presented with an error message and the access rule will not be configured. The beginning and end of the port list range are separated by a dash. Entering <i>all</i> will denote all ports on the Switch.</p>
RX Rate (1-156249)	<p>Use this to limit RX bandwidth for the profile being configured. This rate is implemented using the following equation: 1 value = 64kbit/sec. (ex. If the user selects an RX rate of 10 then the ingress rate is 640kbit/sec.) The user may select a value between 1 and 156249 or <i>No Limit</i>. The default setting is <i>No Limit</i>.</p>
Time Range	<p>Tick the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.</p>
Counter	<p>Tick the check box and use the pull-down menu to employ the Counter that will count the packets identified with this rule. Users must note that if the Counter is employed in the ACL Flow Meter function, the Counter will automatically be disabled here, regardless of this setting.</p>
Replace DSCP (0-63)	<p>Select this option to instruct the Switch to replace the DSCP value (in a packet that meets the selected criteria) with the value entered in the adjacent field.</p>

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **Access Rule Table** window to view the following window:

Access Rule Display	
Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content
Priority	-----
Replace DSCP	-----
Offset	Chunk 1: 10, Value: 0x00000000
Port	1:4
RX Rate (64Kbps)	No Limit
Show All Access Rule Entries	

Figure 5 - 22 Access Rule Display window (Packet Content)



NOTE: When using the ACL Mirror function, ensure that the Port Mirroring function is enabled and a target mirror port is set.

ACL Flow Meter

Before configuring the ACL Flow Meter, here is a list of acronyms and terms users will need to know.

trTCM – Two Rate Three Color Marker. This, along with the srTCM, are two methods available on the switch for metering and marking packet flow. The trTCM meters and IP flow and marks it as a color based on the flow’s surpassing of two rates, the CIR and the PIR.

CIR – Committed Information Rate. Common to both the trTCM and the srTCM, the CIR is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. For the trTCM, the packet flow is marked green if it doesn’t exceed the CIR and yellow if it does. The configured rate of the CIR must not exceed that of the PIR. The CIR can also be configured for unexpected packet bursts using the CBS and PBS fields.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

PIR – Peak Information Rate. This rate is measured in bytes of IP packets. IP packet bytes are measured by taking the size of the IP header but not the link specific headers. If the packet flow exceeds the PIR, that packet flow is marked red. The PIR must be configured to be equal or more than that of the CIR.

PBS – Peak Burst Size. Measured in bytes, the PBS is associated with the PIR and is used to identify packets that exceed the normal boundaries of packet size. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.

srTCM – Single Rate Three Color Marker. This, along with the trTCM, are two methods available on the switch for metering and marking packet flow. The srTCM marks its IP packet flow based on the configured CBS and EBS. A packet flow that does not reach the CBS is marked green, if it exceeds the CBS but not the EBS its marked yellow, and if it exceeds the EBS its marked red.

CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.

EBS – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS.

DSCP – Differentiated Services Code Point. The part of the packet header where the color will be added. Users may change the DSCP field of incoming packets.

The ACL Flow Meter function will allow users to color code IP packet flows based on the rate of incoming packets. Users have two types of Flow metering to choose from, trTCM and srTCM, as explained previously. When a packet flow is placed in a color code, the user can choose what to do with packets that have exceeded that color-coded rate.

Green – When an IP flow is in the green mode, its configurable parameters can be set in the Conform field, where the packets can have their DSCP field changed. This is an acceptable flow rate for the ACL Flow Meter function.

Yellow – When an IP flow is in the yellow mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Red – When an IP flow is in the red mode, its configurable parameters can be set in the Exceed field. Users may choose to either **Permit** or **Drop** exceeded packets. Users may also choose to change the DSCP field of the packets.

Users may also choose to count exceeded packets by clicking the **Counter** check box. If the counter is enabled, the counter setting in the access profile will be disabled. Users may only enable two counters for one flow meter at any given time.

To view this window, click **ACL > ACL Flow Meter**, as shown below.

Figure 5 - 23 ACL Flow Meter window

The following fields may be configured:

Parameter	Description
Profile ID	The pre-configured Profile ID for which to configure the Flow Metering parameters.
Access ID	The pre-configured Access ID for which to configure the Flow Metering parameters.

The previous window allows users to view the ACL profile and rule that is utilizing the ACL Flow Meter function, and the mode associated with that profile and rule. Users may search a particular Profile ID or Access ID by entering that value into one of the available fields and clicking Search. The result should be displayed in the table. Click Show All to show all ACL Profiles and Access IDs that are utilizing the ACL Flow Metering function. To add an ACL Flow Meter configuration for an Access Profile and Rule, click the **Add** button, which will display the following window for users to configure.

ACL Flow Meter Configuration			
Profile ID (1-6)	<input type="text"/>		
Access ID (1-128)	<input type="text"/>		
Mode	<input checked="" type="radio"/> trTCM	CIR (0-156249)64Kbps	<input type="text"/>
		PIR (0-156249)64Kbps	<input type="text"/>
		<input type="checkbox"/> CBS (0-16384)Kbyte	<input type="text"/>
		<input type="checkbox"/> PBS (0-16384)Kbyte	<input type="text"/>
	<input type="radio"/> srTCM	CIR (0-156249)64Kbps	<input type="text"/>
		CBS (0-16384)Kbyte	<input type="text"/>
		EBS (0-16384)Kbyte	<input type="text"/>
Action	Conform	<input type="checkbox"/> Replace DSCP (0-63)	<input type="text"/>
		<input type="checkbox"/> Counter	
	Exceed <input checked="" type="radio"/> Permit <input type="radio"/> Drop		
	<input type="radio"/> Replace DSCP (0-63) <input type="text"/>	<input type="checkbox"/> Counter	
	Violate <input checked="" type="radio"/> Permit <input type="radio"/> Drop		
	<input type="radio"/> Replace DSCP (0-63) <input type="text"/>	<input type="checkbox"/> Counter	

[Show All ACL Flow Meter Entries](#)

Figure 5 - 24 ACL Flow Meter Configuration - Add window

The following fields may be configured:

Parameter	Description
Profile ID (1-6)	Enter the pre-configured Profile ID for which to configure the ACL Flow Metering parameters.
Access ID (1-128)	Enter the pre-configured Access ID for which to configure the ACL Flow Metering parameters.
Mode	In this field the user may choose they type of mode to be employed for the ACL Flow Meter function, and then the limits of the packet flow.
trTCM	<p>Choosing this field will allow users to employ the Two Rate Three Color Mode and set the following parameters to determine the color rate of the IP packet flow.</p> <p>CIR – The Committed Information Rate can be set between 0 and 156249. IP flow rates at or below this level will be considered green. IP flow rates that exceed this rate but not the PIR rate are considered yellow.</p> <p>PIR – The Peak information Rate. IP flow rates that exceed this setting will be considered as red. This field must be set at an equal or higher value than the CIR.</p> <p>CBS – The Committed Burst Size. Used to gauge packets that are larger than the normal IP packets. Click the check box to employ the CBS. This field does not have to be set for this feature to function properly but is to be used in conjunction with the CIR setting. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow.</p> <p>PBS - The Peak Burst Size. This optional field is to be used in conjunction with the PIR. The PBS should be configured to accept the biggest IP packet that is expected in the IP flow.</p>
srTCM	Choosing this field will allow users to employ the Single Rate Three Color Mode and set the

	<p>following parameters to determine the color rate of the IP packet flow.</p> <p>CIR – The Committed Information Rate can be set between 0 and 156249. The color rates are based on the following two fields which are used in conjunction with the CIR.</p> <p>CBS – Committed Burst Size. Measured in bytes, the CBS is associated with the CIR and is used to identify packets that exceed the normal boundaries of packet size. The CBS should be configured to accept the biggest IP packet that is expected in the IP flow. Packet flows that are lower than this configured value are marked green. Packet flows that exceed this value but are less than the EBS value are marked yellow.</p> <p>EBS – Excess Burst Size. Measured in bytes, the EBS is associated with the CIR and is used to identify packets that exceed the boundaries of the CBS packet size. The EBS is to be configured for an equal or larger rate than the CBS. Packet flows that exceed this value are marked as red.</p>
Action	This field is used to determine the course of action when a packet flow has been marked as a color, based on the following fields.
Conform	This field denotes the green packet flow. Green packet flows may have their DSCP field rewritten to a value stated in this field. Users may also choose to count green packets by ticking the Counter check box.
Exceed	This field denotes the yellow packet flow. Yellow packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. Users may also choose to count yellow packets by ticking the Counter check box.
Violate	This field denotes the red packet flow. Red packet flows may have excess packets permitted through or dropped. Users may replace the DSCP field of these packets by checking its radio button and entering a new DSCP value in the allotted field. Users may also choose to count yellow packets by ticking the Counter check box.

Click **Apply** to save the changes. To view the ACL Flow Meter configurations for a particular Profile and Access ID, click its corresponding **View** button, as seen in the **ACL Flow Meter Table** window that will display the following read-only window.

ACL Flow Meter Display		
Profile ID	1	
Access ID	1	
Mode	trTCM	CIR: 1 (64Kbps)
		PIR: 1 (64Kbps)
		CBS: 1 (Kbyte)
		PBS: 1 (Kbyte)
Action	Conform: Permit	Replace DSCP: -----
		Counter: Disabled
	Exceed: Permit	Replace DSCP: -----
		Counter: Enabled
	Violate: Permit	Replace DSCP: -----
		Counter: Disabled
Show All ACL Flow Meter Entries		

Figure 5 - 25 ACL Flow Meter Configuration - View window

CPU Interface Filtering

Due to a chipset limitation and needed extra switch security, the xStack® DGS-3400 Series switch incorporates CPU Interface filtering. This added feature increases the running security of the Switch by enabling the user to create a list of access rules for packets destined for the Switch's CPU interface. Employed similarly to the Access Profile feature previously mentioned, CPU interface filtering examines Ethernet, IP and Packet Content Mask packet headers destined for the CPU and will either forward them or filter them, based on the user's implementation. As an added feature for the CPU Filtering, the xStack® DGS-3400 Series switch allows the CPU filtering mechanism to be enabled or disabled globally, permitting the user to create various lists of rules without immediately enabling them.

Creating an access profile for the CPU is divided into two basic parts. The first is to specify which part or parts of a frame the Switch will examine, such as the MAC source address or the IP destination address. The second part is entering the criteria the Switch will use to determine what to do with the frame. The entire process is described below.

CPU Interface Filtering State

In the following window, the user may globally enable or disable the CPU Interface Filtering mechanism by using the pull-down menu to change the running state. Choose **Enabled** to enable CPU packets to be scrutinized by the Switch and **Disabled** to disallow this scrutiny.

To view this window, click **ACL > CPU Interface Filtering > CPU Interface Filtering State**, as shown below.

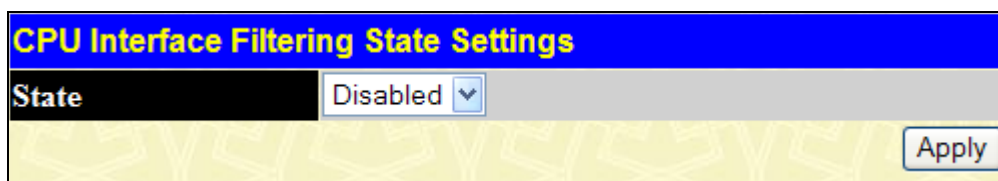


Figure 5 - 26 CPU Interface Filtering State Settings window

CPU Interface Filtering Table

This window displays the CPU Access Profile Table entries created on the Switch.

To view this window, click **ACL > CPU Interface Filtering > CPU Interface Filtering Table**, as shown below.

Profile ID	Type	Access Rule	Display	Delete
1	Ethernet	Modify	View	X
2	IP	Modify	View	X
3	Packet Content	Modify	View	X
4	IPv6	Modify	View	X

Figure 5 - 27 CPU Interface Filtering Table window

To add an entry to this window, click the **Add Profile** button. This will open the **CPU Interface Filtering Configuration** window, as shown below. To remove all CPU Interface Filtering Table entries, click the **Clear All** button. There are four **Access Profile Configuration** windows; one for Ethernet (or MAC address-based) profile configuration, one for IP address-based profile configuration, one for the Packet Content Mask and one for IPv6. You can switch between the four **Access Profile Configuration** windows by using the Type drop-down menu. The window shown below is the **Ethernet CPU Interface Filtering Configuration** window.

Profile ID (1-5)	1
Type	Ethernet
VLAN	<input type="checkbox"/>
Source MAC	<input type="checkbox"/> 00-00-00-00-00-00
Destination MAC	<input type="checkbox"/> 00-00-00-00-00-00
Ethernet Type	<input type="checkbox"/>

[Apply](#)

[Show All CPU Interface Filtering Table Entries](#)

Figure 5 - 28 CPU Interface Filtering Configuration window (Ethernet)

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 to 5.
Type	Select profile based on Ethernet (MAC Address), IP address, IPv6 address or packet content mask. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header.

VLAN	Selecting this option instructs the Switch to examine the VLAN identifier of each packet header and use this as the full or partial criterion for forwarding.
Source MAC	Source MAC Mask - Enter a MAC address mask for the source MAC address.
Destination MAC	Destination MAC Mask - Enter a MAC address mask for the destination MAC address.
Ethernet type	Selecting this option instructs the Switch to examine the Ethernet type value in each frame's header.

Click **Apply** to set this entry in the Switch's memory.

To view the settings of a previously correctly created profile, click **View** in the **CPU Interface Filtering Table** window to view the following window:

CPU Interface Filtering Entry Display	
Profile ID	1
Type	Ethernet
VLAN	Enabled
Source MAC	-----
Destination MAC	-----
Ethernet Type	-----
Show All CPU Interface Filtering Table Entries	

Figure 5 - 29 CPU Interface Filtering Entry Display window (Ethernet)

The page shown below is the CPU Interface Filtering Profile Configuration for IP page.

CPU Interface Filtering Configuration			
Profile ID (1-5)	<input type="text" value="1"/>		
Type	<input type="text" value="IP"/>		
VLAN	<input type="checkbox"/>		
Source IP Mask	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	
Destination IP Mask	<input type="checkbox"/>	<input type="text" value="0.0.0.0"/>	
DSCP	<input type="checkbox"/>		
Protocol	<input type="checkbox"/>	<input checked="" type="radio"/> ICMP	<input type="checkbox"/> type <input type="checkbox"/> code
		<input type="radio"/> IGMP	<input type="checkbox"/> type
		<input type="radio"/> TCP	<input type="checkbox"/> src port mask <input type="text" value="0000"/> <input type="checkbox"/> dst port mask <input type="text" value="0000"/> <input type="checkbox"/> flag bit <input type="checkbox"/> urg <input type="checkbox"/> ack <input type="checkbox"/> psh <input type="checkbox"/> rst <input type="checkbox"/> syn <input type="checkbox"/> fin
		<input type="radio"/> UDP	<input type="checkbox"/> src port mask <input type="text" value="0000"/> <input type="checkbox"/> dst port mask <input type="text" value="0000"/>
		<input type="radio"/> Protocol id <input type="text" value="00"/>	<input type="checkbox"/> user mask <input type="text" value="00000000"/>
<input type="button" value="Apply"/>			
Show All CPU Interface Filtering Table Entries			

Figure 5 - 30 CPU Interface Filtering Configuration window (IP)

The following parameters may be configured for the IP CPU filter.

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 to 5.
Type	Select profile based on Ethernet (MAC Address), IP address, IPv6 address or Packet Content Mask. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header.
VLAN	Selecting this option instructs the Switch to examine the VLAN part of each packet header and use this as the, or part of the criterion for forwarding.
Source IP Mask	Enter an IP address mask for the source IP address.
Destination IP Mask	Enter an IP address mask for the destination IP address.
DSCP	Selecting this option instructs the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding.
Protocol	Selecting this option instructs the Switch to examine the protocol type value in each frame's header. You must then specify what protocol(s) to include according to the following guidelines: Select <i>ICMP</i> to instruct the Switch to examine the Internet Control Message Protocol (ICMP) field in each frame's header. <ul style="list-style-type: none"> Select <i>Type</i> to further specify that the access profile will apply an ICMP type value,

or specify *Code* to further specify that the access profile will apply an ICMP code value.

Select *IGMP* to instruct the Switch to examine the Internet Group Management Protocol (IGMP) field in each frame's header.

- Select *Type* to further specify that the access profile will apply an IGMP type value.

Select *TCP* to use the TCP port number contained in an incoming packet as the forwarding criterion. Selecting TCP requires a source port mask and/or a destination port mask is to be specified. The user may also identify which flag bits to filter. Flag bits are parts of a packet that determine what to do with the packet. The user may filter packets by filtering certain flag bits within the packets, by checking the boxes corresponding to the flag bits of the TCP field. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize), fin (finish).

- src port mask* – Specify a TCP port mask for the source port in hex form (hex 0x0-0xffff), which you wish to filter.
- dst port mask* – Specify a TCP port mask for the destination port in hex form (hex 0x0-0xffff) which you wish to filter.

Select *UDP* to use the UDP port number contained in an incoming packet as the forwarding criterion. Selecting UDP requires that you specify a source port mask and/or a destination port mask.

- src port mask* – Specify a UDP port mask for the source port in hex form (hex 0x0-0xffff).
- dst port mask* – Specify a UDP port mask for the destination port in hex form (hex 0x0-0xffff).

Protocol id – Enter a value defining the protocol ID in the packet header to mask. Specify the protocol ID mask in hex form (hex 0x0-0xff).

Click **Apply** to set this entry in the Switch's memory.

To view the settings of a previously correctly created profile, click **View** in the **CPU Interface Filtering Table** window to view the following screen:

CPU Interface Filtering Entry Display	
Profile ID	2
Type	IP
VLAN	Enabled
Source IP Mask	-----
Destination IP Mask	-----
DSCP	-----
Protocol	-----
Show All CPU Interface Filtering Table Entries	

Figure 5 - 31 CPU Interface Filtering Entry Display window (IP)

The page shown below is the CPU Interface Filtering Profile Configuration for IPv6 page.

Figure 5 - 32 CPU Interface Filtering Configuration window (IPv6)

The following parameters may be configured for the IP CPU filter.

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 to 5.
Type	Select profile based on Ethernet (MAC Address), IP address, IPv6 address or Packet Content Mask. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header.
Class	Checking this field will instruct the Switch to examine the <i>class</i> field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
Flow Label	Checking this field will instruct the Switch to examine the <i>flow label</i> field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Mask	The user may specify an IP address mask for the source IPv6 address by checking the corresponding box and entering the IP address mask.
Destination IPv6 Mask	The user may specify an IP address mask for the destination IPv6 address by checking the corresponding box and entering the IP address mask.

Click **Apply** to set this entry in the Switch's memory.

To view the settings of a previously correctly created profile, click **View** in the **CPU Interface Filtering Table** window to view the following screen:

CPU Interface Filtering Entry Display	
Profile ID	4
Type	IPv6
Class	Enabled
Flow Label	-----
Source IPv6 Mask	-----
Destination IPv6 Mask	-----
Show All CPU Interface Filtering Table Entries	

Figure 5 - 33 CPU Interface Filtering Entry Display window (IPv6)

The window shown below is the Packet Content Mask configuration window.

CPU Interface Filtering Configuration		
Profile ID (1-5)	1	
Type	Packet Content	
Offset	<input type="checkbox"/> value (0-15)	mask 00000000
		mask 00000000
		mask 00000000
		mask 00000000
	<input type="checkbox"/> value (16-31)	mask 00000000
		mask 00000000
		mask 00000000
		mask 00000000
	<input type="checkbox"/> value (32-47)	mask 00000000
		mask 00000000
		mask 00000000
		mask 00000000
	<input type="checkbox"/> value (48-63)	mask 00000000
		mask 00000000
		mask 00000000
		mask 00000000
	<input type="checkbox"/> value (64-79)	mask 00000000
		mask 00000000
		mask 00000000
		mask 00000000
<input type="button" value="Apply"/>		
Show All CPU Interface Filtering Table Entries		

Figure 5 - 34 CPU Interface Filtering Configuration window (Packet Content)

This screen will aid the user in configuring the Switch to mask packet headers beginning with the offset value specified. The following fields are used to configure the Packet Content Mask:

Parameter	Description
Profile ID (1-5)	Type in a unique identifier number for this profile set. This value can be set from 1 to 5.
Type	Select profile based on Ethernet (MAC Address), IP address, IPv6 address or packet content mask. This will change the menu according to the requirements for the type of profile. Select <i>Ethernet</i> to instruct the Switch to examine the layer 2 part of each packet header. Select <i>IP</i> to instruct the Switch to examine the IP address in each frame's header. Select <i>Packet Content Mask</i> to specify a mask to hide the content of the packet header. Select <i>IPv6</i> to instruct the Switch to examine the IPv6 address in each frame's header.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: <ul style="list-style-type: none"> <i>value (0-15)</i> – Enter a value in hex form to mask the packet from the beginning of the

	<p>packet to the 15th byte.</p> <ul style="list-style-type: none"> • <i>value (16-31)</i> – Enter a value in hex form to mask the packet from byte 16 to byte 31. • <i>value (32-47)</i> – Enter a value in hex form to mask the packet from byte 32 to byte 47. • <i>value (48-63)</i> – Enter a value in hex form to mask the packet from byte 48 to byte 63. • <i>value (64-79)</i> – Enter a value in hex form to mask the packet from byte 64 to byte 79.
--	--

Click **Apply** to implement changes made.

To view the settings of a previously correctly created profile, click **View** in the **CPU Interface Filtering Table** window to view the following window:

CPU Interface Filtering Entry Display	
Profile ID	3
Type	Packet Content
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	-----
Offset 32-47	-----
Offset 64-79	-----
Show All CPU Interface Filtering Table Entries	

Figure 5 - 35 CPU Interface Filtering Display window (Packet Content)

To establish the rule for a previously created CPU Access Profile:

<input type="button" value="Add Profile"/>		<input type="button" value="Clear All"/>		
Total Rule Entries:0				
CPU Interface Filtering Table				
Profile ID	Type	Access Rule	Display	Delete
1	Ethernet	<input type="button" value="Modify"/>	<input type="button" value="View"/>	<input type="button" value="X"/>
2	IP	<input type="button" value="Modify"/>	<input type="button" value="View"/>	<input type="button" value="X"/>
3	Packet Content	<input type="button" value="Modify"/>	<input type="button" value="View"/>	<input type="button" value="X"/>
4	IPv6	<input type="button" value="Modify"/>	<input type="button" value="View"/>	<input type="button" value="X"/>

Figure 5 - 36 CPU Interface Filtering Table window

In this window, the user may add a rule to a previously created CPU access profile by clicking the corresponding **Modify** button of the entry to configure, Ethernet, IP, IPv6 or Packet Content. Each entry will open a new and unique window, as shown in the examples below.

Add Rule

CPU Interface Filtering Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
1	Permit	Ethernet	1	View	

[Show All CPU Interface Filtering Entries](#)

Figure 5 - 37 CPU Interface Filtering Table (Ethernet)

To create a new rule set for an access profile click the **Add Rule** button. A new window is displayed. To remove a previously created rule, click the corresponding button. The following window is used for the Ethernet Rule configuration.

CPU Interface Filtering Rule Configuration	
Profile ID	1
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny
Access ID (1-100)	<input type="text" value="1"/>
Type	Ethernet
VLAN Name	<input type="text"/>
Source MAC	<input type="text" value="00-00-00-00-00-00"/>
Destination MAC	<input type="text" value="00-00-00-00-00-00"/>
Ethernet Type	<input type="text" value="0000"/>
Port	<input type="text"/>
Time Range	Range Name <input type="checkbox"/> <input type="text"/>

[Apply](#)

[Show All CPU Interface Filtering Rule Entries](#)

Figure 5 - 38 CPU Interface Filtering Rule Configuration window (Ethernet)

The following parameters can be configured.

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access and priority. This value can be set from 1 to 100.
Type	Specifies the type of profile that is being created.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source MAC	Source MAC Address – Enter a MAC Address for the source MAC address.
Destination	Destination MAC Address – Enter a MAC Address mask for the destination MAC address.

MAC	
Ethernet Type	Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value (hex 0x0-0xffff) in the packet header. The Ethernet type value may be set in the form: hex 0x0-0xffff, which means the user may choose a combination of letters and numbers ranging from a-f and from 0-9.
Port	Enter the port or range of ports.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **CPU Interface Filtering Rule Table** window to view the following window:

CPU Interface Filtering Rule Display	
Profile ID	1
Access ID	1
Mode	Permit
Type	Ethernet
VLAN Name	default
Source MAC	-----
Destination MAC	-----
Ethernet Type	-----
Port	1:1
Show All CPU Interface Filtering Rule Entries	

Figure 5 - 39 CPU Interface Filtering Rule Display window (Ethernet)

The following window is the CPU Interface Filtering Rule Table for IP.

Add Rule					
CPU Interface Filtering Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
2	Permit	IP	1	View	<input type="button" value="X"/>
Show All CPU Interface Filtering Entries					

Figure 5 - 40 CPU Interface Filtering Rule Table window (IP)

To create a new rule set for an access profile click the **Add Rule** button. A new window is displayed. To remove a previously created rule, click the corresponding button. The following window is used for the IP Rule configuration.

CPU Interface Filtering Rule Configuration

Profile ID 2

Mode Permit Deny

Access ID (1-100) 1

Type IP

VLAN Name

Source IP 0.0.0.0

Destination IP 0.0.0.0

DSCP (0-63) 0

Port

Time Range Range Name

[Show All CPU Interface Filtering Rule Entries](#)

Figure 5 - 41 CPU Interface Filtering Rule Configuration window (IP)

Configure the following Access Rule Configuration settings for IP:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 to 100.
Type	Specifies the type of profile that is being created.
VLAN Name	Allows the entry of a name for a previously configured VLAN.
Source IP	Source IP Address – Enter an IP Address mask for the source IP address.
Destination IP	Destination IP Address – Enter an IP Address mask for the destination IP address.
DSCP (0-63)	This field allows the user to enter a DSCP value in the space provided, which will instruct the Switch to examine the DiffServ Code part of each packet header and use this as the, or part of the criterion for forwarding. The user may choose a value between 0 and 63.
Port	Enter a port or range of ports.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **CPU Interface Filtering Rule Table** to view the following window:

CPU Interface Filtering Rule Display	
Profile ID	2
Access ID	1
Mode	Permit
Type	IP
VLAN Name	default
Source IP	-----
Destination IP	-----
DSCP	-----
Protocol	-----
Port	1:2

[Show All CPU Interface Filtering Rule Entries](#)

Figure 5 - 42 CPU Interface Filtering Rule Display window (IP)

The following window is the CPU Interface Filtering Rule Table for IPv6.

Add Rule

CPU Interface Filtering Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
4	Permit	IPv6	1	View	<input type="button" value="X"/>

[Show All CPU Interface Filtering Entries](#)

Figure 5 - 43 CPU Interface Filtering Rule Table window (IPv6)

To create a new rule set for an access profile click the **Add Rule** button. A new window is displayed. To remove a previously created rule, click the corresponding button. The following window is used for the IP Rule configuration.

Figure 5 - 44 CPU Interface Filtering Rule Configuration window (IPv6)

Configure the following Access Rule Configuration settings for IPv6:

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID (1-100)	Type in a unique identifier number for this access. This value can be set from 1 to 100.
Type	Specifies the type of profile that is being created.
Class (0-255)	Entering a value between 0 and 255 will instruct the Switch to examine the class field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field of IPv4.
Flow Label	Configuring this field, in hex form, will instruct the Switch to examine the flow label field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.
Source IPv6 Address	The user may specify an IP address mask for the source IPv6 address by entering the IP address mask, in hex form.
Destination IPv6 Address	The user may specify an IP address mask for the destination IPv6 address by and entering the IP address mask, in hex form.
Port	Enter a port or range of ports.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **CPU Interface Filtering Rule Table** to view the following window:

CPU Interface Filtering Rule Display	
Profile ID	4
Access ID	1
Mode	Permit
Type	IPv6
Class	0
Flow Label	-----
Source IPv6	-----
Destination IPv6	-----
Port	1:4

[Show All CPU Interface Filtering Rule Entries](#)

Figure 5 - 45 CPU Interface Filtering Rule Display window (IPv6)

The following window is the CPU Interface Filtering Rule Table for Packet Content.

CPU Interface Filtering Rule Table					
Profile ID	Mode	Type	Access ID	Display	Delete
3	Permit	Packet Content	1	View	<input type="button" value="X"/>

[Show All CPU Interface Filtering Entries](#)

Figure 5 - 46 CPU Interface Filtering Rule Table window (Packet Content)

To remove a previously created rule, select it and click the  button. To add a new Access Rule, click the **Add Rule** button:

CPU Interface Filtering Rule Configuration		
Profile ID	3	
Mode	<input checked="" type="radio"/> Permit <input type="radio"/> Deny	
Access ID (1-100)	<input type="text" value="1"/>	
Type	Packet Content	
Offset	<input type="checkbox"/> value (0-15)	mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
	<input type="checkbox"/> value (16-31)	mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
	<input type="checkbox"/> value (32-47)	mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
	<input type="checkbox"/> value (48-63)	mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
	<input type="checkbox"/> value (64-79)	mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
		mask <input type="text" value="00000000"/>
Port	<input type="text"/>	
Time Range	Range Name <input type="checkbox"/> <input type="text"/>	
<input type="button" value="Apply"/>		
Show All CPU Interface Filtering Rule Entries		

Figure 5 - 47 CPU Interface Filtering Rule Configuration window (Packet Content)

The following parameters can be configured.

Parameter	Description
Profile ID	This is the identifier number for this profile set.
Mode	Select <i>Permit</i> to specify that the packets that match the access profile are forwarded by the Switch, according to any additional rule added (see below). Select <i>Deny</i> to specify that packets that match the access profile are not forwarded by the Switch and will be filtered.
Access ID	Type in a unique identifier number for this access. This value can be set from 1 - 100.
Type	Specifies the type of profile that is being created.
Offset	This field will instruct the Switch to mask the packet header beginning with the offset value specified: <i>value (0-15)</i> – Enter a value in hex form to mask the packet from the beginning of the packet to the 15th byte. <i>value (16-31)</i> – Enter a value in hex form to mask the packet from byte 16 to byte 31. <i>value (32-47)</i> – Enter a value in hex form to mask the packet from byte 32 to byte 47. <i>value (48-63)</i> – Enter a value in hex form to mask the packet from byte 48 to byte 63. <i>value (64-79)</i> – Enter a value in hex form to mask the packet from byte 64 to byte 79.
Port	Type in the port or range of ports that will be affected.
Time Range	Click the check box and enter the name of the Time Range settings that has been previously configured in the Time Range Settings window. This will set specific times when this access rule will be implemented on the Switch.

Click **Apply** to implement the changes.

To view the settings of a previously correctly configured rule, click **View** in the **CPU Interface Filtering Rule Table** window to view the following window:

CPU Interface Filtering Rule Display	
Profile ID	3
Access ID	1
Mode	Permit
Type	Packet Content
Offset 0-15	0x00000000 0x00000000 0x00000000 0x00000000
Offset 16-31	-----
Offset 32-47	-----
Offset 48-63	-----
Offset 64-79	-----
Port	1:3
Show All CPU Interface Filtering Rule Entries	

Figure 5 - 48 CPU Interface Filtering Rule Display window (Packet Content)

Security

Authorization Attributes State Settings

Traffic Control

Port Security

IP-MAC-Port Binding

802.1X

Web-based Access Control (WAC)

Trust Host

BPDU Attack Protection Settings

ARP Spoofing Prevention Settings

Access Authentication Control

MAC-based Access Control (MAC)

Safeguard Engine

Traffic Segmentation

Secure Socket Layer (SSL)

Secure Shell (SSH)

Compound Authentication

Japanese Web-based Access Control (JWAC)

Authorization Attributes State Settings

This window is used to Enable or Disable the Authorization Network State Settings.

To view this window, click **Security > Authorization Attributes State Settings**, as shown below.

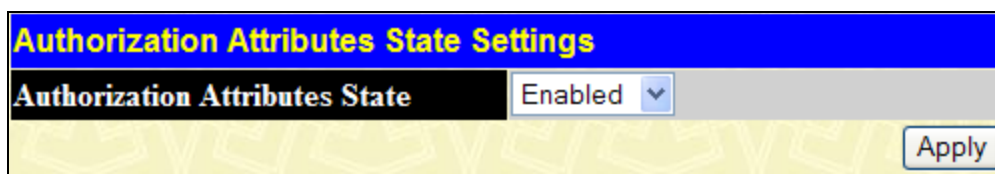


Figure 6 - 1 Authorization Attributes State Settings Window

Use the pull-down menu to enable or disable the function, and click **Apply** to implement the changes.

Traffic Control

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase do to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the **Drop** option of the **Action** field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the Countdown field.

The screenshot shows the 'Traffic Control Settings' window. It includes sections for 'Traffic Control Recover Settings', 'Traffic Control Global Settings', and 'Traffic Control Settings'. The 'Traffic Control Settings' section contains a table for configuring traffic control for each port (Unit 1).

Unit	From	To	Broadcast	Multicast	Unicast	Action	Threshold (0-255000)	Countdown (0 or 3-30)	Time Interval (5-600)	Apply
1	Port 1	Port 1	Disabled	Disabled	Disabled	Drop	131072	0	5	Apply

Port	Broadcast	Multicast	Unicast	Action	Threshold	Countdown	Time Interval	Forever
1	Disabled	Disabled	Disabled	Drop	131072	0	5	
2	Disabled	Disabled	Disabled	Drop	131072	0	5	
3	Disabled	Disabled	Disabled	Drop	131072	0	5	
4	Disabled	Disabled	Disabled	Drop	131072	0	5	
5	Disabled	Disabled	Disabled	Drop	131072	0	5	
6	Disabled	Disabled	Disabled	Drop	131072	0	5	
7	Disabled	Disabled	Disabled	Drop	131072	0	5	
8	Disabled	Disabled	Disabled	Drop	131072	0	5	
9	Disabled	Disabled	Disabled	Drop	131072	0	5	
10	Disabled	Disabled	Disabled	Drop	131072	0	5	
11	Disabled	Disabled	Disabled	Drop	131072	0	5	
12	Disabled	Disabled	Disabled	Drop	131072	0	5	
13	Disabled	Disabled	Disabled	Drop	131072	0	5	
14	Disabled	Disabled	Disabled	Drop	131072	0	5	
15	Disabled	Disabled	Disabled	Drop	131072	0	5	
16	Disabled	Disabled	Disabled	Drop	131072	0	5	
17	Disabled	Disabled	Disabled	Drop	131072	0	5	
18	Disabled	Disabled	Disabled	Drop	131072	0	5	
19	Disabled	Disabled	Disabled	Drop	131072	0	5	
20	Disabled	Disabled	Disabled	Drop	131072	0	5	
21	Disabled	Disabled	Disabled	Drop	131072	0	5	
22	Disabled	Disabled	Disabled	Drop	131072	0	5	
23	Disabled	Disabled	Disabled	Drop	131072	0	5	
24	Disabled	Disabled	Disabled	Drop	131072	0	5	

Figure 6 - 2 Traffic Control Settings window

If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, the only method of recovering this port is to manually recoup it using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the **Shutdown** option of the **Action** field in the window below.

Use the **Traffic Control** window to enable or disable storm control and adjust the threshold for multicast and broadcast storms, as well as DLF (Destination Look Up Failure).

To view the following window, click **Security > Traffic Control**, as shown above:

To configure **Traffic Control**, enable or disable the **Broadcast Storm**, **Multicast Storm** and **DLF** using their corresponding pull-down menus. Click **Apply** to implement changes made.

Parameter	Description
Traffic Control Recover	
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From / To	Select the ports to be shutdown.
Traffic Trap Configuration	
Traffic Control Trap	Enable sending of Storm Trap messages when the type of action taken by the Traffic Control function in handling a Traffic Storm is one of the following: <ul style="list-style-type: none"> <i>None</i> – Will not send Storm trap warning messages regardless of action taken by the Traffic Control mechanism.

	<ul style="list-style-type: none"> • <i>Storm Occurred</i> – Will send Storm Trap warning messages upon the occurrence of a Traffic Storm only. • <i>Storm Cleared</i> – Will send Storm Trap messages when a Traffic Storm has been cleared by the Switch only. • <i>Both</i> – Will send Storm Trap messages when a Traffic Storm has been both detected and cleared by the Switch. <p>This function cannot be implemented in the Hardware mode. (When Drop is chosen in the Action field).</p>
Traffic Control Auto Recover Time (0-65535)	Enter the time allowed for auto recovery from shutdown for a port. The default value is 0, which means no auto recovery is possible and the port remains in shutdown forever mode. This requires manual entry of the CLI command “config ports [<portlist> all] state enable” to return the port to a forwarding state.
Traffic Control Settings	
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From / To	Select the ports of this Switch to configure for Storm Control.
Broadcast	Enables or disable Broadcast Storm Control.
Multicast	Enables or disables Multicast Storm Control.
Unicast	Enables or disables Unicast Storm Control.
Action	<p>Select the method of traffic Control from the pull-down menu. The choices are:</p> <p><i>Drop</i> – Utilizes the hardware Traffic Control mechanism, which means the Switch’s hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved.</p> <p><i>Shutdown</i> – Utilizes the Switch’s software Traffic Control mechanism to determine the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the Countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the Storm Control Recover setting at the top of this window. Choosing this option obligates the user to configure the Interval setting as well, which will provide packet count samplings from the Switch’s chip to determine if a Packet Storm is occurring.</p>
Threshold (0-255000)	Specifies the maximum number of packets per second that will trigger the Traffic Control function to commence. The configurable threshold range is from 0 to 255000 with a default setting of 131072.
Count Down (0 or 3-30)	The Count Down timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. This parameter is only useful for ports configured as Shutdown in their Action field and therefore will not operate for Hardware based Traffic Control implementations. The possible time settings for this field are 0, 3 to 30 minutes. 0 is the default setting for this field and will denote that the port will never shutdown.
Time Interval (5-600)	The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch’s chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. The Interval may be set between 5 and 600 seconds with the default setting of 5 seconds.

Click **Apply** to implement the settings of each field.



NOTE: Traffic Control cannot be implemented on ports that are set for Link Aggregation (Port Trunking).



NOTE: Ports that are in the Shutdown (Forever) mode will be seen as Discarding in Spanning Tree windows and implementations though these ports will still be forwarding BPDUs to the Switch's CPU.



NOTE: Ports that are in Shutdown (Forever) mode will be seen as link down in all windows and screens until the user recovers these ports.

Port Security

Port Security Settings

A given port's (or a range of ports') dynamic MAC address learning can be locked such that the current source MAC addresses entered into the MAC address forwarding table can not be changed once the port lock is enabled. The port can be locked by using the **Admin State** pull-down menu to *Enabled*, and clicking **Apply**.

Port Security is a security feature that prevents unauthorized computers (with source MAC addresses) unknown to the Switch prior to locking the port (or ports) from connecting to the Switch's locked ports and gaining access to the network.

To view this window, click **Security > Port Security > Port Security Settings**, as shown below:


Port Security Settings						
Unit	From	To	Admin State	Max.Addr (0-64)	Mode	Apply
1	Port 1	Port 1	Disabled	1	DeleteOnReset	Apply
Port Security Table-Unit 1						
Port	Admin State	Max.Learning Addr	Lock Address Mode	Clear		
1	Disabled	1	DeleteOnReset	X		
2	Disabled	1	DeleteOnReset	X		
3	Disabled	1	DeleteOnReset	X		
4	Disabled	1	DeleteOnReset	X		
5	Disabled	1	DeleteOnReset	X		
6	Disabled	1	DeleteOnReset	X		
7	Disabled	1	DeleteOnReset	X		
8	Disabled	1	DeleteOnReset	X		
9	Disabled	1	DeleteOnReset	X		
10	Disabled	1	DeleteOnReset	X		
11	Disabled	1	DeleteOnReset	X		
12	Disabled	1	DeleteOnReset	X		
13	Disabled	1	DeleteOnReset	X		
14	Disabled	1	DeleteOnReset	X		
15	Disabled	1	DeleteOnReset	X		
16	Disabled	1	DeleteOnReset	X		
17	Disabled	1	DeleteOnReset	X		
18	Disabled	1	DeleteOnReset	X		
19	Disabled	1	DeleteOnReset	X		
20	Disabled	1	DeleteOnReset	X		
21	Disabled	1	DeleteOnReset	X		
22	Disabled	1	DeleteOnReset	X		
23	Disabled	1	DeleteOnReset	X		
24	Disabled	1	DeleteOnReset	X		

Figure 6 - 3 Port Security Settings window

The following parameters can be set:


Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.

From / To	A consecutive group of ports may be configured starting with the selected port.
Admin State	This pull-down menu allows the user to enable or disable Port Security (locked MAC address table for the selected ports).
Max. Addr. (0-64)	The number of MAC addresses that will be in the MAC address forwarding table for the selected switch and group of ports.
Mode	This pull-down menu allows the option of how the MAC address table locking will be implemented on the Switch, for the selected group of ports. The options are: <i>Permanent</i> – The locked addresses will only age out after the Switch has been reset. <i>DeleteOnTimeout</i> – The locked addresses will age out after the aging timer expires. <i>DeleteOnReset</i> – The locked addresses will not age out until the Switch has been reset or rebooted.

Click the corresponding  button to clear MAC address entries which were learned by the Switch by a specified port. This only relates to the port security function. This command will only take effect if the Mode is set as *Permanent* or *DeleteonReset*. Click **Apply** to implement changes made.

Port Security Entries

The Port Lock Entry Delete window is used to remove an entry from the port security entries learned by the Switch and entered into the forwarding database.

This function is only operable if the **Mode** in the **Port Security** window is selected as **Permanent** or **DeleteOnReset**, or in other words, only addresses that are statically learned by the Switch can be deleted. Once the entry has been defined by entering the correct information into the window above, click the  under the **Delete** heading of the corresponding MAC address to be deleted. Click the **Next** button to view the next page of entries listed in this table.

To view this window, click **Security > Port Security > Port Lock Entries**, as shown below.

Total Entries: 0						
Port Security Entries Table						
VID	VLAN Name	MAC Address	Unit	Port	Type	Delete

Figure 6 - 4 Port Lock Entries Table

This window displays the following information:

Parameter	Description
VID	The VLAN ID of the entry in the forwarding database table that has been permanently learned by the Switch.
VLAN Name	The VLAN Name of the entry in the forwarding database table that has been permanently learned by the Switch.
MAC Address	The MAC address of the entry in the forwarding database table that has been permanently learned by the Switch.
Unit	The Switch ID number of the Switch in the switch stack.
Port	The ID number of the port that has permanently learned the MAC address.
Type	The type of MAC address in the forwarding database table. Only entries marked Permanent or Delete on Reset can be deleted.

Click the  to delete the corresponding MAC address that was permanently learned by the Switch.

IP-MAC-Port Binding

General Overview

The Switch offers IP-MAC-Port Binding (IMPB), a D-Link security application used most often on edge switches directly connected to network hosts. IMPB is also an integral part of D-Link's End-to-End Security Solution (E2ES). The primary purpose of IP-MAC-Port Binding is to restrict client access to a switch by enabling administrators to configure pairs of client MAC and IP addresses that are allowed to access networks through a switch. Specifically, IMPB binds together the four-byte IP address and the six-byte Ethernet link layer MAC address to allow the transmission of data between the layers.

The IMPB function is port-based, meaning that a user can enable or disable the function on any individual port. Once IMPB is enabled on a switch port, the switch will restrict or allow client access by checking the pair of IP-MAC addresses with the pre-configured database, also known as the "IMPB white list". If an unauthorized user tries to access an IMPB-enabled port, the system will block access by dropping its packet. The creation of the IMPB white list can be manually configured by CLI or Web.

Common IP Management Security Issues

Currently, certain limitations and issues in IP management structures can lead to serious security problems. Auditing mechanisms, such as syslog, application log, firewall log, etc, are mainly based on client IP information. However, such log information is meaningless if the client IP address can be easily changed. IP conflict, the most common problem in today's networks, is another major security concern. Without IMPB, any user can change an IP address manually and cause conflict with other resources, such as other PCs, core switches, routers or servers. Not only does this duplicate IP create an auditing issue, it also poses potential risk to the entire network.

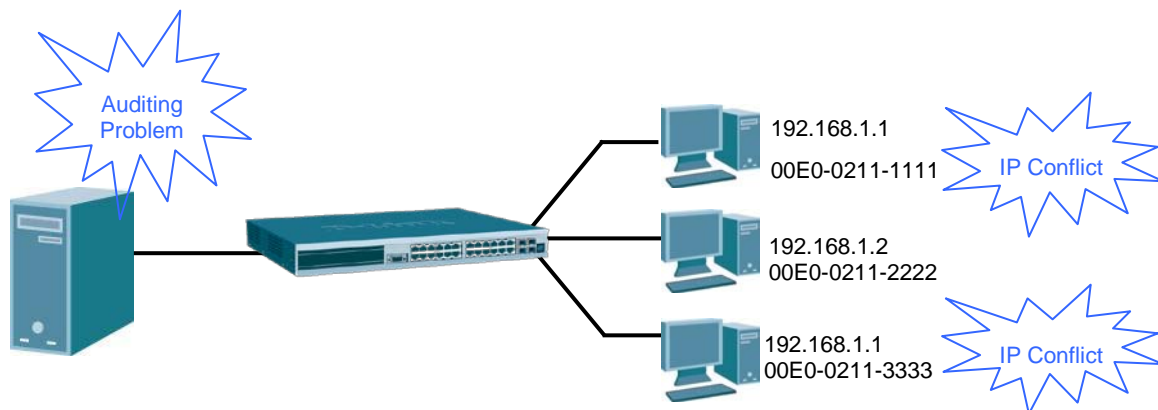


Figure 6 - 5 Common IP Management IP Security Issues

ARP spoofing attacks in which malicious users intercept traffic or interrupt connections by manipulating ARP packets are another serious challenge in securing today's network. Further information on how ARP spoofing attacks work can be found in the Appendix, "Mitigating ARP Spoofing Attack via Packet Content ACL," located in the back of this manual.

Solutions to Improve IP Management Security

D-Link has introduced IMPB technology to protect networks from attacks. By using IP-MAC-Port Binding, all packets are dropped by a switch when the combination of MAC address, IP address, and connected port is not in the IMPB white list. IMPB allows the user to choose either ARP or ACL mode. In addition, an IMPB white list can be dynamically created with the DHCP snooping option. DHCP snooping is a global setting and can be enabled on top of ACL or ARP mode. Each option has its advantages and disadvantages.

ARP Mode

In ARP Mode, a switch performs ARP Packet Inspection in which it checks the IP-MAC pairs in ARP packets with the IMPB white list and denies unauthorized ones. An advantage of ARP mode is that it does not consume any ACL rules on the Switch. Nonetheless, since the switch only checks ARP packets, it cannot block unauthorized clients who do not send out ARP packets.

ACL Mode

In ACL Mode, a switch performs IP Packet Inspection in addition to ARP Packet Inspection. Essentially, ACL rules will be used to permit statically configured IMPB entries and deny other IP packets with the incorrect IP-MAC pairs. The distinct advantage of ACL Mode is that it ensures better security by checking both ARP Packets and IP Packets. However, doing so requires the use of ACL rules. ACL Mode can be viewed as an enhanced version of ARP Mode because ARP Mode is enabled by default when ACL Mode is selected.

Strict and Loose State

Other than ACL and ARP mode, users can also configure the state on a port for granular control. There are two states: Strict and Loose, and only one state can be selected per port. If a port is set to Strict state, all packets entering the port are denied (dropped) by default. The switch will continuously compare all IP and ARP packets it receives on that port with its IMPB entries. If the IP-MAC pair in the packet matches the IMPB entry, the MAC address will be unblocked and subsequent packets sent from this client will be forwarded. On the other hand, if a port is set to Loose state, all packets entering the port are permitted (forwarded) by default. The switch will continuously compare all ARP packets it receives on that port with its IMPB entries. If the IP-MAC pair in the ARP packet does not match the IMPB white list, the MAC address will be blocked and subsequent packets sent from this client will be dropped.

DHCP Snooping Option

If DHCP snooping is enabled, the switch learns IP-MAC pairs by snooping DHCP packets automatically and then saves them to the IP-MAC-Port Binding white list. This enables a hassle-free configuration because the administrator does not need to manually enter each IMPB entry. A prerequisite for this is that the valid DHCP server’s IP-MAC pair must be configured on the switch’s IMPB while list first; otherwise the DHCP server packets will be dropped. DHCP snooping is generally considered to be more secure because it enforces all clients to acquire IP through the DHCP server. Additionally, it makes IP Information auditable because clients cannot manually configure their own IP address.

An example of DHCP snooping in which PC-A and PC-B get their IP addresses from a DHCP server is depicted below. The switch snoops the DHCP conversation between PC-A, PC-B, and the DHCP server. The IP address, MAC address, and connecting ports of both PC-A and PC-B are learned and stored in the switch’s IMPB white list. Therefore, these PCs will be able to connect to the network. Then there is PC-C, whose IP address is manually configured by the user. Since this PC’s IP-MAC pair does not match the one on Switch’s IMPB white list, traffic from PC-C will be blocked.

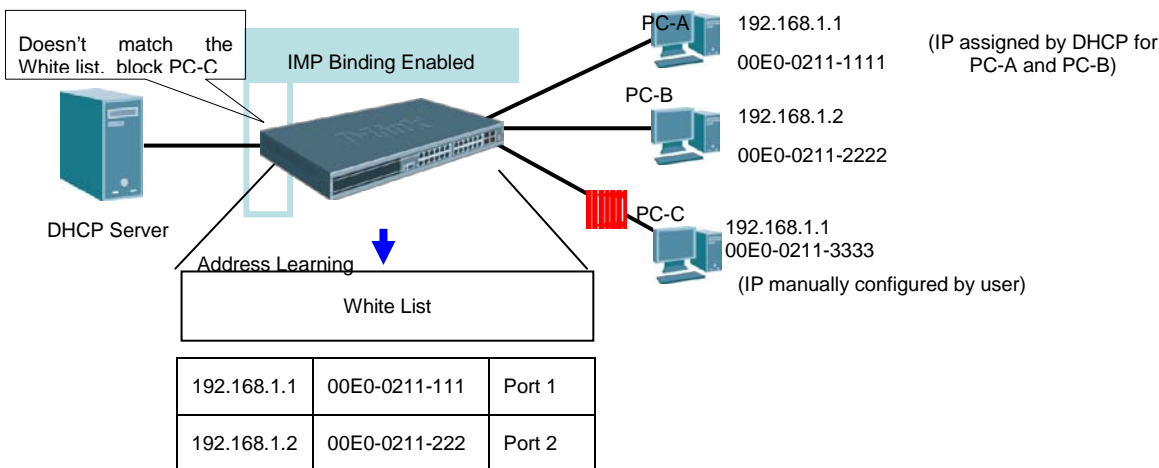


Figure 6 - 6 DHCP Snooping Example

ARP Inspection

ARP spoofing can attack hosts, switches, and routers connected to a Layer 2 network by “poisoning” their ARP caches. As the figure below shows, Host C can “poison” the ARP caches of Host B by broadcasting forged ARP responses with bindings (IP B, MAC C). As a result, Host C intercepts the traffic sent to Host B. IMPB v3.8 was developed to prevent this kind of ARP spoofing (including Netcut and Netcut restore attacks).

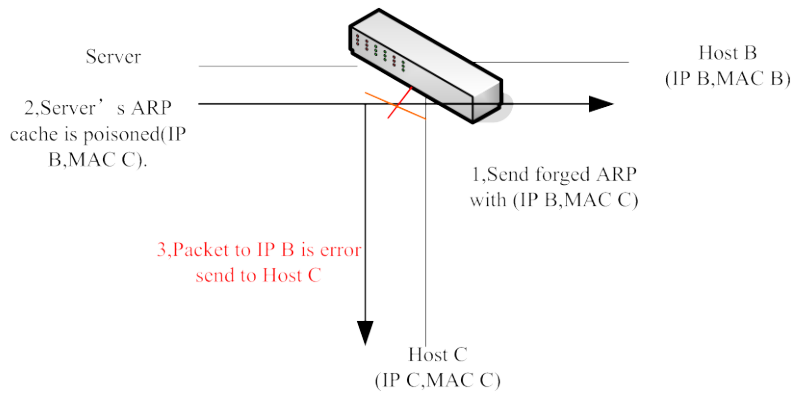


Figure 6 - 7 ARP Cache Poisoning

When the user configures strict mode and enables IMPB on a port, ARP inspection is enabled. For an ARP inspection active port: All ARP packets should be captured to the CPU (including broadcast ARP and unicast ARP packets) and the CPU will make the decision to either forward or drop.

The switch will validate the ARP packets by retrieving the sender's MAC/ IP address from the ARP packet payload and sender hardware address. If the IP/ MAC address are in the IMPB forwarding list, the ARP packets will be forwarded. Otherwise, the ARP packet will be discarded.

Strict Mode Behavior Change

As the figure below shows, in a mixed network (both IPv4 and IPv6 used), if illegal IPv4-A packets are detected and there are write-blocked FDB entries, then IPv6-Global also cannot access the network. To avoid this case, do not write-block FDB. Not write-blocking FDB can also avoid netcut attacks and recover attacks.

- For host A, for each IP:
- 1, IPv6-Global can access IPv6 sites.
 - 2, IPv6-Local can't access IPv6 sites.
 - 2, IPv4-A can't access network.

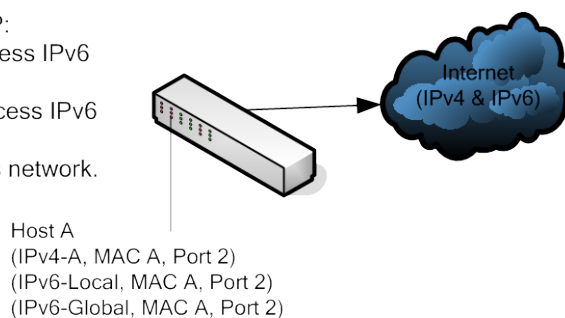


Figure 6 - 8 IPv4 and IPv6 Sharing

When enabling Strict mode, the Switch will stop writing dropped FDB entries on these ports. If the Switch detects legal packets, the Switch will need to create the FDB forwarding entries. ACL mode always run under strict mode. When a user enables ACL mode on some ports, these ports will change from Loose mode to Strict mode and the configuration will also change to Strict mode. For compound authentication AND mode (IMPB+1X, IMPB+WAC, IMPB+JWAC), the ports always run in Strict mode.

IMPB Global Settings

This window is used to enable or disable the global IMPB settings: Trap Log State and DHCP Snoop state, on the Switch.

The Trap/Log field will enable and disable the sending of trap / log messages for IMPB. When enabled, the Switch will send traps and log messages when an ARP packet is received that doesn't match the IP-MAC binding entries configured on the Switch.

The DHCP Snoop State field will enable and disable the DHCP Snooping option.

To view this window, click **Security > IP-MAC-Port Binding > IMPB Global Settings**:

IMPB Global Settings	
Trap / Log	Disabled
DHCP Snoop (IPv4)	Disabled
DHCP Snoop (IPv6)	Disabled
ND Snoop	Disabled

Apply

Figure 6 - 9 IMPB Global Settings window

The following parameters can be set:

Parameter	Description
Trap / Log	This field will enable and disable the sending of trap log messages for IP-MAC binding. When enabled, the Switch will send a trap log message to the SNMP agent and the Switch log when an ARP packet is received that doesn't match the IP-MAC binding configuration set on the Switch.
DHCP Snoop (IPv4)	Use the pull-down menu to enable or disable the DHCP snooping state (IPv4) for IP-MAC-port binding.
DHCP Snoop (IPv6)	Use the pull-down menu to enable or disable the DHCP snooping state (IPv6) for IP-MAC-port binding.
ND Snoop	Use the pull-down menu to enable or disable the ND snooping state for IP-MAC-port binding.

Click **Apply** to implement the settings made.

IMPB Port Settings

This window is used to configure IMP settings on a port basis.

Select a port or a range of ports with the From Port and To Port fields. Enable or disable the port with Strict or Loose State, enable or disable Allow Zero IP and Forward DHCP Packet fields, and configure the port's Max IMPB entry.

To view this window, click **Security > IP-MAC-Port Binding > IMPB Port Settings**, as shown below.

IMPB Port Settings										
Unit	From	To	State	Allow Zero IP	Forward DHCP PKT	Mode	Stop Learning Threshold (0-500)	Recover Learning	Max Entry (1-50)	Apply
1	Port 1	Port 1	Disabled	Disabled	Enabled	ARP	500	<input type="checkbox"/> Normal	<input checked="" type="checkbox"/> No Limit	Apply

IMPB Port Table							
Port	IPv4 State	IPv6 State	Zero IP	DHCP Packet	Mode	Max Entry	Stop Learning Threshold/Mode
1	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
2	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
3	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
4	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
5	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
6	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
7	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
8	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
9	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
10	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
11	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
12	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
13	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
14	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
15	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
16	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
17	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
18	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
19	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
20	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
21	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
22	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
23	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal
24	Disabled	Disabled	Not Allow	Forward	ARP	No Limit	500/Normal

Figure 6 - 10 IMPB Port Settings window

The following fields can be set or modified:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From / To	Select a port or range of ports to set for IP-MAC Binding.
State	<p>Use the pull-down menu to enable or disable these ports for IP-MAC Binding.</p> <p><i>Enabled Strict</i> – This state provides a stricter method of control. If the user selects this mode, all packets are blocked by the Switch by default. The Switch will compare all incoming ARP and IP Packets and attempt to match them against the IMPB white list. If the IP-MAC pair matches the white list entry, the packets from that MAC address are unblocked. If not, the MAC address will stay blocked. While the Strict state uses more CPU resources from checking every incoming ARP and IP packet, it enforces better security and is thus the recommended setting.</p> <p><i>Enabled Loose</i> – This mode provides a looser way of control. If the user selects loose mode, the Switch will forward all packets by default. However, it will still inspect incoming ARP packets and compare them with the Switch’s IMPB white list entries. If the IP-MAC pair of a packet is not found in the white list, the Switch will block the MAC address. A major benefit of Loose state is that it uses less CPU resources because the Switch only checks incoming ARP packets. However, it also means that Loose state cannot block users who send only unicast IP</p>

	<p>packets. An example of this is that a malicious user can perform DoS attacks by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks because the PC will not send out ARP packets.</p>
Allow Zero IP	<p>Use the pull-down menu to enable or disable this feature. Once enabled, the Switch will allow ARP packets with a Source IP of 0.0.0.0 to pass through.</p> <p>This is useful in some scenarios when a client (for example, a wireless Access Point,) sends out an ARP request packet before accepting the IP address from a DHCP server. In this case, the ARP request packet sent out from the client will contain a Source IP of 0.0.0.0. The Switch will need to allow such packets to pass, or else the client cannot know if there is another duplicate IP address in the network.</p>
Forward DHCP PKT	<p>By default, the Switch will forward all DHCP packets. However, if the port state is set to Strict, all DHCP packets will be dropped. In that case, select <i>Enable</i> so that the port will forward DHCP packets even under Strict state. Enabling this feature also ensures that DHCP snooping works properly.</p>
Mode	<p>Use the pull-down menu to select ARP or ACL mode.</p> <p><i>ARP Mode</i> – When selecting this mode, the Switch will perform ARP Packet Inspection only and no ACL rules will be used.</p> <p><i>ACL Mode</i> – When selecting this mode, the Switch will perform IP Packet Inspection in addition to ARP Packet Inspection. ACL rules will be used under this mode.</p>
Stop Learning Threshold (0-500)	<p>Whenever a MAC address is blocked by the Switch, it will be recorded in the Switch's L2 Forwarding Database (FDB) and associated with a particular port. To prevent the Switch FDB from overloading in case of an ARP DoS attack, the administrator can configure the threshold when a port should stop learning illegal MAC addresses.</p> <p>Enter a Stop Learning threshold between 0 and 500. Entering 500 means the port will enter the Stop Learning state after 500 illegal MAC entries and will not allow additional MAC entries, both legal or illegal, to be learned on this port. In the Stop Learning state, the port will also automatically purge all blocked MAC entries on this port. Traffic from legal MAC entries are still forwarded.</p> <p>Entering 0 means no limit has been set and the port will keep learning illegal MAC addresses.</p>
Recover Learning	<p>This feature can only be applied when a port is already in Stop Learning state. Check <i>Normal</i> to recover the port back to normal state, under which the port will start learning both illegal and legal MAC addresses again.</p> <p>Selecting this feature when the port is in Normal state will do nothing.</p>
Max Entry (1-50)	<p>Specifies the maximum number of dynamic (DHCP snooped) IP-MAC-Port Binding entries that can be learned on the port. Enter a value between 1 to 50 to restrict dynamic IMPB entries on this port.</p> <p>By default, the-per port max entry has No Limit.</p>

Click **Apply** to implement the changes.

IMPB Entry Settings

The table on this window, which is also known as the “IMPB white list,” is used to create Static IP-MAC-Port Binding entries on the Switch.

To view this window, click **Security > IP-MAC-Port Binding > IMPB Entry Settings**, as shown below.

Figure 6 - 11 IMPB Entry Settings window

The following fields can be set or modified:

Parameter	Description
IPv4 Address	Click the radio button and enter the IPv4 address to bind to the MAC address set below.
IPv6 Address	Click the radio button and enter the IPv6 address to bind to the MAC address set below.
MAC Address	Enter the MAC address to bind to the IP Address set above.
Ports	Specify the switch ports for which to configure this IP-MAC binding entry (IP Address + MAC Address). Tick the All Ports check box to configure this entry for all ports on the Switch.

Click **Add** to create a new entry, click **Find** to search for an entry, click **View All** to display all entries, and click **Delete All** to remove all entries on the window.

DHCP Snoop Entries

This window is used to view DHCP Snooping entries on specific ports.

To view this window, click **Security > IP-MAC-Port Binding > DHCP Snoop Entries**, as shown below.

Figure 6 - 12 DHCP Snooping Entries window

The following fields can be set:

Parameter	Description
Unit - Port	Use the pull-down menu to choose the Switch ID number of the Switch in the switch stack and the port on the Switch.
Ports (e.g: 1, 5, 7-12)	Specify the switch ports or tick the All Ports check box to select all ports.
Clear Type	Use the pull-down menu to select the <i>IPv4</i> , <i>IPv6</i> or <i>All</i> type.

To view particular port settings, choose the unit - port number and click **Find**. To view all entries on the window, click **View All**. To delete an entry, enter the port number, choose the Clear Type, and click **Clear**.

MAC Block List

This window is used to view unauthorized devices that have been blocked by IP-MAC binding restrictions.

To view this window, click **Security > IP-MAC-Port Binding > MAC Block List**, as shown below.

Figure 6 - 13 MAC Blocked List window

To find an unauthorized device MAC address that has been blocked by the IP-MAC binding restrictions, enter the VLAN Name and MAC Address in the appropriate fields and click **Find**. To delete an entry, click the **Delete** button next to the entry's port. To delete all the entries in this window, click **Delete All**.

ND Snoop Entries

This table is used to view ND snooping entries on specific ports.

To view this window, click **Security > IP-MAC-Port Binding > NP Snoop Entries**, as shown below.

Figure 6 - 14 ND Snoop Entries window

The following fields can be set:

Parameter	Description
Unit - Port	Use the pull-down menu to choose the Switch ID number of the Switch in the switch stack and the port on the Switch.
Ports (e.g: 1, 5, 7-12)	Specify the switch ports or tick the All Ports check box to select all ports.

To view particular port settings, choose the unit - port number from the pull-down menu and click **Find**. To view all entries on the window, click **View All**. To delete an entry, enter the port number, and click **Clear**.

802.1X

802.1X Port-based and Host-based Access Control

The IEEE 802.1X standard is a security measure for authorizing and authenticating users to gain access to various wired or wireless devices on a specified Local Area Network by using a Client and Server based access control model. This is accomplished by using a RADIUS server to authenticate users trying to access a network by relaying Extensible Authentication Protocol over LAN (EAPOL) packets between the Client and the Server. The following figure represents a basic EAPOL packet:

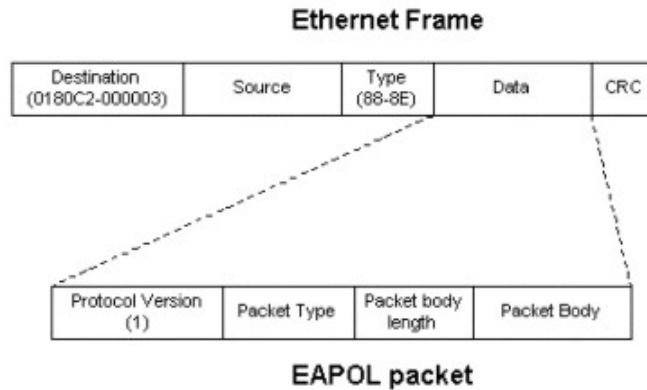


Figure 6 - 15 The EAPOL Packet

Utilizing this method, unauthorized devices are restricted from connecting to a LAN through a port to which the user is connected. EAPOL packets are the only traffic that can be transmitted through the specific port until authorization is granted. The 802.1x Access Control method holds three roles, each of which are vital to creating and upkeeping a stable and working Access Control security method.

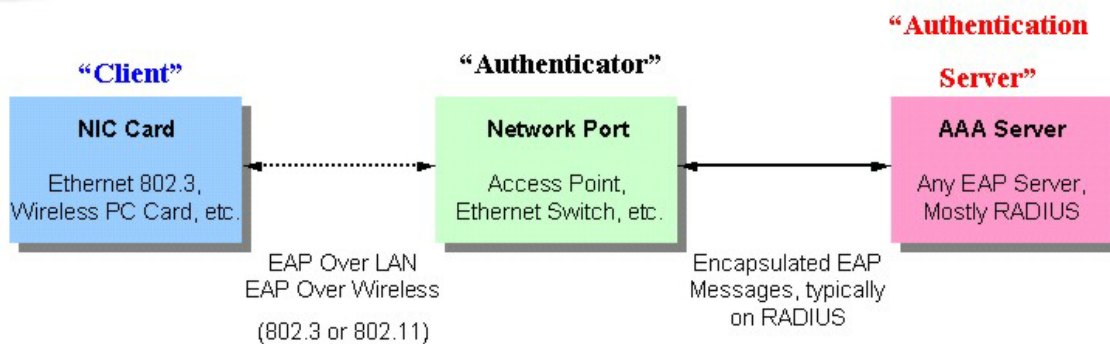


Figure 6 - 16 The three roles of 802.1X

The following section will explain the three roles of Client, Authenticator, and Authentication Server in greater detail.

Authentication Server

The Authentication Server is a remote device that is connected to the same network as the Client and Authenticator, must be running a RADIUS Server program and must be configured properly on the Authenticator (Switch). Clients connected to a port on the Switch must be authenticated by the Authentication Server (RADIUS) before attaining any services offered by the Switch on the LAN. The role of the Authentication Server is to certify the identity of the Client attempting to access the network by exchanging secure information between the RADIUS server and the Client through EAPOL packets and, in turn, informs the Switch whether or not the Client is granted access to the LAN and/or switches services.

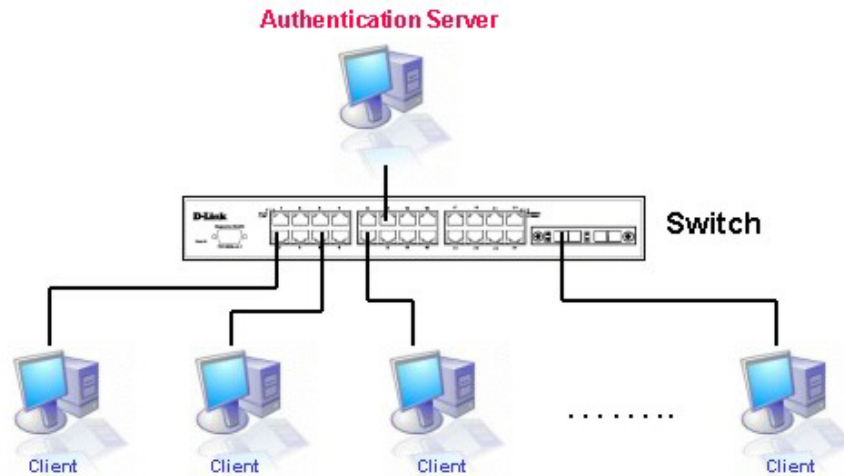


Figure 6 - 17 The Authentication Server

Authenticator

The Authenticator (the Switch) is an intermediary between the Authentication Server and the Client. The Authenticator serves two purposes when utilizing 802.1X. The first purpose is to request certification information from the Client through EAPOL packets, which is the only information allowed to pass through the Authenticator before access is granted to the Client. The second purpose of the Authenticator is to verify the information gathered from the Client with the Authentication Server, and to then relay that information back to the Client.

Three steps must be implemented on the Switch to properly configure the Authenticator.

1. The 802.1X State must be *Enabled*. (**DGS-3400 Web Management Tool**)
2. The 802.1X settings must be implemented by port (**Security / 802.1X / Configure 802.1X Authenticator Parameter**)
3. A RADIUS server must be configured on the Switch. (**Security / 802.1X / Authentic RADIUS Server**)

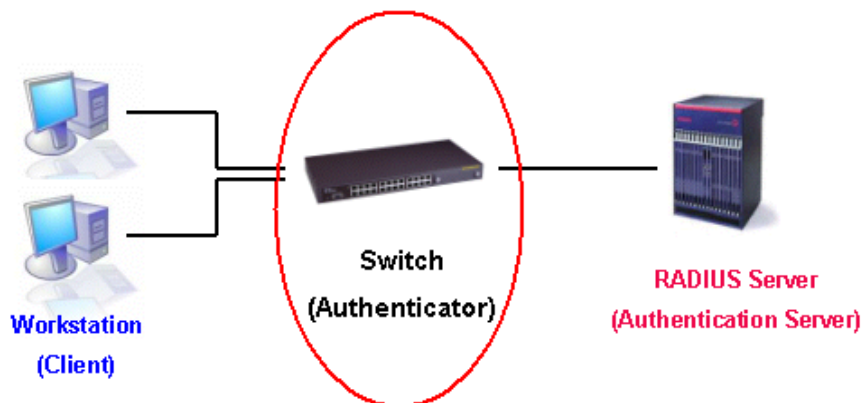


Figure 6 - 18 The Authenticator

Client

The Client is simply the endstation that wishes to gain access to the LAN or switch services. All endstations must be running software that is compliant with the 802.1X protocol. For users running Windows XP, that software is included within the operating system. All other users are required to attain 802.1X client software from an outside source. The Client will request access to the LAN and or Switch through EAPOL packets and, in turn will respond to requests from the Switch.

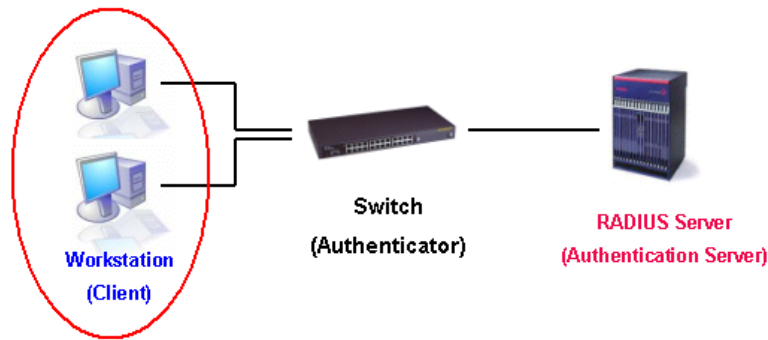


Figure 6 - 19 The Client

Authentication Process

Utilizing the three roles stated above, the 802.1X protocol provides a stable and secure way of authorizing and authenticating users attempting to access the network. Only EAPOL traffic is allowed to pass through the specified port before a successful authentication is made. This port is “locked” until the point when a Client with the correct username and password (and MAC address if 802.1X is enabled by MAC address) is granted access and therefore successfully “unlocks” the port. Once unlocked, normal traffic is allowed to pass through the port. The following figure displays a more detailed explanation of how the authentication process is completed between the three roles stated above.

802.1X Authentication process

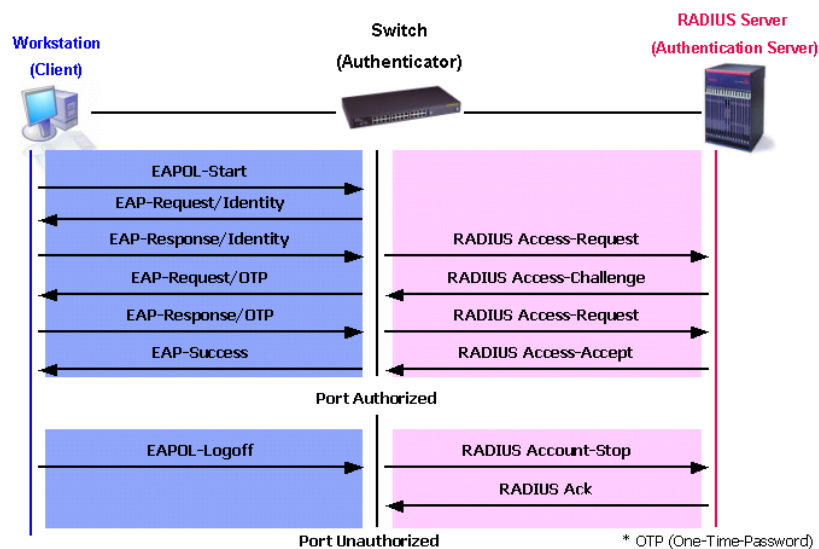


Figure 6 - 20 The 802.1X Authentication Process

The D-Link implementation of 802.1X allows network administrators to choose between two types of Access Control used on the Switch, which are:

1. Port-based Access Control – This method requires only one user to be authenticated per port by a remote RADIUS server to allow the remaining users on the same port access to the network.
2. MAC-based Access Control – Using this method, the Switch will automatically learn up to 128 MAC addresses by port and set them in a list. Each MAC address must be authenticated by the Switch using a remote RADIUS server before being allowed access to the Network.

Understanding 802.1X Port-based and MAC-based Network Access Control

The original intent behind the development of 802.1X was to leverage the characteristics of point-to-point in LANs. As any single LAN segment in such infrastructures has no more than two devices attached to it, one of which is a Bridge Port. The Bridge Port detects events that indicate the attachment of an active device at the remote end of the link, or an active device becoming inactive. These events can be used to control the authorization state of the Port and initiate the process of authenticating the attached device if the Port is unauthorized. This is the Port-based Network Access Control.

Port-based Network Access Control

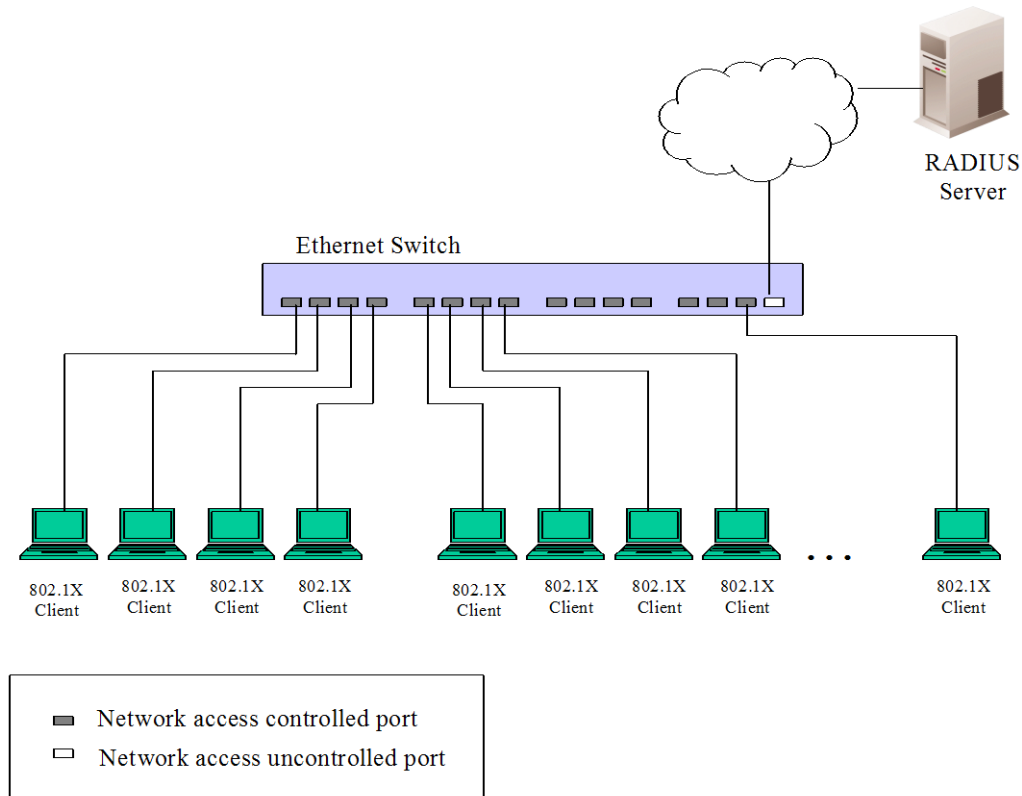


Figure 6 - 21 Example of Typical Port-based Configuration

Once the connected device has successfully been authenticated, the Port then becomes Authorized, and all subsequent traffic on the Port is not subject to access control restriction until an event occurs that causes the Port to become Unauthorized. Hence, if the Port is actually connected to a shared media LAN segment with more than one attached device, successfully authenticating one of the attached devices effectively provides access to the LAN for all devices on the shared segment. Clearly, the security offered in this situation is open to attack.

MAC-Based Network Access Control

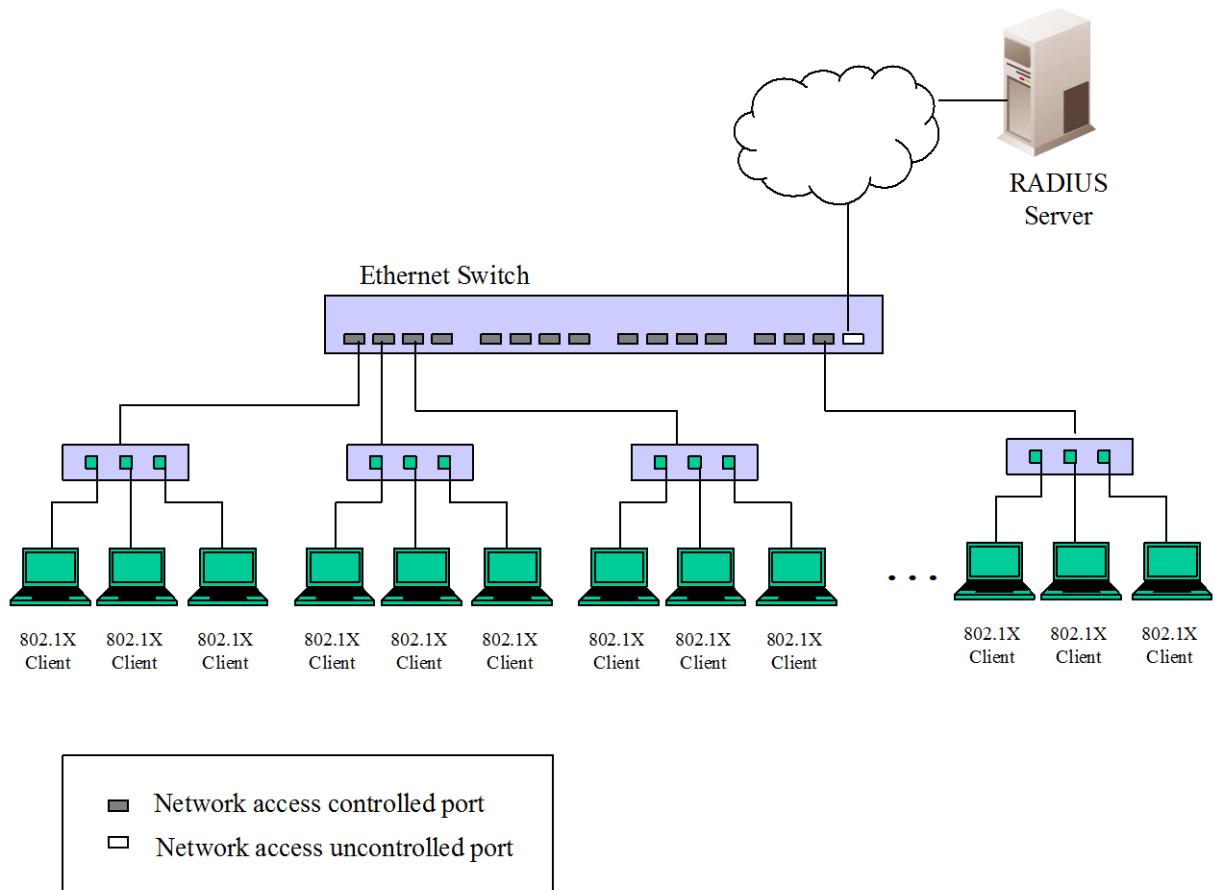


Figure 6 - 22 Example of Typical MAC-Based Configuration

In order to successfully make use of 802.1X in a shared media LAN segment, it would be necessary to create “logical” Ports, one for each attached device that required access to the LAN. The Switch would regard the single physical Port connecting it to the shared media segment as consisting of a number of distinct logical Ports, each logical Port being independently controlled from the point of view of EAPOL exchanges and authorization state. The Switch learns each attached devices’ individual MAC addresses, and effectively creates a logical Port that the attached device can then use to communicate with the LAN via the Switch.

Guest VLANs

On 802.1X security enabled networks, there is a need for non 802.1X supported devices to gain limited access to the network, due to the lack of the proper 802.1X software or incompatible devices, such as computers running Windows 98 or lower operating systems, or the need for guests to gain access to the network without full authorization or local authentication on the Switch. To supplement these circumstances, this switch now implements Guest 802.1X VLANs. These VLANs should have limited access rights and features separate from other VLANs on the network.

To implement Guest 802.1X VLANs, the user must first create a VLAN on the network with limited rights and then enable it as an 802.1X guest VLAN. Then the administrator must configure the guest accounts accessing the Switch to be placed in a Guest VLAN when trying to access the Switch. Upon initial entry to the Switch, the client wishing services on the Switch will need to be authenticated by a remote RADIUS Server or local authentication on the Switch to be placed in a fully operational VLAN. If authenticated and the authenticator possesses the VLAN placement information, that client will be accepted into the fully operational target VLAN and normal switch functions will be open to the client. If the authenticator does not have target VLAN placement information, the client will be returned to its originating VLAN. Yet, if the client is denied authentication by the authenticator, it will be placed in the Guest VLAN where it has limited rights and access. The adjacent figure should give the user a better understanding of the Guest VLAN process.

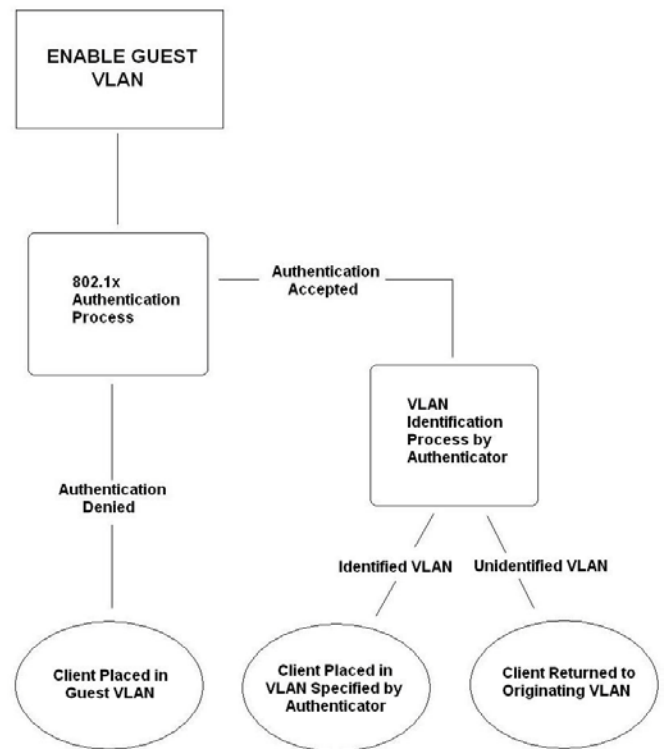


Figure 6 - 23 Guest VLAN Authentication Process

Limitations Using the Guest VLAN

1. Ports supporting Guest VLANs cannot be GVRP enabled and vice versa.
2. A port cannot be a member of a Guest VLAN and a static VLAN simultaneously.
3. Once a client has been accepted into the target VLAN, it can no longer access the Guest VLAN.

802.1X Port Settings

This window is used to configure the 802.1X authenticator settings on the Switch. The user may toggle between switches in the switch stack by using the **Unit** pull-down menu.

To view this window, click **Security > 802.1X > 802.1X Port Settings**, as shown below.

Unit: 1

802.1X Port Table-Unit 1

Port	AdmDir	Port Control	TxPeriod (sec)	Quiet Period (sec)	Supp-Timeout (sec)	Server-Timeout (sec)	MaxReq	ReAuth Period (sec)	Max User	ReAuth Enabled	Forward EAPOL PDU	Capability	Modify
1	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
2	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
3	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
4	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
5	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
6	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
7	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
8	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
9	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
10	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
11	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
12	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
13	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
14	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
15	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
16	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
17	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
18	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
19	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
20	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
21	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
22	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
23	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify
24	both	Auto	30	60	30	30	2	3600	16	No	Disabled	None	Modify

Figure 6 - 24 Configure 802.1X Authenticator Parameter window

To configure the settings by port, click its corresponding **Modify** button, which will display the following table to configure:

802.1X Port Settings-Unit 1	
Unit	1
From	Port 1
To	Port 1
AdmDir	both
Port Control	auto
TXPeriod (1-65535)	30 sec
QuietPeriod (0-65535)	60 sec
SuppTimeout (1-65535)	30 sec
ServerTimeout (1-65535)	30 sec
MaxReq (1-10)	2
ReAuthPeriod (1-65535)	3600 sec
Max User (1-128)	16 <input type="checkbox"/> No Limit
ReAuth	Disabled
Forward EAPOL PDU	Disabled
Capability	None
Show Authenticators Setting for Unit 1 Apply	

Figure 6 - 25 Configure 802.1X Port Settings window

This screen allows setting of the following features:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From / To	Enter the port or ports to be set.
AdmDir	Sets the administrative-controlled direction to either <i>in</i> or <i>both</i> . If <i>in</i> is selected, control is only exerted over incoming traffic through the port selected in the first field. If <i>both</i> is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field.
Port Control	This allows the user to control the port authorization state. Select <i>forceAuthorized</i> to disable 802.1X and cause the port to transition to the authorized state without any authentication exchange required. This means the port transmits and receives normal traffic without 802.1X-based authentication of the client. If <i>forceUnauthorized</i> is selected, the port will remain in the unauthorized state, ignoring all attempts by the client to authenticate. The Switch cannot provide authentication services to the client through the interface. If <i>Auto</i> is selected, it will enable 802.1X and cause the port to begin in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port transitions from down to up, or when an EAPOL-start frame is received. The Switch then requests the identity of the client and begins relaying authentication messages between the client and the authentication server. The default setting is <i>Auto</i> .

TXPeriod (1-65535)	This sets the TXPeriod of time for the authenticator PAE state machine. This value determines the period of an EAP Request/Identity packet transmitted to the client. The default setting is 30 seconds.
QuietPeriod (0-65535)	This allows the user to set the number of seconds that the Switch remains in the quiet state following a failed authentication exchange with the client. The default setting is 60 seconds.
SuppTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the client. The default setting is 30 seconds.
ServerTimeout (1-65535)	This value determines timeout conditions in the exchanges between the Authenticator and the authentication server. The default setting is 30 seconds.
MaxReq (1-10)	The maximum number of times that the Switch will retransmit an EAP Request to the client before it times out of the authentication sessions. The default setting is 2.
ReAuthPeriod (1-65535)	A constant that defines a nonzero number of seconds between periodic reauthentication of the client. The default setting is 3600 seconds.
MaxUser (1-128)	The maximum number of users for each port that can be learned via 802.1X authentication. Tick No Limit check box to support up to 128 users.
ReAuth	Determines whether regular reauthentication will take place on this port. The default setting is <i>Disabled</i> .
Forward EAPOL PDU	This enables or disables the Switch retransmit EAPOL PDU Request on a per port basis.
Capability	This allows the 802.1X Authenticator settings to be applied on a per-port basis. Select <i>Authenticator</i> to apply the settings to the port. When the setting is activated, a user must pass the authentication process to gain access to the network. Select <i>None</i> disable 802.1X functions on the port.

Click **Apply** to implement your configuration changes. To view configurations for the 802.1X Authenticator Settings on a port-by-port basis, click [Show Authenticators Settings for Unit 1](#) link.

Guest VLAN Settings

This window is used to configure the 802.1X Guest VLAN on the Switch. Remember, to set a Guest 802.1x VLAN, the user must first configure a normal VLAN which can be enabled here for Guest VLAN status.

To view this window, click **Security > 802.1x > Guest VLAN Settings**, as shown below.

Figure 6 - 26 Configure 802.1x Guest VLAN window

The following fields may be modified to enable the guest 802.1x VLAN:

Parameter	Description
VLAN Name	Enter the pre-configured VLAN name to create as a Guest 802.1x VLAN.
Operation	The user has four choices in configuring the Guest 802.1X VLAN, which are:

	<p><i>Enabled ports</i> – Selecting this option will enable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message.</p> <p><i>Disabled ports</i> – Selecting this option will disable ports listed in the Port List below, as part of the Guest VLAN. Be sure that these ports are configured for this VLAN or users will be prompted with an error message.</p> <p>Select <i>Add</i> or <i>Delete</i> to add or remove a guest VLAN.</p>
Port List	Set the port list of ports to be enabled for the Guest 802.1x VLAN using the pull-down menus.

Click **Apply** to implement the guest 802.1x VLAN settings entered. Only one VLAN may be assigned as the 802.1X Guest VLAN.

Authentication RADIUS Server Settings

The RADIUS feature of the Switch allows the user to facilitate centralized user administration as well as providing protection against a sniffing, active hacker. The Web Manager offers three windows.

To view this window, click **Security > 802.1X > Authentication RADIUS Server Settings**, as shown below.

Authentication RADIUS Server Settings

Index	First <input type="button" value="v"/>	
IPv4 Address	<input type="text" value="0.0.0.0"/>	<input checked="" type="radio"/>
IPv6 Address	<input type="text"/>	<input type="radio"/>
Authentication UDP Port (1-65535)	<input type="text" value="1812"/>	<input type="checkbox"/> Default
Accounting UDP Port (1-65535)	<input type="text" value="1813"/>	<input type="checkbox"/> Default
Key	<input type="text"/>	
Confirm Key	<input type="text"/>	
Timeout (1-255)	<input type="text" value="5"/> sec	<input type="checkbox"/> Default
Retransmit (1-20)	<input type="text" value="2"/>	<input type="checkbox"/> Default
Status	Valid <input type="button" value="v"/>	

Current RADIUS Server(s) Settings Table

Index	IP Address	Authentication UDP Port	Accounting UDP Port	Status	Key	Timeout (sec)	Retransmit
First							
Second							
Third							

Figure 6 - 27 Authentic RADIUS Server window

This window displays the following information:

Parameter	Description
Index	Choose the desired RADIUS server to configure: <i>First</i> , <i>Second</i> or <i>Third</i> .
IPv4 Address	Click the radio button and enter the RADIUS IPv4 address.

IPv6 Address	Click the radio button and enter the RADIUS IPv6 address.
Authentic UDP Port (1-65535)	Set the RADIUS authentic server(s) UDP port. The default port is 1812.
Accounting UDP Port (1-65535)	Set the RADIUS account server(s) UDP port. The default port is 1813.
Key	Set the key the same as that of the RADIUS server.
Confirm Key	Confirm the shared key is the same as that of the RADIUS server.
Timeout (1-255)	Enter the timeout value in seconds (1 to 255). The default value is 5.
Retransmit (1-20)	Set the count for retransmit(1 to 20).The default value is 2.
Status	This allows the user to set the RADIUS Server as <i>Valid</i> (Enabled) or <i>Invalid</i> (Disabled).

Click **Apply** to implement the changes.

802.1X User Settings

This window allows the user to set different local users on the Switch and set a global limitation on the maximum number of users that can be learned via 802.1X authentication.


To view this window, click **Security > 802.1X > 802.1X User Settings**, as shown below.

Figure 6 - 28 802.1X User Setting window

This screen allows setting of the following features:

Parameter	Description
Max User (1-4000)	Enter the maximum number of users to be allowed. Check the No Limit check box to specify that there will be the maximum number of users. By default there is no limit.
User Name	Enter the User Name of the new profile to be created.
Password	Enter a password for the new user.

Confirm Password	Re-enter the password entered in the field above.
-------------------------	---

Click **Apply** to implement the changes. The new User will be displayed in the 802.1X User Table. To remove a user click the corresponding  button.



NOTE: The user must first globally enable 802.1X in the **DGS-3400 Web Management Tool** window before setting up ports.

Initialize Port(s)

Existing 802.1X port and MAC settings are displayed and can be configured using the window below.

To view this window, click **Security > 802.1X > Initialize Port(s)**, as shown below.

Figure 6 - 29 Initialize Port window (Port-based 802.1X)

This window allows initialization of a port or group of ports. The Initialize Port Table in the bottom half of the window displays the current status of the port(s).

To initialize ports for the MAC side of 802.1X, the user must first enable 802.1X by MAC address in the **DGS-3400 Web Management Tool** window.

Click **Security > 802.1X > Initialize Port(s)**, as shown below.

Figure 6 - 30 Initialize Ports window (MAC-based 802.1X)

To initialize ports, first choose the switch in the switch stack by using the pull-down menu and then choose the range of ports in the From and To field. Then the user must specify the MAC address to be initialized by entering it into the MAC Address field and ticking the corresponding check box. To begin the initialization, click **Apply**.

The following parameters can be configured or viewed:

Parameter	Description
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.

From / To	Select ports to be initialized.
MAC Address	The MAC address of the Switch connected to the corresponding port, if any.
Port	A read-only field indicating a port on the Switch.
Auth PAE State	The Authenticator PAE State will display one of the following: Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuth, ForceUnauth, and N/A.
Backend State	The Backend Authentication State will display one of the following: Request, Response, Success, Fail, Timeout, Idle, Initialize, and N/A.
Port Status	The status of the controlled port can be <i>Authorized</i> , <i>Unauthorized</i> , or <i>N/A</i> .

Click **Apply** to implement the changes.



NOTE: The user must first globally enable 802.1X in the **DGS-3400 Web Management Tool** window before initializing ports. Information in the Initialize Ports Table cannot be viewed before enabling 802.1X.

Reauthenticate Port(s)

This window allows reauthentication of a port or group of ports by using the pull-down menus From and To and clicking **Apply**. The Reauthenticate Port Table displays the current status of the reauthenticated port(s) once **Apply** has been clicked.

To view this window, click **Security > 802.1X > Reauthenticate Port(s)**, as shown below.

Reauthenticate Port(s)			
Unit	From	To	Apply
1	Port 1	Port 1	Apply

Reauthenticate Port Table-Unit 1			
Port	Auth PAE State	Backend State	Port Status

Figure 6 - 31 Reauthenticate Port window (Port-based 802.1X)



NOTE: The user must first globally enable 802.1X in the **DGS-3400 Web Management Tool** window before initializing ports. Information in the Initialize Ports Table cannot be viewed before enabling 802.1X.

To reauthenticate ports for the MAC side of 802.1X, the user must first enable 802.1X by MAC address in the **DGS-3600 Web Management Tool** window.

Click **Security > 802.1X > Reauthenticate Port(s)**, as shown below.

Reauthenticate Port(s)	
Unit	1 ▾
From	Port 1 ▾
To	Port 1 ▾
MAC Address	<input type="checkbox"/> <input type="text"/>
<input type="button" value="Apply"/>	

Figure 6 - 32 Reauthenticate Port(s) window (MAC-based 802.1X)

To reauthenticate ports, first choose the switch in the switch stack by using the pull-down menu and then choose the range of ports in the From and To field. Then the user must specify the MAC address to be reauthenticated by entering it into the MAC Address field and ticking the corresponding check box. To begin the reauthentication, click **Apply**.

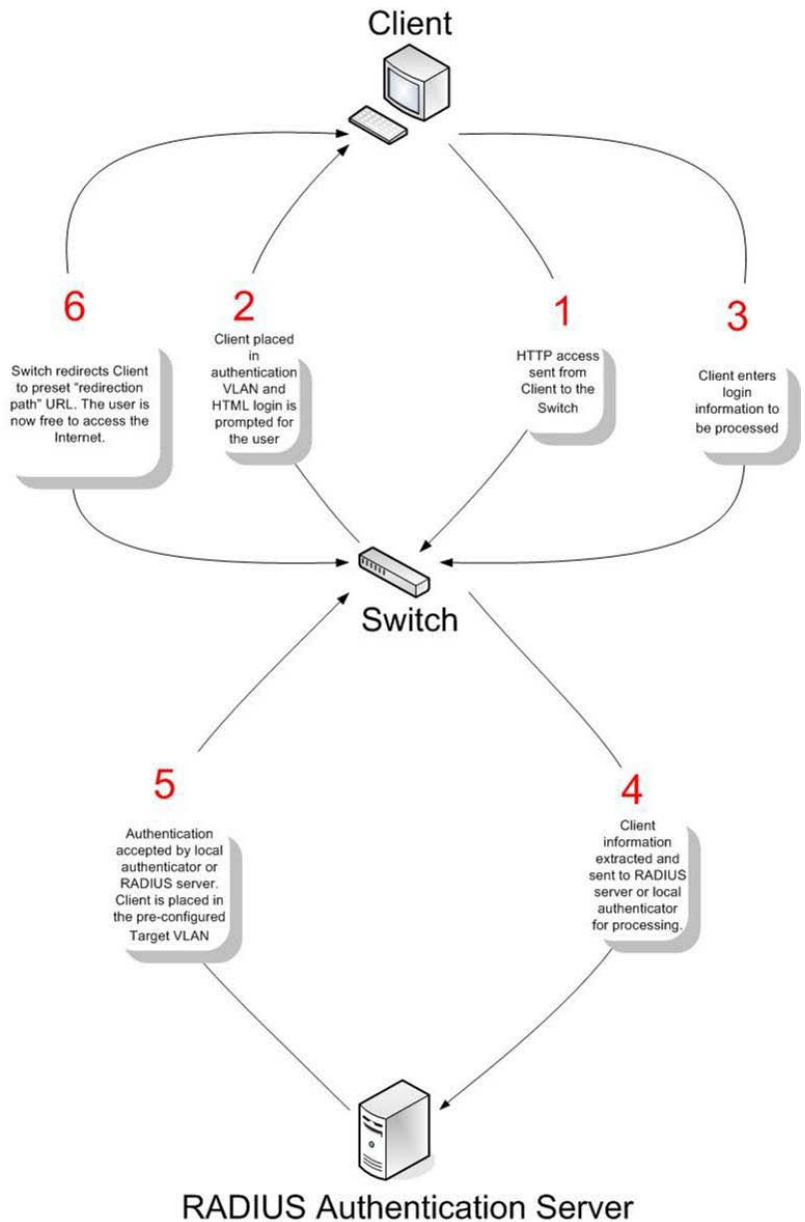
Web-based Access Control (WAC)

Web-Based Authentication Login is a feature designed to authenticate a user when the user is trying to access the Internet via the Switch.

The authentication process uses HTTP protocol. The switch enters the authenticating stage when users would like to browse web screen (Ex: <http://www.dlink.com>) through the web browser (Ex: IE). When the switch detects HTTP packets, and this port or host (host-based mode) is unauthenticated, the Switch will pop out username/password screen to query users. The user cannot access the Internet until passing the authentication process.

The Switch can be the authentication server itself, and perform the authentication based on a local database. The Switch also can be a RADIUS client and perform the authentication process via RADIUS protocol with a remote RADIUS server.

The client user initiates the authentication process of WAC via a Web access.



Conditions and Limitations

1. The subnet of the authentication VLAN's IP interface must be the same as that of the client. If not configured properly, the authentication will be permanently denied by the authenticator. It cannot be a Guest VLAN.
2. If the client is utilizing DHCP to attain an IP address, the authentication VLAN must provide a DHCP server or a DHCP relay function so that client may obtain an IP address.
3. The authentication VLAN of this function must be configured to access a DNS server to improve CPU performance, and allow the processing of DNS, UDP and HTTP packets.
4. Certain functions exist on the Switch that will filter HTTP packets, such as the Access Profile function. The user needs to be very careful when setting filter functions for the target VLAN, so that these HTTP packets are not denied by the Switch.
5. The Redirection Path must be set before the Web-based Access Control can be enabled. If not, the user will be prompted with an error message and the Web-based Access Control will not be enabled.
6. If a RADIUS server is to be used for authentication, the user must first establish a RADIUS Server with the appropriate parameters, including the target VLAN, before enabling the Web-based Access Control on the Switch.

WAC Global Settings

This window is used to enable and configure Web-based Access Control Global State on the Switch.

To view this window, click **Security > Web-based Access control (WAC) > WAC Global Settings**, as shown below.

Figure 6 - 33 WAC Global State window

The following parameters can be configured:

Parameter	Description
WAC Global State	Use this drop-down menu to either enable or disable WAC on the Switch.
WAC Settings	
Method	Use the drop-down menu to configure the Method, choose between Local or RADIUS. <i>Local</i> – Specifies that authentication will be done via the local database. <i>RADIUS</i> – Specifies that authentication will be done via the RADIUS server.
Redirection Path	Enter a redirection path that the client will be redirected to after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.
Virtual IP	Enter a virtual IPv4 address so that the TCP packets sent to the virtual IP will get a reply. If the virtual IP is enabled, the TCP packets sent to the virtual IP or physical IPIF's (IP Interface's) IP address will both get a reply. When the virtual IP is set to <i>0.0.0.0</i> the function will be disabled. To ensure that this function works correctly, the virtual IP address must not be configured to be an IP address that exists on the subnet.
Virtual IPv6	Enter a virtual IPv6 address so that the TCP packets sent to the virtual IP for IPv6 will get a reply. If the virtual IP for IPv6 is enabled, the TCP packets sent to the virtual IP or physical IPIF's IPv6 address will both get a reply. When the virtual IPv6 is set to <i>::</i> , the function is disabled. To ensure that this function works correctly, the virtual IPv6 address must not be

	configured to be an IPv6 address that exists on the subnet.
HTTP(S) Ports(1-65535)	<p>This function specifies the TCP port that will be used to identify the HTTP or HTTPS packets to be trapped to the CPU for the authentication process.</p> <p>Select either HTTP or HTTPS and enter the ports.</p> <p>HTTP – Specifies that the TCP port will run the WAC HTTP protocol. The default value is 80. HTTP port cannot run at TCP port 443.</p> <p>HTTPS – Specifies that the TCP port will run the WAC HTTPS protocol. The default value is 443. HTTPS cannot run at TCP port 80.</p> <p>If no protocol is specified the protocol used is HTTP.</p>
WAC Authorization Network Settings	
RADIUS Authorization	Specifies to <i>Enable</i> or <i>Disable</i> RADIUS Authorization.
Local Authorization	Specifies to <i>Enable</i> or <i>Disable</i> Local Authorization.

Click **Apply** to the implement changes.

WAC Port Settings

This window is used to enable and configure Web-based Access Control Port Settings on the Switch.

To view this window, click **Security > Web-based Access control (WAC) > WAC Port Settings**, as shown below.

WAC Port Settings							
Unit	From	To	State	Aging Time (1-1440 min)	Idle Time (1-1440 min)	Block Time (0-300 sec)	Apply
1	Port 1	Port 1	Disabled	1440 <input type="checkbox"/> Infinite	<input type="checkbox"/> Infinite <input checked="" type="checkbox"/> Infinite	60	Apply

WAC Port Table				
Port	State	Aging Time (min)	Idle Time (min)	Block Time (sec)
1	Disabled	1440	Infinite	60
2	Disabled	1440	Infinite	60
3	Disabled	1440	Infinite	60
4	Disabled	1440	Infinite	60
5	Disabled	1440	Infinite	60
6	Disabled	1440	Infinite	60
7	Disabled	1440	Infinite	60
8	Disabled	1440	Infinite	60
9	Disabled	1440	Infinite	60
10	Disabled	1440	Infinite	60
11	Disabled	1440	Infinite	60
12	Disabled	1440	Infinite	60
13	Disabled	1440	Infinite	60
14	Disabled	1440	Infinite	60
15	Disabled	1440	Infinite	60
16	Disabled	1440	Infinite	60
17	Disabled	1440	Infinite	60
18	Disabled	1440	Infinite	60
19	Disabled	1440	Infinite	60
20	Disabled	1440	Infinite	60
21	Disabled	1440	Infinite	60
22	Disabled	1440	Infinite	60
23	Disabled	1440	Infinite	60
24	Disabled	1440	Infinite	60

Figure 6 - 34 WAC Port Settings window

The following parameters can be configured:

Parameter	Description
Unit	Use the drop-down menu to select the unit you wish to configure.
From / To	Enter the range of ports you wish to configure.
State	<i>Enable</i> or <i>Disable</i> the WAC port settings on the specified ports.
Aging Time (1-1440 min)	This parameter specifies the period of time a host will keep in authenticated state after it succeeds to authenticate. Enter a value between 1 and 1440 minutes. The default setting is 1440 minutes. To maintain a constant Port Configuration tick the Infinite box in the WAC configuration window.
Idle Time (1-1440 min)	This parameter specifies the period of time during which there is no traffic for an authenticated host and the host will be moved back to the unauthenticated state. Enter a value between 1 and 1440 minutes. A value of Infinite indicates the Idle state of the authenticated host on the port will never be checked. The default setting is Infinite.

Block Time (0-300 sec)	This parameter specifies the period of time a host will keep in a blocked state after it fails to authenticate. Enter a value between 0 and 300 seconds. The default setting is 60 seconds.
-------------------------------	---

Click **Apply** to implement the changes.

WAC User Account

This window is used to enable and configure Web-based Access Control User Account Settings on the Switch.

To view this window, click **Security > Web-based Access control (WAC) > WAC User Account**, as shown below.

<input type="button" value="Add"/>				
Total Entries: 1				
WAC User Account				
User Name	Password	VID	Modify	Delete
RG	1	1	<input type="button" value="Modify"/>	<input type="button" value="X"/>

Figure 6 - 35 WAC User Account window

To create a new user account click **Add**, the following window will be displayed for the user to configure.

Create a New User Account

User Name	<input style="width: 90%;" type="text"/>
Password	<input style="width: 90%;" type="password"/>
Confirmation	<input style="width: 90%;" type="password"/>
VLAN Name	<input style="width: 90%;" type="text"/>
VID (1-4094)	<input style="width: 90%;" type="text"/>

[Show All WAC User Table Entries](#)

Figure 6 - 36 WAC User Account - Add window

To edit an entry click the corresponding **Modify** button, as shown below.

Figure 6 - 37 User Account Modify window

The following parameters can be configured:

Parameter	Description
User Name	Enter a user name for the new account.
Old Password	Enter the original password for the user. This field is case-sensitive and must be a complete alphanumeric string.
Password	Enter the new password for the user. This field is case-sensitive and must be a complete alphanumeric string.
Confirmation	Confirm the new password entered above. Entering a different password here from the one set above will result in a fail message.
VLAN Name	Enter a VLAN to be associated with the WAC account.
VID (1-4094)	Enter the VLAN ID to be associated with the WAC account.

Click **Apply** to implement the changes.

WAC Authentication State

This window is used to enable and configure Web-based Access Control Host Table Settings on the Switch.

To view this window, click **Security > Web-based Access control (WAC) > WAC Authentication State**, as shown below.

WAC Authentication State

Port List	<input type="text"/>	<input type="checkbox"/> Select All Ports
State	<input type="checkbox"/> Authenticated <input type="checkbox"/> Authenticating <input type="checkbox"/> Blocked	

WAC Authentication State Table

Port	MAC Address	Original RX VID	State	VID	Priority	Aging Time	Idle Time	Block Time	Clear
Total Authenticating Hosts: 0 Total Authenticated Hosts: 0 Total Blocked Hosts: 0									
Show All WAC Authentication State Entries									

Figure 6 - 38 WAC Host Table Settings window

The following parameters can be configured:

Parameter	Description
Port List	Enter the ports you wish to <i>Find</i> or <i>Delete</i> . Check the <i>All Ports</i> box to select all ports.
State	Select the state of the ports. Choose between <i>Authenticated</i> , <i>Authenticating</i> or <i>Blocked</i> .

Click **Find** to display the Host table entries or click **Delete** to remove an entry.

Trust Host

The Switch allows users to enter trusted host secure IP addresses and netmasks used for remote Switch management. It should be noted that if one or more trusted hosts are enabled, the Switch will immediately accept remote instructions from only the specified IP address or addresses. If you enable this feature, be sure to first enter the IP address of the station you are currently using.

To view this window, click **Security** > **Trust Host**, as shown below.

Security IP			
IP1 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP2 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP3 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP4 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP5 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP6 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP7 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP8 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP9 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP10 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP11 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP12 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP13 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP14 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP15 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP16 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP17 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP18 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP19 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP20 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP21 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP22 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP23 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP24 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP25 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP26 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP27 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP28 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP29 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>
IP30 Access to Switch	<input type="text" value="0.0.0.0"/>	Net Mask	<input type="text" value="0.0.0.0"/>

Note: Create a list of IP address that can access the switch. Your local host IP address must be one of the IP addresses to avoid disconnection.

Figure 6 - 39 Security IP window

To configure secure IP addresses for trusted host management of the Switch, type the IP address of the station you are currently using in the first field as well as up to three additional IP addresses of trusted hosts. Click the **Apply** button to assign trusted host status to the IP addresses. This goes into effect immediately. Click **Delete All** to remove all configured trusted hosts from this switch.

BPDU Attack Protection Settings

This window is used to configure the BPDU protection function for the ports on the Switch. In general, there are two states in BPDU protection function. One is the normal state, and another is the under attack state. The under attack state has three modes: drop, block, and shutdown. A BPDU protection-enabled port will enter under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on STP-disabled port. BPDU protection has high priority than FBPDU setting configured by configure STP command in determination of BPDU handling. That is, when FBPDU is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has high priority than BPDU tunnel port setting in determination of BPDU handling. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU.

To view this window, click **Security > BPDU Attack Protection Settings**, as shown below.

BPDU Attack Protection Global Settings

Global State	<input type="text" value="Disabled"/> <input type="button" value="v"/>
Trap State	<input checked="" type="radio"/> <input type="text" value="None"/> <input type="button" value="v"/>
Log State	<input type="radio"/> <input type="text" value="Both"/> <input type="button" value="v"/>
Recover Time (60-1000000)	<input type="text" value="60"/> <input type="text" value="sec"/> <input type="checkbox"/> Infinite

BPDU Attack Protection Port Settings

Unit	From	To	State	Mode	Apply
<input type="text" value="1"/> <input type="button" value="v"/>	<input type="text" value="Port 1"/> <input type="button" value="v"/>	<input type="text" value="Port 1"/> <input type="button" value="v"/>	<input type="text" value="Disabled"/> <input type="button" value="v"/>	<input type="text" value="Shutdown"/> <input type="button" value="v"/>	<input type="button" value="Apply"/>

BPDU Attack Protection Port Table

Port	State	Mode	Status
1	Disabled	Shutdown	Normal
2	Disabled	Shutdown	Normal
3	Disabled	Shutdown	Normal
4	Disabled	Shutdown	Normal
5	Disabled	Shutdown	Normal
6	Disabled	Shutdown	Normal
7	Disabled	Shutdown	Normal
8	Disabled	Shutdown	Normal
9	Disabled	Shutdown	Normal
10	Disabled	Shutdown	Normal
11	Disabled	Shutdown	Normal
12	Disabled	Shutdown	Normal
13	Disabled	Shutdown	Normal
14	Disabled	Shutdown	Normal
15	Disabled	Shutdown	Normal

Figure 6 - 40 BPDU Attack Protection Global Settings window

The following parameters can be configured:

Parameter	Description
Global State	Enable or disable the BPDU attack protection global state.
Trap State	Enable or disable the BPDU attack trap state.
Log State	Enable or disable the BPDU attack log state.
Recover Time (60-1000000)	Enter the BPDU protection Auto-Recovery recovery timer. The default value is 60. If Infinite is ticked, the port will not be auto recovered.
Unit	Select the unit to be configured.
From/To	Select the port or range of ports to be configured.
State	Enable or disable BPDU attack protection for the specified individual ports.
Mode	Select the BPDU attack protection mode: <i>Drop</i> , <i>Block</i> , or <i>Shutdown</i> . <i>Drop</i> - Drop all received BPDU packets when the port enters under_attack state. <i>Block</i> - Drop all packets (include BPDU and normal packets) when the port enters the under attack state. <i>Shutdown</i> - Shut down the port when the port enters the under attack state.

Click **Apply** to implement the changes.

ARP Spoofing Prevention Settings

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send fake or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or a random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

To prevent an ARP spoofing attack, Packet Content ACL is used to block the invalid ARP packets which contain a faked gateway's MAC and IP binding. Packet Content ACL can inspect any specified content in the first 48 bytes of a packet. It utilizes offsets to match individual fields in the Ethernet frame. An offset contains 16 bytes and each offset is divided into four 4-byte values in HEX format.

The configuration logic is as follows:

- The traffic can only pass through the Switch if the ARP entry matches a source MAC address in the Ethernet frame, the sender MAC address, or the sender IP address in the ARP protocol.
- The Switch will deny all other ARP packets which claim they are from the gateway's IP.

To view this window, click **Security > ARP Spoofing Prevention Settings**, as shown below.

Figure 6 - 41 ARP Spoofing Prevention Settings window

The following parameters can be configured:

Parameter	Description
Gateway IP Address	Enter the gateway IP address.
Gateway MAC Address	Enter the gateway MAC address.
Ports	Enter the port or range of ports to be configured. Alternatively, tick the All Ports check box to configure all of the ports.

Click **Apply** to implement the changes.

Access Authentication Control

The TACACS / XTACACS / TACACS+ / RADIUS commands allow users to secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

TACACS (Terminal Access Controller Access Control System) - Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.

Extended TACACS (XTACACS) - An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.

TACACS+ (Terminal Access Controller Access Control System plus) - Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called an Authentication Server Host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

The server verifies the username and password, and the user is granted normal user privileges on the Switch.

The server will not accept the username and password and the user is denied access to the Switch.

The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in Authentication Server Groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in Authentication Server Groups are used to authenticate users trying to access the Switch. The users will set Authentication Server Hosts in a preferable order in the built-in Authentication Server Groups and when a user tries to gain access to the Switch, the Switch will ask the first Authentication Server Hosts for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in Authentication Server Groups can only have hosts that are running the specified protocol. For example, the TACACS Authentication Server Groups can only have TACACS Authentication Server Hosts.

The administrator for the Switch may set up six different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its Authentication Server Hosts and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that users granted access to the Switch will be granted normal user privileges on the Switch. To gain access to administrator level privileges, the user must access the **Enable Admin** window and then enter a password, which was previously configured by the administrator of the Switch.



NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

Authentication Policy and Parameter Settings

This command will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the **Login Method List** and choose a technique for user authentication upon login.

To view this window, click **Security > Access Authentication Control > Authentication Policy and Parameter Settings**, as shown below.

Figure 6 - 42 Authentication Policy and Parameter Settings window

The following parameters can be set:

Parameter	Description
Authentication Policy	Use the pull-down menu to enable or disable the Authentication Policy on the Switch.
Response Timeout (0-255)	This field will set the time the Switch will wait for a response of authentication from the user. The user may set a time between 0 and 255 seconds. The default setting is 30 seconds.
User Attempts (1-255)	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet and web users will be disconnected from the Switch. The user may set the number of attempts from 1 to 255. The default setting is 3.

Click **Apply** to implement the changes.

Application's Authentication Settings

This window is used to configure switch configuration applications (console, Telnet, SSH, web) for login at the user level and at the administration level (**Enable Admin**) utilizing a previously configured method list.

To view this window, click **Security > Access Authentication Control > Application Authentication Settings**, as shown below.

Figure 6 - 43 Application Authentication Settings window

The following parameters can be set:

Parameter	Description
Application	Lists the configuration applications on the Switch. The user may configure the Login Method List and Enable Method List for authentication for users utilizing the Console (Command Line Interface) application, the Telnet application, SSH and the Web (HTTP) application.
Login Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Login Method Lists window, in this section, for more information.
Enable Method List	Using the pull-down menu, configure an application for normal login on the user level, utilizing a previously configured method list. The user may use the default Method List or other Method List configured by the user. See the Enable Method Lists window, in this section, for more information

Click **Apply** to implement the changes.

Authentication Server Group

This window will allow users to set up Authentication Server Groups on the Switch. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user-defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. The Switch has three built-in Authentication Server Groups that cannot be removed but can be modified. Up to eight authentication server hosts may be added to any particular group.

To view this window, click **Security > Access Authentication Control > Authentication Server Group**, as shown below.



Figure 6 - 44 Authentication Server Group window

This window displays the Authentication Server Groups on the Switch. The Switch has four built-in Authentication Server Groups that cannot be removed but can be modified. To modify a particular group, click its hyperlinked **Group Name**, which will then display the following window.

Figure 6 - 45 Add a Server Host to Server Group - XTACACS window

To add an Authentication Server Host to the list, enter its IP address in the IP Address field, choose the protocol associated with the IP address of the Authentication Server Host and click **Add to Group** to add this Authentication Server Host to the group. Click [Show All Server Group Entries](#) link to return to Authentication Server Group window.

To add a server group other than the ones listed, click the **Add** button, revealing the following window to configure.

Figure 6 - 46 Authentication Server Group Table Add Settings window

Enter a group name of up to 15 characters into the Group Name field and click **Apply**. The entry should appear in the Authentication Server Group Settings window. Click [Show All Server Group Table Entries](#) link to return to Authentication Server Group window.



NOTE: The user must configure Authentication Server Hosts using the Authentication Server Hosts window before adding hosts to the list. Authentication Server Hosts must be configured for their specific protocol on a remote centralized server before this function can work properly.



NOTE: The three built in server groups can only have server hosts running the same TACACS daemon. TACACS/XTACACS/TACACS+ protocols are separate entities and are not compatible with each other.

Authentication Server Host

This window will set user-defined Authentication Server Hosts for the TACACS / XTACACS / TACACS+ / RADIUS security protocols on the Switch. When a user attempts to access the Switch with Authentication Policy enabled, the Switch will send authentication packets to a remote TACACS / XTACACS / TACACS+ / RADIUS server host on a remote host. The TACACS / XTACACS / TACACS+ / RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS / XTACACS / TACACS+ / RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.

To view the following window, click **Security > Access Authentication Control > Authentication Server Host:**



Figure 6 - 47 Authentication Server Host window

To add an Authentication Server Host, click the **Add** button, revealing the following window:

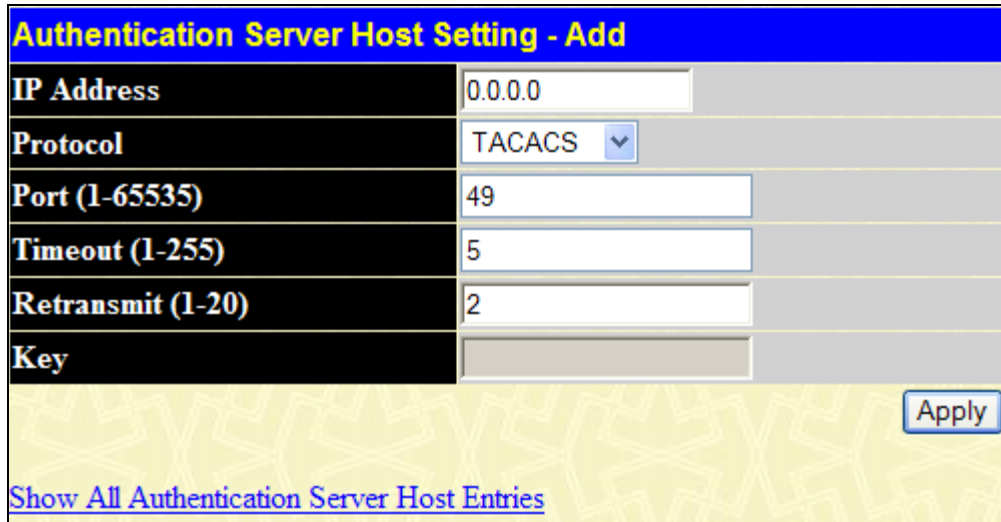


Figure 6 - 48 Authentication Server Host Setting - Add window

Configure the following parameters to add an Authentication Server Host:

Parameter	Description
IP Address	The IP address of the remote server host to add.
Protocol	The protocol used by the server host. The user may choose one of the following: <i>TACACS</i> - Enter this parameter if the server host utilizes the TACACS protocol. <i>XTACACS</i> - Enter this parameter if the server host utilizes the XTACACS protocol. <i>TACACS+</i> - Enter this parameter if the server host utilizes the TACACS+ protocol. <i>RADIUS</i> - Enter this parameter if the server host utilizes the RADIUS protocol.
Port (1-65535)	Enter a number between 1 and 65535 to define the virtual port number of the authentication protocol on a server host. The default port number is 49 for TACACS/XTACACS/TACACS+ servers and 1813 for RADIUS servers but the user may set a unique port number for higher security.
Timeout (1-255)	Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is 5 seconds.
Retransmit (1-20)	Enter the value in the retransmit field to change how many times the device will resend an authentication request.
Key	Authentication key to be shared with a configured TACACS+ or RADIUS servers only. Specify an alphanumeric string up to 254 characters.

Click **Apply** to add the server host.



NOTE: More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+ are separate entities and are not compatible with each other.

Login Method Lists

This command will configure a user-defined or default Login Method List of authentication techniques for users logging on to the Switch. The sequence of techniques implemented in this command will affect the authentication result. For example, if a user enters a sequence of techniques, for example TACACS - XTACACS- local, the Switch will send an authentication request to the first TACACS host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the local account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch.

Successful login using any of these techniques will give the user a “User” privilege only. If the user wishes to upgrade his or her status to the administrator level, the user must use the **Enable Admin** window, in which the user must enter a previously configured password, set by the administrator. (See the **Enable Admin** part of this section for more detailed information concerning the **Enable Admin** command.)

To view this window, click **Security > Access Authentication Control > Login Method Lists**, as shown below.

(Note: Maximum of 8 entries.)

Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local				<input type="checkbox"/>

Figure 6 - 49 Login Method Lists window

The Switch contains one Method List that is set and cannot be removed, yet can be modified. To delete a Login Method List defined by the user, click the under the Delete heading corresponding to the entry desired to be deleted. To modify a Login Method List, click its hyperlinked **Method List Name**. To configure a new Method List, click the **Add** button.

Both actions will result in the same screen to configure:

Method List Name	default
Method 1	local Keyword
Method 2	
Method 3	
Method 4	

[Show All Authentication Login Method List Entries](#)

Figure 6 - 50 Login Method List – Edit window (default)

Figure 6 - 51 Login Method List – Add window

To define a Login Method List, set the following parameters and click **Apply**:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Method 1, 2, 3, 4	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <p><i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p> <p><i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the TACACS+ protocol from a remote TACACS+ server.</p> <p><i>radius</i> – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p> <p><i>server_group</i> – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.</p> <p><i>local</i> – Adding this parameter will require the user to be authenticated using the local user account database on the Switch.</p> <p><i>none</i> – Adding this parameter will require no authentication to access the Switch.</p>

Click **Apply** to implement the changes. To return to the Login Method Lists window, click the [Show All Authentication Login Method List Entries](#) link.

Enable Method Lists

This window is used to set up Method Lists to promote users with user level privileges to Administrator (Admin) level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight Enable Method Lists can be implemented on the Switch, one of which is a default Enable Method List. This default Enable Method List cannot be deleted but can be configured.

The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like TACACS - XTACACS - Local Enable, the Switch will send an authentication request to the first TACACS host in the server group. If no verification is found, the Switch will send an authentication request to the second TACACS host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, XTACACS. If no authentication takes place using the XTACACS list, the Local Enable password set in the Switch is used to authenticate the user.

Successful authentication using any of these methods will give the user an “Admin” privilege.



NOTE: To set the Local Enable Password, see the next section, entitled Local Enable Password.

To view this window, click **Security > Access Authentication Control > Enable Method Lists**, as shown below.

<input type="button" value="Add"/>					
<i>(Note:Maximum of 8 entries.)</i>					
Enable Method Lists					
Method List Name	Method 1	Method 2	Method 3	Method 4	Delete
default	local_enable				<input type="button" value="X"/>

Figure 6 - 52 Enable Method Lists window

To delete an Enable Method List defined by the user, click the under the Delete heading corresponding to the entry desired to be deleted. To modify an Enable Method List, click its hyperlinked **Method List Name**. To configure a Method List, click the **Add** button.

Both actions will result in the same window to configure:

Enable Method List - Edit	
Method List Name	<input type="text" value="default"/>
Method 1	<input type="text" value="local_enable"/> Keyword
Method 2	<input type="text"/> ▼
Method 3	<input type="text"/> ▼
Method 4	<input type="text"/> ▼
<input type="button" value="Apply"/>	
Show All Authentication Enable List Entries	

Figure 6 - 53 Enable Method List - Edit window

Enable Method List - Add	
Method List Name	<input type="text"/>
Method 1	<input type="text" value="local_enable"/> ▼
Method 2	<input type="text"/> ▼
Method 3	<input type="text"/> ▼
Method 4	<input type="text"/> ▼
<input type="button" value="Apply"/>	
Show All Authentication Enable List Entries	

Figure 6 - 54 Enable Method List - Add window

To define an Enable Login Method List, set the following parameters:

Parameter	Description
Method List Name	Enter a method list name defined by the user of up to 15 characters.
Method 1, 2, 3, 4	<p>The user may add one, or a combination of up to four of the following authentication methods to this method list:</p> <p><i>local_enable</i> – Adding this parameter will require the user to be authenticated using the local enable password database on the Switch. The local enable password must be set by the user in the next section entitled Local Enable Password.</p> <p><i>none</i> – Adding this parameter will require no authentication to access the Switch.</p> <p><i>radius</i> – Adding this parameter will require the user to be authenticated using the RADIUS protocol from a remote RADIUS server.</p> <p><i>tacacs</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>xtacacs</i> – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server.</p> <p><i>tacacs+</i> – Adding this parameter will require the user to be authenticated using the TACACS protocol from a remote TACACS server.</p> <p><i>server_group</i> – Adding a previously configured server group will require the user to be authenticated using a user-defined server group previously configured on the Switch.</p>

Click **Apply** to implement the changes. To return to the Enable Method Lists window, click the [Show All Authentication Enable List Entries](#) link.

Configure Local Enable Password

This window will configure the locally enabled password for the **Enable Admin** command. When a user chooses the “local_enable” method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is locally set on the Switch.

To view this window, click **Security > Access Authentication Control > Configure Local Enable Password**, as shown below.

Figure 6 - 55 Configure Local Enable Password window

To set the Local Enable Password, set the following parameters and click **Apply**.

Parameter	Description
Old Local Enable	If a password was previously configured for this entry, enter it here in order to change it to a new password
New Local Enable	Enter the new password that you wish to set on the Switch to authenticate users attempting to access Administrator Level privileges on the Switch. The user may set a password of up to 15 characters.
Confirm Local Enable	Confirm the new password entered above. Entering a different password here from the one set in the New Local Enabled field will result in a fail message.

Click **Apply** to implement changes made.

Enable Admin

The **Enable Admin** window is for users who have logged on to the Switch on the normal user level, and wish to be promoted to the administrator level. After logging on to the Switch, users will have only user level privileges. To gain access to administrator level privileges, the user will open this window and will have to enter an authentication password. Possible authentication methods for this function include TACACS/XTACACS/TACACS+/RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because XTACACS and TACACS do not support the enable function, the user must create a special account on the server host, which has the username “enable”, and a password configured by the administrator that will support the “enable” function. This function becomes inoperable when the authentication policy is disabled.

To view this window, click **Security > Access Authentication Control > Enable Admin**, as shown below.

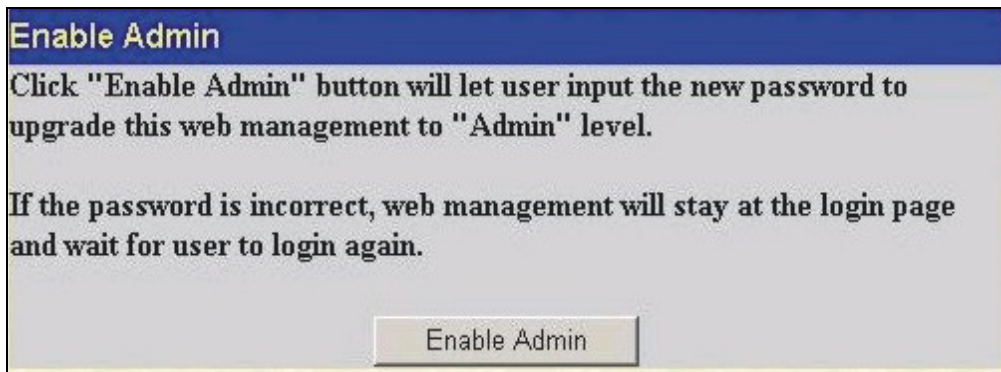


Figure 6 - 56 Enable Admin window

When this window appears, click the **Enable Admin** button revealing a window for the user to enter authentication (password, username). A successful entry will promote the user to Administrator level privileges on the Switch.

RADIUS Accounting Settings

The Accounting feature of the Switch uses a remote RADIUS server to collect information regarding events occurring on the Switch. The following is a list of information that will be sent to the RADIUS server when an event triggers the Switch to send these informational packets.

- Account Session ID
- Account Status Type
- Account Terminate Cause
- Account Authentic
- Account Delay Time
- Account Session Time
- Username
- Service Type
- NAS IP Address
- NAS Identifier
- Calling Station ID

There are three types of Accounting that can be enabled on the Switch.

Network – When enabled, the Switch will send informational packets to a remote RADIUS server when 802.1X users connect to the physical ports on the switch to access the network. Network accounting only works when 802.1X is enabled

Shell – When enabled, the Switch will send informational packets to a remote RADIUS server when a user either logs in, logs out or times out on the Switch, using the console, Telnet, or SSH.

System – When enabled, the Switch will send informational packets to a remote RADIUS server when system events occur on the Switch, such as a system reset or system boot.

Remember, this feature will not work properly unless a RADIUS Server has first been configured. This RADIUS server will format, store and manage the information collected here.

To view this window, click **Security > Access Authentication Control > RADIUS Accounting Settings**, as shown below.

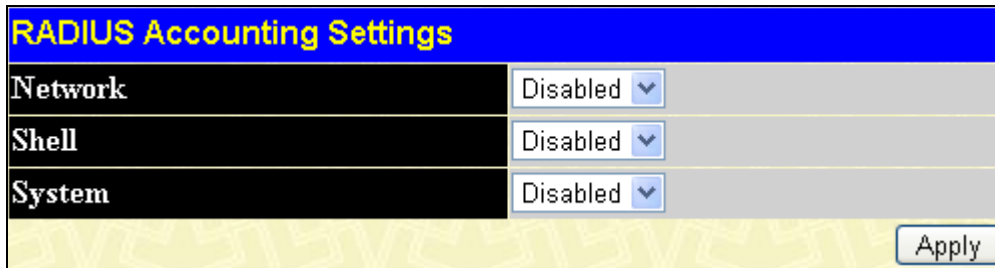


Figure 6 - 57 RADIUS Accounting Settings window

MAC-based Access Control (MAC)

The MAC-based Access Control feature will allow users to configure a list of MAC addresses, either locally or on a remote RADIUS server, to be authenticated by the Switch and given access rights based on the configurations set on the Switch of the target VLAN where these authenticated users are placed.

For local authentication on the Switch, the user must enter a list of MAC addresses to be accepted through this mechanism using the MAC-based Access Control Local Database Settings window, as seen below. The user may enter up to 1024 MAC addresses locally on the Switch. Once a MAC address has been authenticated by the Switch on the local side, the port where that MAC address resides will be placed in the previously configured target VLAN, where the rights and privileges are set by the switch administrator. If the VLAN Name for the target VLAN is not found by the Switch, the Switch will return the port containing that MAC address to the originating VLAN. If the MAC address is not found and the port is in the Guest VLAN, it will remain in the Guest VLAN, with the associated rights. If the port is not in the guest VLAN, this MAC address will be blocked by the Switch.

For remote RADIUS server authentication, the user must first configure the RADIUS server with a list of MAC addresses and relative target VLANs that are to be authenticated on the Switch. Once a MAC address has been discovered by the Switch, the Switch will then query the remote RADIUS server with this potential MAC address, using a RADIUS Access Request packet. If a match is made with this MAC address, the RADIUS server will return a notification stating that the MAC address has been accepted and is to be placed in the target VLAN. If the VID for the target VLAN is not found, the Switch will return the port containing the MAC address to the original VLAN. If the MAC address is not found, and if the port is in the Guest VLAN, it will remain in the Guest VLAN, with the associated rights. If the port is not in the guest VLAN, this MAC address will be blocked by the Switch.

Notes about MAC-based Access Control

There are certain limitations and regulations regarding the MAC-based Access Control:

1. Once this feature is enabled for a port, the Switch will clear the FDB of that port.
2. MAC-based Access Control is its own entity and is not dependant on other authentication functions on the Switch, such as 802.1X, Web-Based authentication etc.
3. Ports that have been enabled for Link Aggregation and Port Security cannot be enabled for MAC-based Authentication.
4. Ports that have been enabled for GVRP cannot be enabled for Guest VLAN.

MAC-based Access Control Global Settings

The following window is used to set the parameters for the MAC-based Access Control function on the Switch. Here the user can set the state, password, authentication method, as well as create, configure or delete Guest VLANs.

To view this window, click **Security > MAC-based Access Control > MAC-based Access Control Global Settings**, as shown below.

MAC-based Access Control Global Settings

State	Disabled <input type="button" value="v"/>
Method	Local <input type="button" value="v"/>
Password	default <input type="text"/>
Guest VLAN Name	<input type="text"/> <input checked="" type="radio"/>
Guest VLAN ID	<input type="text"/> <input type="radio"/>
Guest VLAN Member Ports	<input type="text"/>
Max User (1-4000)	1024 <input type="checkbox"/> No Limit

MAC-based Access Control Authorization Network Settings

Radius Authorization	Enabled <input type="button" value="v"/>
Local Authorization	Enabled <input type="button" value="v"/>

MAC-based Access Control Port Settings

Unit	From	To	State	Mode	Max User (1-4000)	Aging Time (1-1440 min)	Block Time (1-300 sec)	Apply
1 <input type="button" value="v"/>	Port 1 <input type="button" value="v"/>	Port 1 <input type="button" value="v"/>	Disabled <input type="button" value="v"/>	Port-based <input type="button" value="v"/>	128 <input type="checkbox"/> No Limit	1440 <input type="checkbox"/> Infinite	300 <input type="checkbox"/> Infinite	<input type="button" value="Apply"/>

MAC-based Access Control Port Table

Port	State	Aging Time	Block Time	Auth Mode	Max User
1	Disabled	1440	300	Host-based	1024
2	Disabled	1440	300	Host-based	1024
3	Disabled	1440	300	Host-based	1024
4	Disabled	1440	300	Host-based	1024
5	Disabled	1440	300	Host-based	1024
6	Disabled	1440	300	Host-based	1024
7	Disabled	1440	300	Host-based	1024
8	Disabled	1440	300	Host-based	1024
9	Disabled	1440	300	Host-based	1024
10	Disabled	1440	300	Host-based	1024
11	Disabled	1440	300	Host-based	1024
12	Disabled	1440	300	Host-based	1024
13	Disabled	1440	300	Host-based	1024
14	Disabled	1440	300	Host-based	1024
15	Disabled	1440	300	Host-based	1024
16	Disabled	1440	300	Host-based	1024
17	Disabled	1440	300	Host-based	1024
18	Disabled	1440	300	Host-based	1024
19	Disabled	1440	300	Host-based	1024
20	Disabled	1440	300	Host-based	1024
21	Disabled	1440	300	Host-based	1024
22	Disabled	1440	300	Host-based	1024
23	Disabled	1440	300	Host-based	1024
24	Disabled	1440	300	Host-based	1024

Figure 6 - 58 MAC-based Access Control Global Settings window

The following parameters may be viewed or set:

Parameter	Description
MAC-based Access Control Global Settings	
State	Use the pull-down menu to globally enable or disable the MAC-based Access Control function on the Switch.
Method	Use the pull-down menu to choose the type of authentication to be used when authentication MAC addresses on a given port. The user may choose between the following methods: <i>Local</i> – Use this method to utilize the locally set MAC address database as the authenticator for MAC-based Access Control. This MAC address list can be configured in the MAC-based Access Control Local Database Settings window. <i>RADIUS</i> – Use this method to utilize a remote RADIUS server as the authenticator for MAC-based Access Control. Remember, the MAC list must be previously set on the RADIUS server and the settings for the server must be first configured on the Switch.
Password	Enter the password for the RADIUS server, which is to be used for packets being sent requesting authentication. The default password is “default”.
Guest VLAN Name	Displays the name of the previously configured Guest VLAN being used for this function. Clicking the hyperlinked name will send the web manager to Guest VLAN configuration screen for MAC-based Authentication.
Guest VLAN ID	Displays the VLAN ID of the previously configured Guest VLAN being used for this function. Clicking the hyperlinked Guest VLAN ID will send the Web manager to Guest VLAN configuration window for MAC-based Authentication.
Guest VLAN Member Ports	Displays the list of ports that have been configured for the Guest VLAN.
Max User (1-4000)	Specifies to set the maximum number of authorized clients on the device. The default value is 1024. “No limit” means 4000, the maximum number of authenticated users on the device.
MAC-based Access Control Authorization Network Settings	
Radius Authorization	If <i>Enabled</i> , the authorized data assigned by the RADIUS server will be accepted when the global authorization network is enabled. The default state is <i>Enabled</i> .
Local Authorization	If <i>Enabled</i> , the authorized data assigned by the Local database will be accepted if the global authorization network is enabled. The default state is <i>Enabled</i> .
MAC-based Access Control Port Settings	
Unit	Choose the Switch ID number of the Switch in the switch stack to be modified.
From /To	Enter the Port range.
State	Use the pull-down menu to enable or disable the MAC-based Access Control function on individual ports.
Mode	<i>Port Based</i> : In this mode, if one of the attached hosts is successfully authorized, all hosts on the same port will be granted access to the network. If the port authorization fails, this port will continue authenticating. <i>Host Based</i> : In this mode, every user can individually authenticate and access the network.
Max User (1-4000)	Specifies per port maximum authenticated number of users. The default value is 1024.

Aging Time (1-1440 min)	Specifies a time period (configurable per port) between 1-1440 minutes, during which an authenticated host will stay in an authenticated state. When the aging time has expired, the host will be moved back to an unauthenticated state. When aging time is set to Infinite, it will disable the aging time.
Block Time (1-300sec)	If a host fails to pass the authentication it will be blocked for a period of time referred to as block time (per port configurable). During this time, this host can't proceed to the authenticating process (unless the user clears the database manually). As a result, this hold mechanism can prevent the switch from frequent authentication which consumes too much computing power.

Click **Apply** to implement changes made.

MAC-based Access Control Local MAC Settings

The following window is used to set a list of MAC addresses, along with their corresponding target VLAN, which will be authenticated for the Switch. Once a queried MAC address is matched in this table, it will be placed in the VLAN associated with it here. The switch administrator may enter up to 1024 MAC addresses to be authenticated using the local method configured here.

To view this window, click **Security > MAC-based Access Control > MAC-based Access Control Local MAC Settings**, as shown below.

Figure 6 - 59 MAC-based Access Control Local MAC Settings window

To add a MAC address to the local authentication list, enter the MAC address and the target VLAN name into their appropriate fields and click **Add**. To clear a VLAN click **Clear VLAN**. To change a MAC address or a VLAN in the list, click the corresponding **Modify** button. To delete an entry by MAC or VLAN, enter its parameters into the appropriate field and click **Delete By MAC** or **Delete By VLAN**. To find an entry by MAC or VLAN, enter its parameters into the appropriate fields and click **Find By MAC** or **Find By VLAN**.

Figure 6 - 60 MAC-based Access Control Local MAC Settings - Edit window

Safeguard Engine

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the switch load beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. The Safeguard Engine has two operating modes, which can be configured by the user, Strict and Fuzzy. In Strict mode, when the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter Exhausted mode. When in this mode, the Switch will drop all ARP and IP broadcast packets and packets from untrusted IP addresses for a calculated time interval. Every five seconds, the Safeguard Engine will check to see if there are too many packets flooding the Switch. If the threshold has been crossed, the Switch will initially stop all ingress ARP and IP broadcast packets and packets from untrusted IP addresses for five seconds. After another five-second checking interval arrives, the Switch will again check the ingress flow of packets. If the flooding has stopped, the Switch will again begin accepting all packets. Yet, if the checking shows that there continues to be too many packets flooding the Switch, it will stop accepting all ARP and IP broadcast packets and packets from untrusted IP addresses for double the time of the previous stop period. This doubling of time for stopping these packets will continue until the maximum time has been reached, which is 320 seconds and every stop from this point until a return to normal ingress flow would be 320 seconds. For a better understanding, examine the following example of the Safeguard Engine.

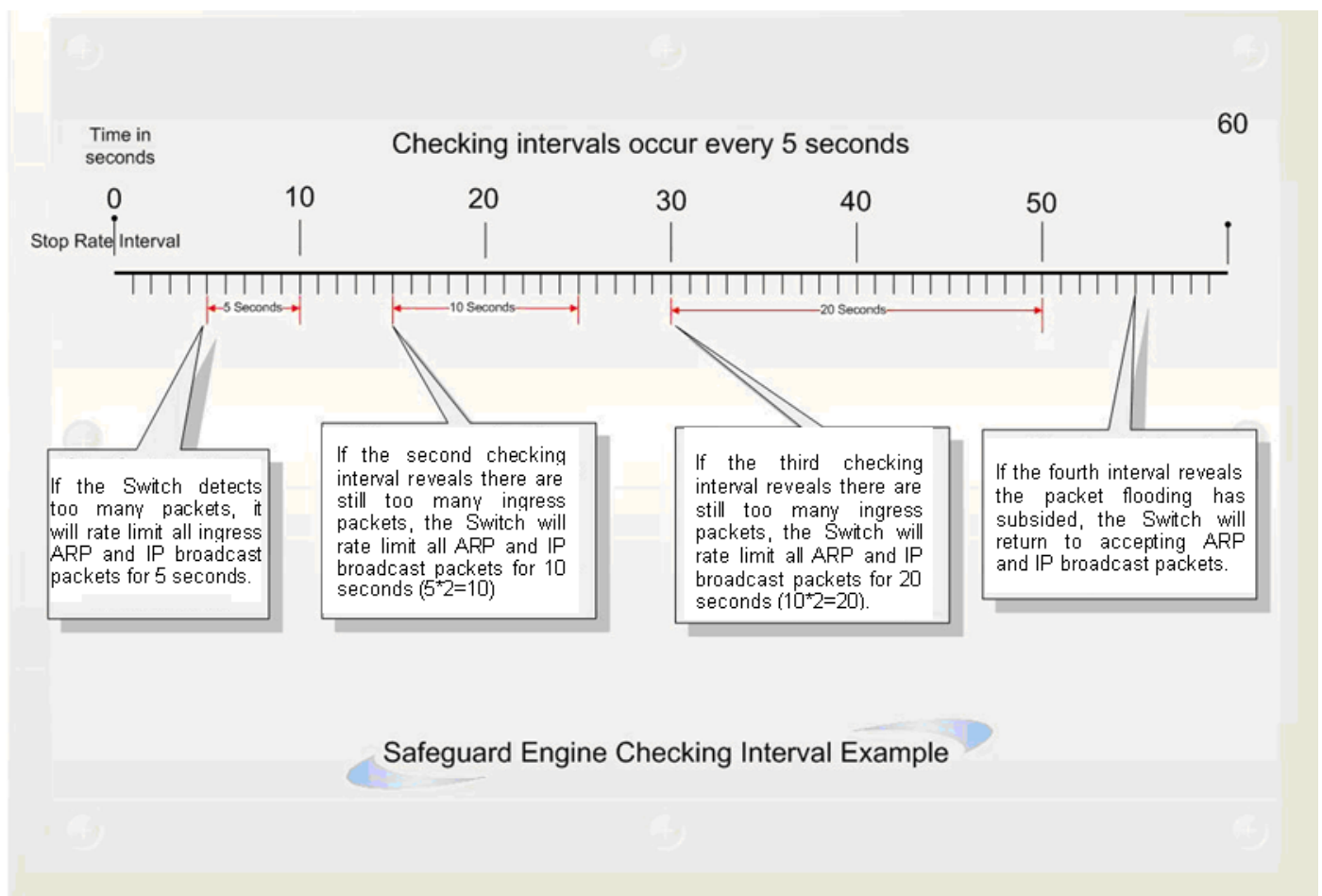


Figure 6 - 61 Safeguard Engine example

For every consecutive checking interval that reveals a packet flooding issue, the Switch will double the time it will discard ingress ARP and IP broadcast packets and packets from untrusted IP addresses. In the example above, the Switch doubled the time for dropping ARP and IP broadcast packets when consecutive flooding issues were detected at 5-second intervals. (First stop = 5 seconds, second stop = 10 seconds, third stop = 20 seconds) Once the flooding is no longer detected, the wait period for dropping ARP and IP broadcast packets will return to 5 seconds and the process will resume.

In Fuzzy mode, once the Safeguard Engine has entered the Exhausted mode, the Safeguard Engine will decrease the packet flow by half. After returning to Normal mode, the packet flow will be increased by 25%. The switch will then return to its interval checking and dynamically adjust the packet flow to avoid overload of the Switch.



NOTICE: When Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

Safeguard Engine Settings

This window is used to enable Safeguard Engine or configure advanced Safeguard Engine settings for the Switch.

To view this window, click **Security > Safeguard Engine > Safeguard Engine Settings**, as shown below.

Safeguard Engine Settings

State: Disabled

CPU Utilization Settings Apply

Developed by D-Link, the Safeguard Engine is a robust and innovative technology which will automatically reduce the negative impact of repeated packet flooding to the Switch's CPU. As a result, D-Link Switches will be better protected from frequent interruptions by malicious viruses or worm attacks.

Figure 6 - 62 1st Safeguard Engine Settings window

To enable the Safeguard Engine option, select *Enabled* with the drop-down State menu and click the **Apply** button.

To configure the advanced settings for the Safeguard Engine, click the **CPU Utilization Settings** button to view the following window.

Safeguard Engine Settings

State: Enabled

Apply

CPU Utilization Settings

Rising Threshold (20%-100%): 30

Falling Threshold (20%-100%): 20

Trap / Log: Disabled

Mode: Fuzzy

Safeguard Engine Current Status: normal mode

Developed by D-Link, the Safeguard Engine is a robust and innovative technology which will automatically reduce the negative impact of repeated packet flooding to the Switch's CPU. As a result, D-Link Switches will be better protected from frequent interruptions by malicious viruses or worm attacks.

Figure 6 - 63 2nd Safeguard Engine Settings window

The following parameters can be configured or viewed.

Parameter	Description
State	Use the pull-down menu to globally enable or disable Safeguard Engine settings for the Switch.
Rising Threshold (20%-100%)	Used to configure the acceptable level of CPU utilization before the Safeguard Engine mechanism is enabled. Once the CPU utilization reaches this percentage level, the Switch will move into Safeguard Engine state, based on the parameters provided in this window.
Falling Threshold (20%-100%)	Used to configure the acceptable level of CPU utilization as a percentage, where the Switch leaves the Safeguard Engine state and returns to normal mode.
Trap / Log	Use the pull-down menu to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate.
Mode	Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select: <i>Fuzzy</i> – If selected, this function will instruct the Switch to minimize the IP and ARP traffic

	<p>flow to the CPU by dynamically allotting an even bandwidth to all traffic flows.</p> <p><i>Strict</i> – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided.</p> <p>The default setting is Fuzzy mode.</p>
Safeguard Engine Current Status	Displays the current mode of the CPU Utilization Settings.

Click **Apply** to implement the changes.

Traffic Segmentation

Traffic segmentation is used to limit traffic flow from a single port to a group of ports. This method of segmenting the flow of traffic is similar to using VLANs to limit traffic, but is more restrictive. It provides a method of directing traffic that does not increase the overhead of the Master switch CPU.

To view this window, click **Security > Traffic Segmentation**, as shown below.

Unit	Port	Configuration	Setup
1	Port 1	View	Setup
Current Traffic Segmentation Table			
Unit	Port Map		
1	1-24		
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			

Figure 6 - 64 Current Traffic Segmentation Table window

Click the **Setup** button to open the **Setup Forwarding Ports** window, as shown below.

Setup Forwarding Ports																									
Unit-Port	1		Port 1																						
Forward Unit	1																								
Forward Port	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	-
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	-
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

[View Settings of Unit 1 Port 1](#)

Figure 6 - 65 Setup Forwarding Ports window

Configuring traffic segmentation on the xStack® DGS-3400 Series is accomplished in two parts. First, select a switch in the switch stack by using the Unit pull-down menu, and then specify a port from the switch, using the Port pull-down menu. Next, specify which ports on the switch that are able to receive packets from the switch and port specified in the first part.

Clicking the **Apply** button will enter the combination of transmitting port and allowed receiving ports into the Switch’s Traffic Segmentation table.

Secure Socket Layer (SSL)

Secure Sockets Layer or SSL is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a ciphersuite, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

- 1. Key Exchange:** The first part of the ciphersuite string specifies the public key algorithm to be used. This switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the DHE DSS Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they “exchange keys” in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
- 2. Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:

Stream Ciphers – There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.

CBC Block Ciphers – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.

- 3. Hash Algorithm:** This part of the ciphersuite allows the user to choose a message digest function, which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, MD5 (Message Digest 5) and SHA (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three-layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a certificate. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

SSL

This window is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions. Currently, all xStack® DGS-3400 Series switch come with a certificate pre-loaded though the user may need to download more, depending on user circumstances.

The configuration screen will allow the user to enable SSL on the Switch and implement any one or combination of listed ciphersuites on the Switch. A ciphersuite is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The Switch possesses four possible ciphersuites for the SSL function, which are all enabled by default. To utilize a particular ciphersuite, disable the unwanted ciphersuites, leaving the desired one for authentication.

When the SSL function has been enabled, the web will become disabled. To manage the Switch through the Web-based management while utilizing the SSL function, the Web browser must support SSL encryption and the header of the URL must begin with https://. (Ex. https://xx.xx.xx.xx) Any other method will result in an error and no access can be authorized for the Web-based management.

To view this window, click **Security > SSL**, as shown below.

The screenshot shows two stacked configuration windows. The top window, titled 'Download Certificate', has a blue header and contains the following fields: 'Certificate Type' (dropdown menu set to 'Local'), 'Server IP' (text input field containing '0.0.0.0'), 'Certificate File Name' (text input field), and 'Key File Name' (text input field). An 'Apply' button is located at the bottom right. Below these fields, a yellow message box states 'Current Certificate: Loaded with RSA Certificate!'. The bottom window, titled 'Configuration', also has a blue header and contains: 'SSL Status' (dropdown menu set to 'Disabled'), 'Cache Timeout (60-86400 sec)' (text input field containing '600'), and a 'Ciphersuite' section with four rows: 'RSA with RC4 128 MD5', 'RSA with 3DES EDE CBC SHA', 'DHE DSS with 3DES EDE CBC SHA', and 'RSA EXPORT with RC4 40 MD5'. Each row has a dropdown menu set to 'Enabled'. An 'Apply' button is at the bottom right.

Figure 6 - 66 Download Certificate window

To download certificates, set the following parameters:

Parameter	Description
Certificate Type	Select <i>Local</i> to specify certificate type.
Server IP	Enter the IPv4 address of the TFTP server where the certificate files are located.
Certificate File Name	Enter the path and the filename of the certificate file to download. This file must have a .der extension. (Ex. c:/cert.der)

Key File Name	Enter the path and the filename of the key file to download. This file must have a .der extension (Ex. c:/pkey.der)
Configuration	
SSL Status	Use the pull-down menu to enable or disable the SSL status on the switch. The default is <i>Disabled</i> .
Cache Timeout (60-86400 sec)	This field will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process. The default setting is 600 seconds.
Ciphersuite	
RSA with RC4 128 MD5	This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
RSA with 3DES EDE CBC SHA	This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
DHE DSS with 3DES EDE CBC SHA	This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.
RSA EXPORT with RC4 40 MD5	This ciphersuite combines the RSA Export key exchange and stream cipher RC4 encryption with 40-bit keys. Use the pull-down menu to enable or disable this ciphersuite. This field is <i>Enabled</i> by default.

Click **Apply** to implement the changes.



NOTE: Certain implementations concerning the function and configuration of SSL are not available on the Web-based management of this Switch and need to be configured using the command line interface.



NOTE: Enabling the SSL command will disable the web-based switch management. To log on to the Switch again, the header of the URL must begin with https://. Entering anything else into the address field of the Web browser will result in an error and no authentication will be granted.

Secure Shell (SSH)

SSH is an abbreviation of Secure Shell, which is a program allowing secure remote login and secure network services over an insecure network. It allows a secure login to remote host computers, a safe method of executing commands on a remote end node, and will provide secure encrypted and authenticated communication between two non-trusted hosts. SSH, with its array of unmatched security features is an essential tool in today's networking environment. It is a powerful guardian against numerous existing security hazards that now threaten network communications.

The steps required to use the SSH protocol for secure communication between a remote PC (the SSH client) and the Switch (the SSH server) are as follows:

1. Create a user account with admin-level access using the User Accounts window in the **Security Management** folder. This is identical to creating any other admin-level User Account on the Switch, including specifying a password. This password is used to logon to the Switch, once a secure communication path has been established using the SSH protocol.
2. Configure the User Account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **SSH User Authentication** window. There are three choices as to the method SSH will use to authorize the user, which are Host Based, Password and Public Key.

3. Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH client and the SSH server, using the **SSH Authentication Mode and Algorithm Settings** window.
4. Finally, enable SSH on the Switch using the **SSH Server Configuration** window.

After completing the preceding steps, a SSH Client on a remote PC can be configured to manage the Switch using a secure, in band connection.

SSH Server Configuration

The following window is used to configure and view settings for the SSH server.

To view this window, click **Security > SSH > SSH Server Configuration**, as shown below.

The screenshot shows two windows. The top window, titled "SSH Server Configuration", displays the following settings:

SSH Server Status	Disabled
Max Session	8
Connection Timeout (sec)	120
Auth. Fail	2
Session Rekeying	Never
Listened Port Number	22

The bottom window, titled "SSH Server Configuration Settings", shows the same parameters with input fields and dropdown menus:

SSH Server Status	Disablec	▼
Max Session (1-8)	8	
Connection Timeout (120-600)	120	Sec
Auth. Fail (2-20)	2	
Session Rekeying	Never	▼
Listened Port Number (1-65535)	22	

An "Apply" button is located at the bottom right of the settings window.

Figure 6 - 67 SSH Server Configuration Settings window

To configure the SSH server on the Switch, modify the following parameters:

Parameter	Description
SSH Server Status	Use the pull-down menu to enable or disable SSH on the Switch. The default is <i>Disabled</i> .
Max Session (1-8)	Enter a value between 1 and 8 to set the number of users that may simultaneously access the Switch. The default setting is 8.
Connection TimeOut (120-600)	Allows the user to set the connection timeout. The user may set a time between 120 and 600 seconds. The default setting is 120 seconds.
Auth. Fail (2-20)	Allows the Administrator to set the maximum number of attempts that a user may try to log on to the SSH Server utilizing the SSH authentication. After the maximum number of attempts has been exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. The number of maximum attempts may be set between 2 and 20. The default setting is 2.
Session Rekeying	This field is used to set the time period that the Switch will change the security shell encryptions by using the pull-down menu. The available options are <i>Never, 10 min, 30 min,</i>

	and 60 min. The default setting is <i>Never</i> .
Listened Port Number	Enter the virtual port number to be used with this feature. The common port number for SSH is 22.

Click **Apply** to implement the changes.

SSH Authentication Mode and Algorithm Settings

This window allows the configuration of the desired types of SSH algorithms used for authentication encryption. There are three categories of algorithms listed and specific algorithms of each may be enabled or disabled by using their corresponding pull-down menus. All algorithms are enabled by default.

To view the following window, click **Security > SSH > SSH Authentication Mode and Algorithm Settings**, as shown below.

SSH Authentication Mode and Algorithm Settings	
Password	Enabled ▾
Publickey	Enabled ▾
Host-based	Enabled ▾
Encryption Algorithm	
3DES-CBC	Enabled ▾
Blow-fish-CBC	Enabled ▾
AES128-CBC	Enabled ▾
AES192-CBC	Enabled ▾
AES256-CBC	Enabled ▾
ARC4	Enabled ▾
Cast128-CBC	Enabled ▾
Twofish128	Enabled ▾
Twofish192	Enabled ▾
Twofish256	Enabled ▾
Data Integrity Algorithm	
HMAC-SHA1	Enabled ▾
HMAC-MD5	Enabled ▾
Public Key Algorithm	
HMAC-RSA	Enabled ▾
HMAC-DSA	Enabled ▾
Apply	

Figure 6 - 68 SSH Authentication Mode and Algorithm Settings window

The following algorithms may be set:

Parameter	Description
Authentication Algorithm	
Password	This field may be <i>Enabled</i> or <i>Disabled</i> to choose if the administrator wishes to use a locally configured password for authentication on the Switch. This field is <i>Enabled</i> by

	default.
Public Key	This field may be <i>Enabled</i> or <i>Disabled</i> to choose if the administrator wishes to use a public key configuration set on a SSH server, for authentication. This field is <i>Enabled</i> by default.
Host-based	This field may be <i>Enabled</i> or <i>Disabled</i> to choose if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. This field is <i>Enabled</i> by default.
Encryption Algorithm	
3DES-CBC	Use the pull-down to enable or disable the Triple Data Encryption Standard encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Blow-fish CBC	Use the pull-down to enable or disable the Blowfish encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES128-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES192-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES192 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
AES256-CBC	Use the pull-down to enable or disable the Advanced Encryption Standard AES256 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
ARC4	Use the pull-down to enable or disable the Arcfour encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Cast128-CBC	Use the pull-down to enable or disable the Cast128 encryption algorithm with Cipher Block Chaining. The default is <i>Enabled</i> .
Twofish128	Use the pull-down to enable or disable the twofish128 encryption algorithm. The default is <i>Enabled</i> .
Twofish192	Use the pull-down to enable or disable the twofish192 encryption algorithm. The default is <i>Enabled</i> .
Twofish256	Use the pull-down to enable or disable the twofish256 encryption algorithm. The default is <i>Enabled</i> .
Data Integrity Algorithm	
HMAC-SHA1	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Secure Hash algorithm. The default is <i>Enabled</i> .
HMAC-MD5	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the MD5 Message Digest encryption algorithm. The default is <i>Enabled</i> .
Public Key Algorithm	
HMAC-RSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the RSA encryption algorithm. The default is <i>Enabled</i> .
HMAC-DSA	Use the pull-down to enable or disable the HMAC (Hash for Message Authentication Code) mechanism utilizing the Digital Signature Algorithm (DSA) encryption. The default is <i>Enabled</i> .

Click **Apply** to implement the changes.

SSH User Authentication Mode

The following windows are used to configure parameters for users attempting to access the Switch through SSH.

To view this window, click **Security > SSH > SSH User Authentication Mode**, as shown below.

(Note: Maximum of 8 entries.)

SSH User Authentication Mode			
User Name	Auth. Mode	Host Name	Host IP

Figure 6 - 69 SSH User Authentication Mode window

In the example above, the User Account “RG” has been previously set using the User Accounts window in the **Administration** folder. A User Account must be set in order to set the parameters for the SSH user. To configure the parameters for a SSH user, click the hyperlinked **User Name** in the **Current Accounts** window, which will reveal the following window to configure.

User Account Add Table	
User Name	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
Access Right	Admin <input type="button" value="v"/>
<input type="button" value="Apply"/>	
Show All User Account Entries	



NOTE: To set the **SSH User Authentication** parameters on the Switch, a User Account must be previously configured.

Figure 6 - 70 User Account Add Table window

Once a User Account has been configured, return to the SSH User Authentication window, which now displays the newly created account, as shown here.

(Note: Maximum of 8 entries.)

SSH User Authentication Mode			
User Name	Auth. Mode	Host Name	Host IP
RG	Password		

Figure 6 - 71 SSH User Authentication Mode window

To configure the SSH settings for this user, click its hyperlinked User Name which will display the following window to configure:

User Name	<input type="text" value="RG"/>
Auth. Mode	Password <input type="button" value="v"/>
Host Name	<input type="text"/>
Host IP	<input type="checkbox"/> <input type="text" value="0.0.0.0"/>
<input type="button" value="Apply"/>	
Show All User Authentication Entries	

Figure 6 - 72 SSH User Authentication Mode - Edit window

The user may set the following parameters:

Parameter	Description
User Name	Enter a User Name of no more than 15 characters to identify the SSH user. This User Name

	must be a previously configured user account on the Switch.
Auth. Mode	<p>The administrator may choose one of the following to set the authorization for users attempting to access the Switch.</p> <p><i>Host Based</i> – This parameter should be chosen if the administrator wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user.</p> <ul style="list-style-type: none"> • <i>Host Name</i> – Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. • <i>Host IP</i> – Enter the corresponding IP address of the SSH user. <p><i>Password</i> – This parameter should be chosen if the administrator wishes to use an administrator-defined password for authentication. Upon entry of this parameter, the Switch will prompt the administrator for a password, and then to re-type the password for confirmation.</p> <p><i>Public Key</i> – This parameter should be chosen if the administrator wishes to use the public key on a SSH server for authentication.</p>
Host Name	Enter an alphanumeric string of no more than 32 characters to identify the remote SSH user. This parameter is only used in conjunction with the <i>Host Based</i> choice in the Auth. Mode field.
Host IP	Enter the corresponding IP address of the SSH user. This parameter is only used in conjunction with the <i>Host Based</i> choice in the Auth. Mode field.

Click **Apply** to implement the changes.

Compound Authentication

Modern networks employ many authentication methods. The Compound Authentication methods supported by this Switch include 802.1X, MAC-based Access Control (MAC), Web-based Access Control (WAC), Japan Web-based Access Control (JWAC), and IP-MAC-Port Binding (IMPB). The Compound Authentication feature allows clients running different authentication methods to connect to the network using the same switch port.

The Compound Authentication feature can be implemented using one of the following modes:

Any (MAC, 802.1X, WAC or JWAC) Mode

In the diagram on the right, the Switch port has been configured to allow clients to authenticate using 802.1X, MAC, WAC, or JWAC. When a client tries to connect to the network, the Switch will try to authenticate the client using one of these methods and if the client passes, it will be granted access to the network.

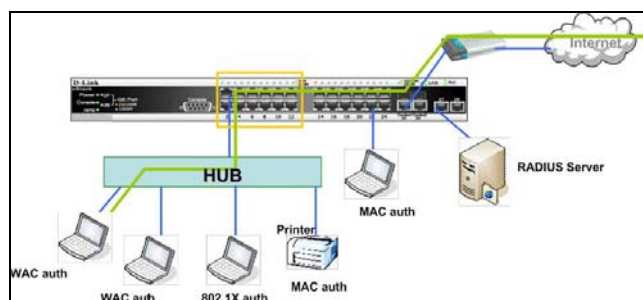


Figure 6 - 73 Any Mode – WAC example

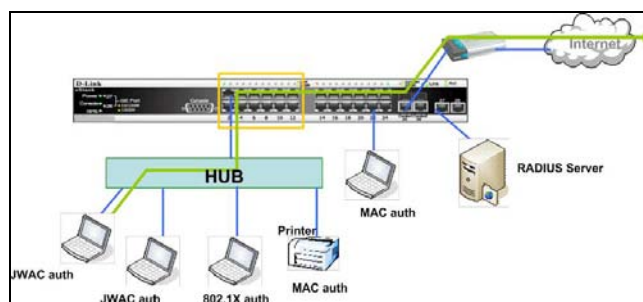


Figure 6 - 74 Any Mode – JWAC example

802.1X + IMPB Mode

This mode adds an extra layer of security by checking the IP MAC-Binding Port Binding (IMPB) table before trying one of the supported authentication methods. The IMPB Table is used to create a “white list” that checks if the IP streams being sent by authorized hosts have been granted or not. In the above diagram the Switch port has been configured to allow clients to authenticate using 802.1X. If the client is in the IMPB table and tries to connect to the network using this authentication method and the client is listed in the white list for legal IP/MAC/port checking, access will be granted. If a client fails one of the authentication methods, access will be denied.

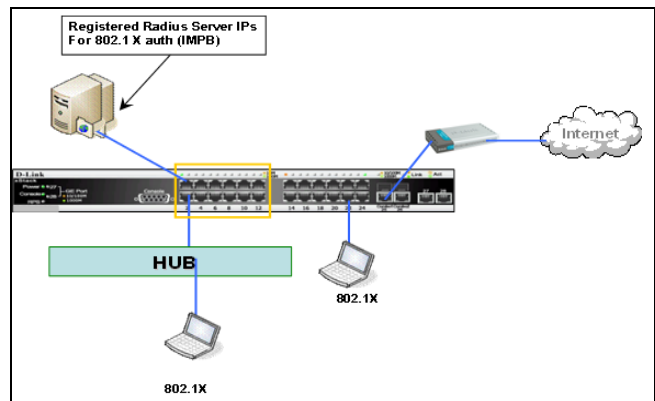


Figure 6 - 75 802.1X + IMPB Mode example

IMPB + JWAC Mode

This mode adds an extra layer of security by checking the IP MAC-Binding Port Binding (IMPB) table before trying one of the supported authentication methods. The IMPB Table is used to create a ‘white-list’ that checks if the IP streams being sent by authorized hosts have been granted or not. In the above diagram, the Switch port has been configured to allow clients to authenticate using either JWAC. If the client is in the IMPB table and tries to connect to the network using either of these supported authentication methods and the client is listed in the white list for legal IP/MAC/port checking, access will be granted. If a client fails one of the authentication methods, access will be denied.

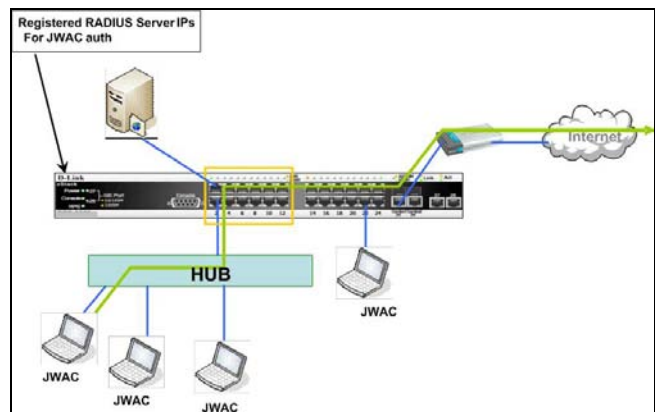


Figure 6 - 76 IMPB + JWAC Mode example

Compound Authentication Global Settings

To view this window, click **Security > Compound Authentication > Compound Authentication Global Settings**, as shown below.

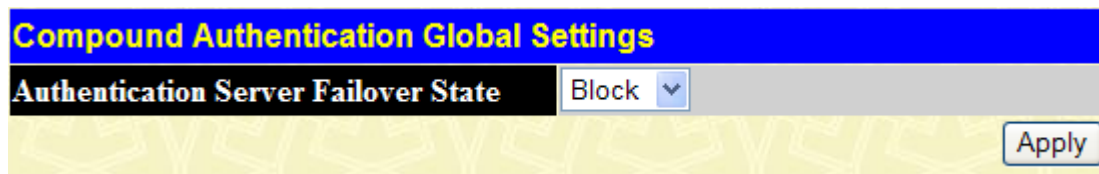


Figure 6 - 77 Compound Authentication Global Settings window

Use the pull-down menu to select the authentication server failover state.

Parameter	Description
Block	If <i>Block</i> is selected, the client is always regarded as an un-authenticated.
Local	If <i>Local</i> is selected, the Switch will resort to using the local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated. Otherwise, the client is regarded as an authenticated.

Permit	If <i>Permit</i> is selected, the client is always regarded as an authenticated. If the guest VLAN enabled, the client will stay at the guest VLAN, otherwise, it will stay at the original VLAN.
---------------	---

Click **Apply** to implement the changes.

Compound Authentication Settings

This window is used to configure the authorization mode and authentication method of individual ports.

To view this window, click **Security > Compound Authentication > Compound Authentication Settings**, as shown below.

Compound Authentication Settings							
Unit	From	To	Authorized Mode	Methods	VID List	State	Apply
1	Port 1	Port 1	Host-based	None		Disabled	Apply

Compound Authentication Table-Unit 1			
Port	Methods	Authorized Mode	Authentication VLAN(s)
1	None	Host-based	
2	None	Host-based	
3	None	Host-based	
4	None	Host-based	
5	None	Host-based	
6	None	Host-based	
7	None	Host-based	
8	None	Host-based	
9	None	Host-based	
10	None	Host-based	
11	None	Host-based	
12	None	Host-based	
13	None	Host-based	
14	None	Host-based	
15	None	Host-based	
16	None	Host-based	
17	None	Host-based	
18	None	Host-based	
19	None	Host-based	
20	None	Host-based	
21	None	Host-based	
22	None	Host-based	
23	None	Host-based	
24	None	Host-based	

Figure 6 - 78 Multiple Authentication Settings window

The following parameters may be set:

Parameter	Description
Unit	Choose the Unit ID of the switch in the switch stack you wish to configure.
From / To	Select a port or range of ports to be configured.
Authorized Mode	Use the drop down menu to select either <i>Port Based</i> or <i>Host Based</i> authorized mode. <i>Port Based</i> – If one of the attached hosts passes the authentication process, all host on the same port will be granted access to the network. If the user fails the authorization, this port will keep trying until the next authentication. <i>Host Based</i> – Each user can be authenticated individually.

Methods	<p><i>None</i> – Specifies that multiple authentication is not enabled.</p> <p><i>Any</i> – Specifies that a client will gain access if it passes any of the authentication methods (802.1X, MAC, or JWAC/WAC).</p> <p><i>802.1X+IMPB</i> – Specifies that 802.1X+IMPB can be enabled on a port at the same time. 802.1X will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. If either authentication method fails, the client will be denied access.</p> <p><i>IMPB+JWAC</i> – Specifies that JWAC and IMPB can be enabled on a port at the same time. JWAC will be verified first, and then IMPB will be verified. Both authentication methods need to be passed. If either authentication method fails, the client will be denied access.</p>
VID List	Enter a list of VLAN ID.
State	Use the pull-down menu to enable or disable the function.

Click **Apply** to implement the changes.

Authentication Guest VLAN Settings

This window is used to display and configure the Authentication Guest VLAN settings on the Switch.

To view this window, click **Security > Compound Authentication > Authentication Guest VLAN Settings**, as shown below.

Figure 6 - 79 Authentication Guest VLAN Settings window

To configure a new entry click the **Add** button, to reveal the following window:

Figure 6 - 80 Authentication Guest VLAN - Add window

The following parameters may be set:

Parameter	Description
VID / VLAN Name	Select either <i>VID</i> or <i>VLAN Name</i> and enter the appropriate information about a previously configured VLAN.
Port List (e.g.: 1, 6-9)	Enter the port or list of ports you wish to configure. Tick the All Ports check box to select all ports.
Action	Select the action you wish to apply to the Guest VLAN. Select <i>Add</i> to add a port to the Guest VLAN portlist or <i>Delete</i> to remove ports from the Guest VLAN portlist.

Click **Apply** to implement changes made.

Japanese Web-based Access Control (JWAC)

The **JWAC** folder contains six windows: **JWAC Global Configuration**, **JWAC Port Settings**, **JWAC User Account**, **JWAC Host Information**, **JWAC Customize Page Language Settings** and **JWAC Customize Page**.

JWAC Global Settings

Use this window to enable and configure Japanese Web-based Access Control on the Switch. Please note that JWAC and Web Authentication are mutually exclusive functions. That is, they cannot be enabled at the same time. To use the JWAC feature, computer users need to pass through the authentication process. For this, the authentication is similar to Web Authentication. The RADIUS server will share the server configuration defined by the 802.1X command set.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Global Settings**, as shown below.

JWAC Global Settings						
JWAC Global State	Disabled <input type="button" value="v"/>					
						<input type="button" value="Apply"/>
JWAC Settings						
Forcible Logout	Enabled <input type="button" value="v"/>					
UDP Filtering	Enabled <input type="button" value="v"/>					
RADIUS Protocol	PAP <input type="button" value="v"/>					
Redirect State	Enabled <input type="button" value="v"/>					
Redirect Destination	Quarantine Server <input type="button" value="v"/>					
Redirect Delay Time (0-10 sec)	1					
Virtual IP	0.0.0.0					
URL	<input type="text"/>					
HTTP(S) Port (1-65535)	80					<input checked="" type="radio"/> HTTP <input type="radio"/> HTTPS
						<input type="button" value="Clear URL"/> <input type="button" value="Apply"/>
JWAC Authorization Network Settings						
RADIUS Authorization	Enabled <input type="button" value="v"/>					
Local Authorization	Enabled <input type="button" value="v"/>					
						<input type="button" value="Apply"/>
Quarantine Server Settings						
Quarantine Server Monitor	Disabled <input type="button" value="v"/>					
Error Timeout (5-300 sec)	60					
Quarantine Server URL	<input type="text"/>					
						<input type="button" value="Apply"/>
Update Server Settings						
Update Server IP	<input type="text"/>					
Mask	<input type="text"/>					
Port (1-65535)	<input type="text"/>					<input checked="" type="radio"/> TCP <input type="radio"/> UDP
						<input type="button" value="Apply"/>
Update Server Table						
Index	IP Address	Mask	TCP/UDP	Port	State	Delete

Figure 6 - 81 JWAC Global State Configuration window

To set JWAC for the Switch, complete the following fields:

Parameter	Description
JWAC Global State Settings	
JWAC Global State	Use this drop-down menu to either enable or disable JWAC on the Switch.
JWAC Configuration	
Forcible Logout	This parameter enables or disables JWAC Forcible Logout. When Forcible Logout is <i>Enabled</i> , a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will move back to the unauthenticated state.
UDP Filtering	This parameter enables or disables JWAC UDP Filtering. When UDP Filtering is <i>Enabled</i> , all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped
RADIUS Protocol	This parameter specifies the RADIUS protocol used by JWAC to complete a RADIUS authentication. The options include <i>Local</i> , <i>EAP MD5</i> , <i>PAP</i> , <i>CHAP</i> , <i>MS CHAP</i> , and <i>MS CHAPv2</i> .
Redirect State	This parameter enables or disables JWAC Redirect. When the redirect quarantine server is enabled, the unauthenticated host will be redirected to the quarantine server when it tries to access a random URL. When the redirect JWAC login page is enabled, the unauthenticated host will be redirected to the JWAC login page in the Switch to finish authentication. When redirect is disabled, only access to the quarantine server and the JWAC login page from the unauthenticated host are allowed, all other web access will be denied. NOTE: When enabling redirect to the quarantine server, a quarantine server must be configured first.
Redirect Destination	This parameter specifies the destination before an unauthenticated host is redirected to either the <i>Quarantine Server</i> or the <i>JWAC Login Page</i> .
Redirect Delay Time (0-10 sec)	This parameter specifies the Delay Time before an unauthenticated host is redirected to the Quarantine Server or JWAC Login Page. Enter a value between 0 and 10 seconds. A value of 0 indicates no delay in the redirect.
Virtual IP	This parameter specifies the JWAC Virtual IP address that is used to accept authentication requests from an unauthenticated host. Only requests sent to this IP will get a correct response. NOTE: This IP does not respond to ARP requests or ICMP packets.
URL	Enter the URL of virtual IP. Clients can use this FQDN URL to access JWAC login page instead of the real Virtual IP.
HTTP(S) Port (1-65535)	This parameter specifies the TCP port that the JWAC Switch listens to and uses to finish the authentication process.
JWAC Authorization Network Configuration	
RADIUS Authorization	If <i>Enabled</i> , the authorized data assigned by the RADIUS server will be accepted when the global authorization attributes is enabled. The default state is <i>Enabled</i> .
Local Authorization	If <i>Enabled</i> , the authorized data assigned by the Local database will be accepted if the global authorization attributes is enabled. The default state is <i>Enabled</i> .
Quarantine Server Configuration	
Quarantine Server Monitor	This parameter enables or disables the JWAC Quarantine Server Monitor. When <i>Enabled</i> , the JWAC Switch will monitor the Quarantine Server to ensure the server is okay. If the Switch detects no Quarantine Server, it will redirect all unauthenticated HTTP access attempts to the JWAC Login Page forcibly if the Redirect is enabled and the Redirect Destination is configured to be a Quarantine Server.

Error Timeout (5-300 sec)	This parameter is used to set the Quarantine Server Error Timeout. When the Quarantine Server Monitor is enabled, the JWAC Switch will periodically check if the Quarantine works okay. If the Switch does not receive any response from the Quarantine Server during the configured Error Timeout, the Switch then regards it as not working properly. Enter a value between 5 and 300 seconds.
Quarantine Server URL	This parameter specifies the JWAC Quarantine Server URL. If the Redirect is enabled and the Redirect Destination is the Quarantine Server, when an unauthenticated host sends the HTTP request packets to a random Web server, the Switch will handle this HTTP packet and send back a message to the host to allow it access to the Quarantine Server with the configured URL. When a computer is connected to the specified URL, the quarantine server will request the computer user to input the user name and password to complete the authentication process.
Update Server Configuration	
Update Server IP	This parameter specifies the Update Server IP address.
Mask	This parameter specifies the Server IP net mask.
Ports (1-65535)	Enter the accessible port number and click the TCP or UDP radio button for the specified update server network.

Click **Apply** to implement the changes.

JWAC Port Settings

To view JWAC port settings for the Switch, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Port Settings**, which will open the following window:

Add

Unit 1

JWAC Port Table Parameter-Unit 1

Port	State	Mode	Max Authenticating Host	Aging Time (min)	Idle Time (min)	Block Time (sec)	Modify
1	Disabled	Host-based	50	1440	Infinite	60	Modify
2	Disabled	Host-based	50	1440	Infinite	60	Modify
3	Disabled	Host-based	50	1440	Infinite	60	Modify
4	Disabled	Host-based	50	1440	Infinite	60	Modify
5	Disabled	Host-based	50	1440	Infinite	60	Modify
6	Disabled	Host-based	50	1440	Infinite	60	Modify
7	Disabled	Host-based	50	1440	Infinite	60	Modify
8	Disabled	Host-based	50	1440	Infinite	60	Modify
9	Disabled	Host-based	50	1440	Infinite	60	Modify
10	Disabled	Host-based	50	1440	Infinite	60	Modify
11	Disabled	Host-based	50	1440	Infinite	60	Modify
12	Disabled	Host-based	50	1440	Infinite	60	Modify
13	Disabled	Host-based	50	1440	Infinite	60	Modify
14	Disabled	Host-based	50	1440	Infinite	60	Modify
15	Disabled	Host-based	50	1440	Infinite	60	Modify
16	Disabled	Host-based	50	1440	Infinite	60	Modify
17	Disabled	Host-based	50	1440	Infinite	60	Modify
18	Disabled	Host-based	50	1440	Infinite	60	Modify
19	Disabled	Host-based	50	1440	Infinite	60	Modify
20	Disabled	Host-based	50	1440	Infinite	60	Modify
21	Disabled	Host-based	50	1440	Infinite	60	Modify
22	Disabled	Host-based	50	1440	Infinite	60	Modify
23	Disabled	Host-based	50	1440	Infinite	60	Modify
24	Disabled	Host-based	50	1440	Infinite	60	Modify

Figure 6 - 82 JWAC Port Table Parameter window

To configure individual JWAC port settings, click the **Add** button, the following window will be displayed:

JWAC Port Settings	
Unit	1
Port List	From: Port 1 To: Port 1
State	Disabled
Mode	Host-based
Max Authenticating Host (0-50)	50
Aging Time (1-1440 min)	1440 <input type="checkbox"/> Infinite
Idle Time (1-1440 min)	<input checked="" type="checkbox"/> Infinite
Block Time (0-300 sec)	60
<input type="button" value="Apply"/>	
Show JWAC All Ports Setting Entries	

Figure 6 - 83 JWAC Port Table Parameter - Add window

To configure the settings by port, click the corresponding **Modify** button, which will display the following window:

JWAC Port Settings	
Unit	1
Port	1
State	Disabled
Mode	Host-based
Max Authenticating Host (0-50)	50
Aging Time (1-1440 min)	1440 <input type="checkbox"/> Infinite
Idle Time (1-1440 min)	<input checked="" type="checkbox"/> Infinite
Block Time (0-300 sec)	60
<input type="button" value="Apply"/>	
Show JWAC All Ports Setting Entries	

Figure 6 - 84 J JWAC Port Table Parameter - Edit window

To set the JWAC on individual ports for the Switch, complete the following fields:

Parameter	Description
Unit	Choose the Unit ID of the switch in the switch stack to configure.
Port List	Lists the range of Ports that will be configured in this window.
State	This parameter specifies the state of the configured ports.
Mode	Use the drop-down menu to select the mode, choose either <i>Port Based</i> or <i>Host Based</i> .
Max Authenticating Host (0-50)	This parameter specifies the maximum number of host process authentication attempts allowed on each port at the same time.
Aging Time (1-1440)	This parameter specifies the period of time a host will keep in authenticated state after it successes to authenticate. Enter a value between 1 and 1440 minutes. The default setting is

min)	1440 minutes. To maintain a constant Port Configuration, tick the Infinite check box.
Idle Time (1-1440 Minutes)	This parameter specifies the period of time during which there is no traffic for an authenticated host and the host will be moved back to the unauthenticated state. Enter a value between 1 and 1440 minutes. A value of Infinite indicates the Idle state of the authenticated host on the port will never be checked. The default setting is <i>Infinite</i> .
Block Time (0-300 sec)	This parameter specifies the period of time a host will keep in a blocked state after it fails to authenticate. Enter a value between 0 and 300 seconds. The default setting is 60 seconds.

Click **Apply** to implement changes made. To return to the JWAC Port Table Parameter window, click the [Show JWAN All Ports Setting Entries](#) link.

JWAC User Account

This window is used to configure JWAC user accounts on the Switch.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC User Account**, as shown below.

Add Clear All					
JWAC User Account					
Index	User Name	VID	Password	Modify	Delete
Total Entries: 0					

Figure 6 - 85 JWAC User Accounts window

To configure JWAC user settings, click the **Add** button, which will open the following window:

Create a New JWAC User Account	
User Name	<input type="text"/>
VID (1-4094)	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
Apply	
Show All JWAC User Account Entries	

Figure 6 - 86 JWAC User Accounts - Add window

The following fields can be configured:

Parameter	Description
User Name	Enter a username of up to 15 alphanumeric characters.
VID (1-4094)	Enter the VLAN ID of the Account you wish to create.
New Password	Enter the password of the user. This field is case-sensitive and must be a complete alphanumeric string.
Confirm New Password	Retype the password entered in the previous field.

Click **Apply** to implement changes made.

To view JWAC user settings for the Switch, click the [Show All JWAC User Account Entries](#) link, to view the following window:

<input type="button" value="Add"/> <input type="button" value="Clear All"/>					
JWAC User Account					
Index	User Name	VID	Password	Modify	Delete
1	GR	1	gr	<input type="button" value="Modify"/>	<input type="button" value="X"/>
Total Entries: 1					

Figure 6 - 87 JWAC User Accounts window

To add another JWAC user account to the Switch, click the **Add** button, to clear all the existing entries, click the **Clear All** button. To modify a JWAC user account, click the corresponding **Modify** button, which will open the following window:

Modify the JWAC User Account	
User Name	GR
VID (1-4094)	<input type="text"/>
Old Password	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/>
<input type="button" value="Apply"/>	
Show All JWAC User Account Entries	

Figure 6 - 88 JWAC User Accounts - Edit window

The following fields can be configured:

Parameter	Description
VID (1-4094)	Enter the VLAN ID of the Account you wish to create.
Old Password	Enter the original password of the user. This field is case-sensitive and must be a complete alphanumeric string.
New Password	Enter a new password of the user. This field is case-sensitive and must be a complete alphanumeric string.
Confirm New Password	Retype the new password entered in the previous field.

Click **Apply** to implement changes made. Click the [Show All JWAC User Account Entries](#) link to return to JWAC User Accounts window.

JWAC Authentication State

The JWAC host information Table allows the user to show or delete the hosts, which are handling or have been handled by the switch.

To view the following window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Authentication State**, as shown below.

JWAC Authentication State

Port List Select All Ports

State Authenticated Authenticating Blocked

JWAC Authentication State Table

Port	MAC Address	User Name	IP Address	State	VID	Priority	Age Time	Block Time	Idle Time	Clear
Total Authenticating Hosts: 0										
Total Authenticated Hosts: 0										
Total Blocked Hosts: 0										

[Show All JWAC Authentication State Entries](#)

Figure 6 - 89 JWAC Authentication State Table window

To search for Hosts, enter the Port list information and click the **Search** button. To clear an entry, enter the Port list information and click the **Delete** button.

JWAC Customize Page Language Settings

This window is used to customize your JWAC language settings on the Switch. Use the drop down menu to select either English or Japanese and click **Apply**.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page Language Settings**, as shown below.

JWAC Customize Page Language Settings

Customize Page Language

Figure 6 - 90 JWAC Customize Page Language Settings window

JWAC Customize Page

This window is used to customize fields in the JWAC Customize page.

To view this window, click **Security > Japanese Web-based Access Control (JWAC) > JWAC Customize Page**, as shown below.

English Japanese

Current Status: **Un-Authenticated**

Authentication Login	
User Name	<input type="text"/>
Password	<input type="password"/>
Enter Clear	

Logout From The Netwc	
Logout	

Notification Line 1	<input type="text"/>
Notification Line 2	<input type="text"/>
Notification Line 3	<input type="text"/>
Notification Line 4	<input type="text"/>
Notification Line 5	<input type="text"/>

Set to default Apply

Figure 6 - 91 JWAC Customize Page window

Enter the new information and click **Apply**.

Monitoring

- Device Status*
- Stacking Information*
- Stacking Device*
- Module Information*
- DRAM & Flash Utilization*
- CPU Utilization*
- Port Utilization*
- Packets*
- Errors*
- Packet Size*
- Browse Router Port*
- Browse MLD Router Port*
- VLAN Status*
- VLAN Status Port*
- Port Access Control*
- MAC Address Table*
- IGMP Snooping Group*
- IGMP Snooping Data Driven Group*
- MLD Snooping Group*
- MLD Snooping Data Driven Group*
- Trace Route*
- Switch Logs*
- Browse ARP Table*
- Session Table*
- IP Forwarding Table*
- Routing Table*
- MAC-based Access Control Authentication Status*

Device Status

This window displays the status of the physical attributes of the Switch, including power sources and fans.

To view this window, click **Monitoring > Device Status**, as shown below.

Device Status						
ID	Internal Power	External Power	Left Fan	Right Fan	Back Fan	CPU Fan
1	Active	Fail	OK	OK	OK	---

Figure 7 - 1 Device Status window

The following fields may be viewed in this window:

Parameter	Description
ID	Specifies the Switch in the Switch Stack that is being displayed.
Internal Power	Displays Active if the internal power supply is powering the system.
External Power (RPS)	Displays Active if the RPS is powering the system.
Left Fan	Displays the status of the Left Fans.
Right Fan	Displays the status of the Right Fans.
Back Fan	Displays the status of the Back Fans.
CPU Fan	Displays the status of the CPU Fans.

Stacking Information

To change a switch's default stacking configuration (for example, the order in the stack), see **Box Information** in the **Configuration** folder.

The number of switches in the switch stack (up to 12 total) are displayed in the upper right-hand corner of your web-browser. The icons are in the same order as their respective Unit numbers, with the Unit 1 switch corresponding to the icon in the upper left-most corner of the icon group.

When the switches are properly interconnected through their optional Stacking Modules, information about the resulting switch stack is displayed under the **Stack Information** link.

To view this window, click **Monitoring > Stacking Information**, as shown below.

Stacking Information								
Box ID	User Set	Type	Exist	Priority	MAC Address	PROM Version	Runtime Version	H/W Version
1	Auto	DGS-3426P	Exist	32	00-21-91-53-3E-C8	1.00-B13	2.70.B43	A1
2	---	Not_Exist	No					
3	---	Not_Exist	No					
4	---	Not_Exist	No					
5	---	Not_Exist	No					
6	---	Not_Exist	No					
7	---	Not_Exist	No					
8	---	Not_Exist	No					
9	---	Not_Exist	No					
10	---	Not_Exist	No					
11	---	Not_Exist	No					
12	---	Not_Exist	No					

Topology :	Duplex Chain
My Box ID :	1
Master ID :	1
Box Count :	1
Force Master Role :	Disabled

Figure 7 - 2 Stacking Information window

The **Stacking Information** window displays the following information:

Parameters	Description
Box ID	Displays the Switch's order in the stack.
User Set	Box ID can be assigned automatically (Auto), or can be assigned statically. The default is Auto .
Type	Displays the model name of the corresponding switch in a stack.

Exist	Denotes whether a switch does or does not exist in a stack.
Priority	Displays the priority ID of the Switch. The lower the number, the higher the priority. The box (switch) with the lowest priority number in the stack denotes the Primary Master switch.
MAC Address	Displays the MAC address of the corresponding switch in the switch stack.
PROM Version	Shows the PROM in use for the Switch. This may be different from the values shown in the illustration.
Runtime Version	Shows the firmware version in use for the Switch. This may be different from the values shown in the illustrations.
H/W Version	Shows the hardware version in use for the Switch. This may be different from the values shown in the illustration.
Topology	Show the current topology employed using this Switch.
My Box ID	Displays the Box ID of the Switch currently in use.
Master ID	Displays the Unit ID number of the Primary Master of the Switch stack.
Backup Master	Displays the Unit ID of the Backup Master of the switch stack.
Box Count	Displays the number of switches in the switch stack.

Stacking Device

This window is used to display the current devices in the Switch Stack.

To view this window, click **Monitoring > Stacking Device**, as shown below.

Stacking Device			
Box ID	Box Type	H/W Version	Serial Number
1	DGS-3426P	A1	P1F8193000001

Figure 7 - 3 Stacking Device window

Module Information

This window displays information about any installed modules.

To view this window, click **Monitoring > Module Information**, as shown below.

Module Information					
Box ID	ID	Module Name	Rev. No.	Serial	Description
1	1	-	-	-	-
1	2	-	-	-	-

Figure 7 - 4 Module Information window

Module information displayed:

Parameter	Description
ID	The slot number where the module is installed.

Module Name	The full name of the module installed.
Rev. No.	The version of the installed module.
Serial	The serial number of the module.
Description	A brief description of the type of module.

DRAM & Flash Utilization

This window is used to display DRAM and Flash utilization information.

To view this window, click **Monitoring > DRAM & Flash Utilization**, as shown below.

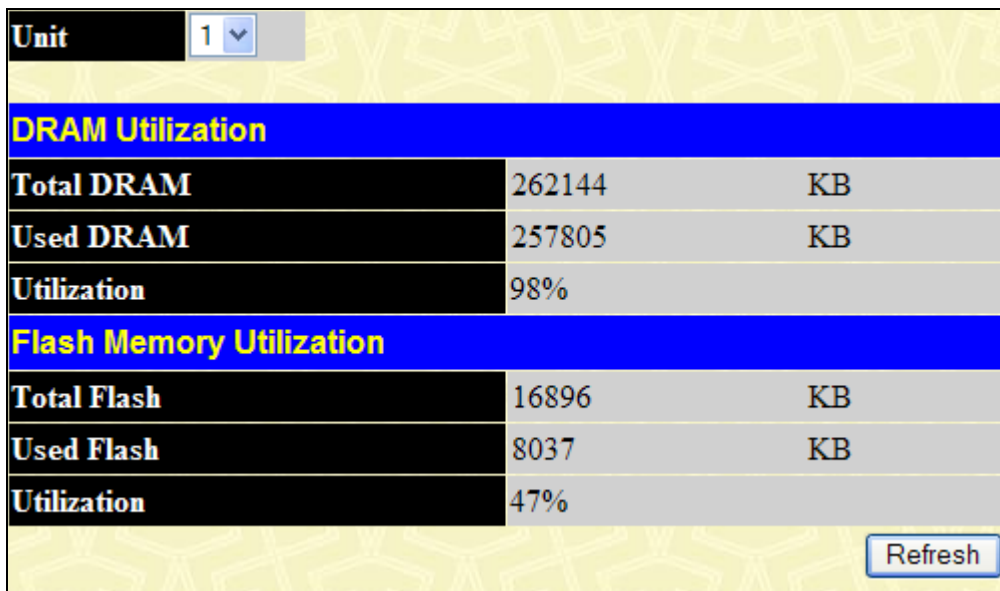


Figure 7 - 5 DRAM Utilization window

CPU Utilization

This window displays the percentage of the CPU being used, expressed as an integer percentage and calculated as a simple average by time interval.

To view this window, click **Monitoring > CPU Utilization**, as shown below.

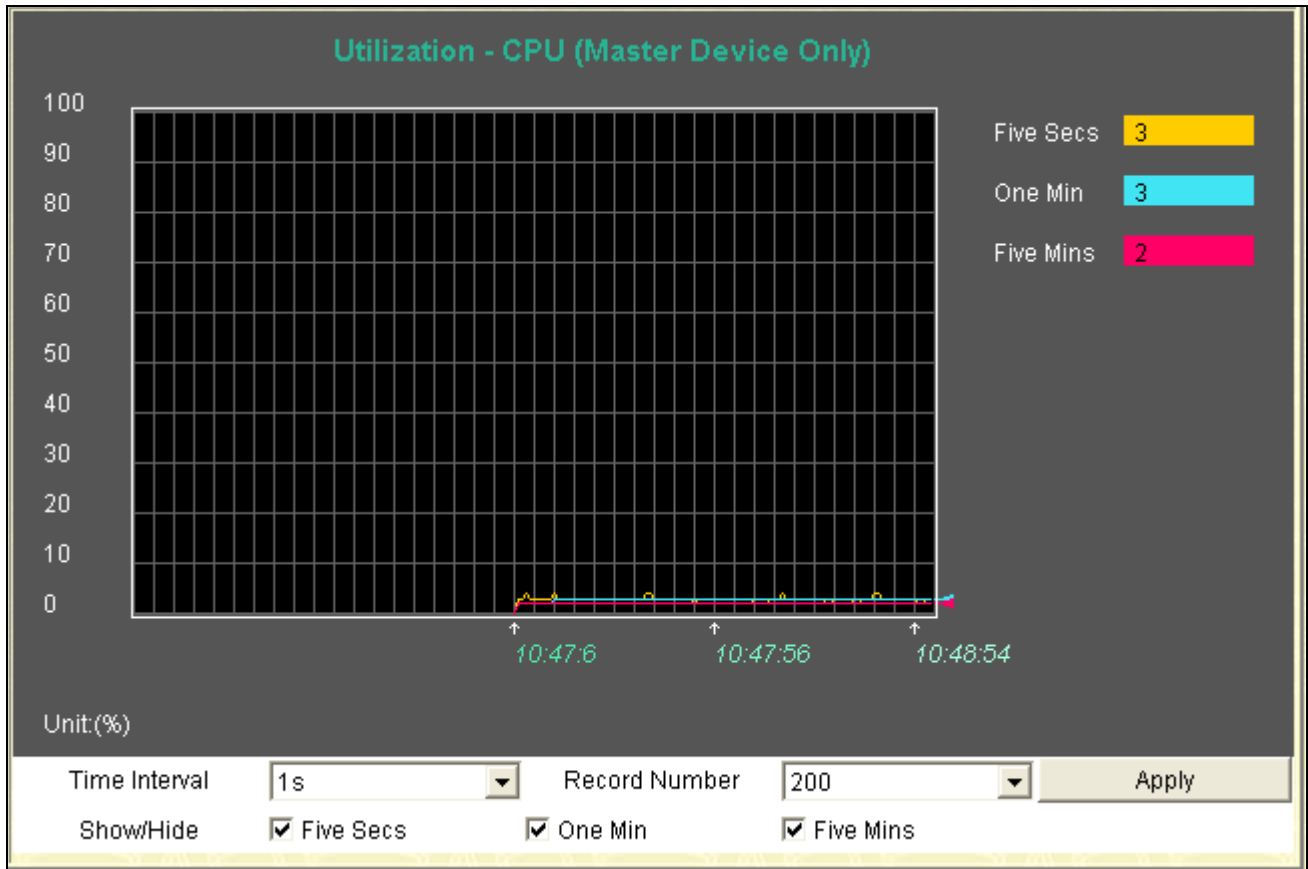


Figure 7 - 6 CPU Utilization graph

To view the CPU utilization by port, use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port. Click **Apply** to implement the configured settings. The window will automatically refresh with new updated statistics.

Change the view parameters as follows:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Port Utilization

This window displays the percentage of the total available bandwidth being used on the port.

To view this window, click **Monitoring > Port Utilization**, as shown below.

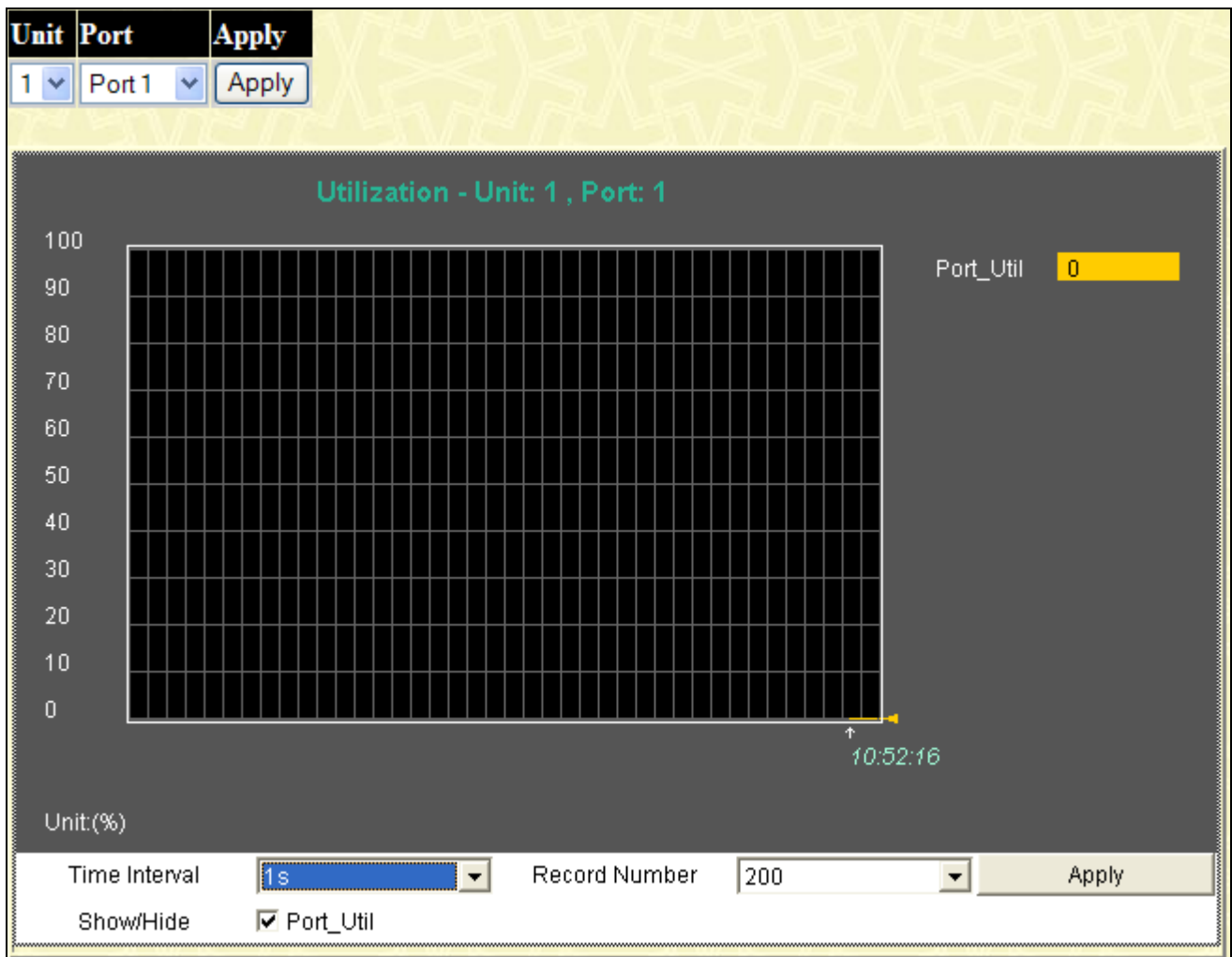


Figure 7 - 7 Port Utilization window

To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

Change the view parameters as follows:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.

Packets

The Web Manager allows various packet statistics to be viewed as either a line graph or a table. Six windows are offered.

Received (RX)

This window displays the following graph of packets received on the Switch. To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the window by simply clicking on a port.

To view this window, click **Monitoring > Packets > Received (RX)**, as shown below.

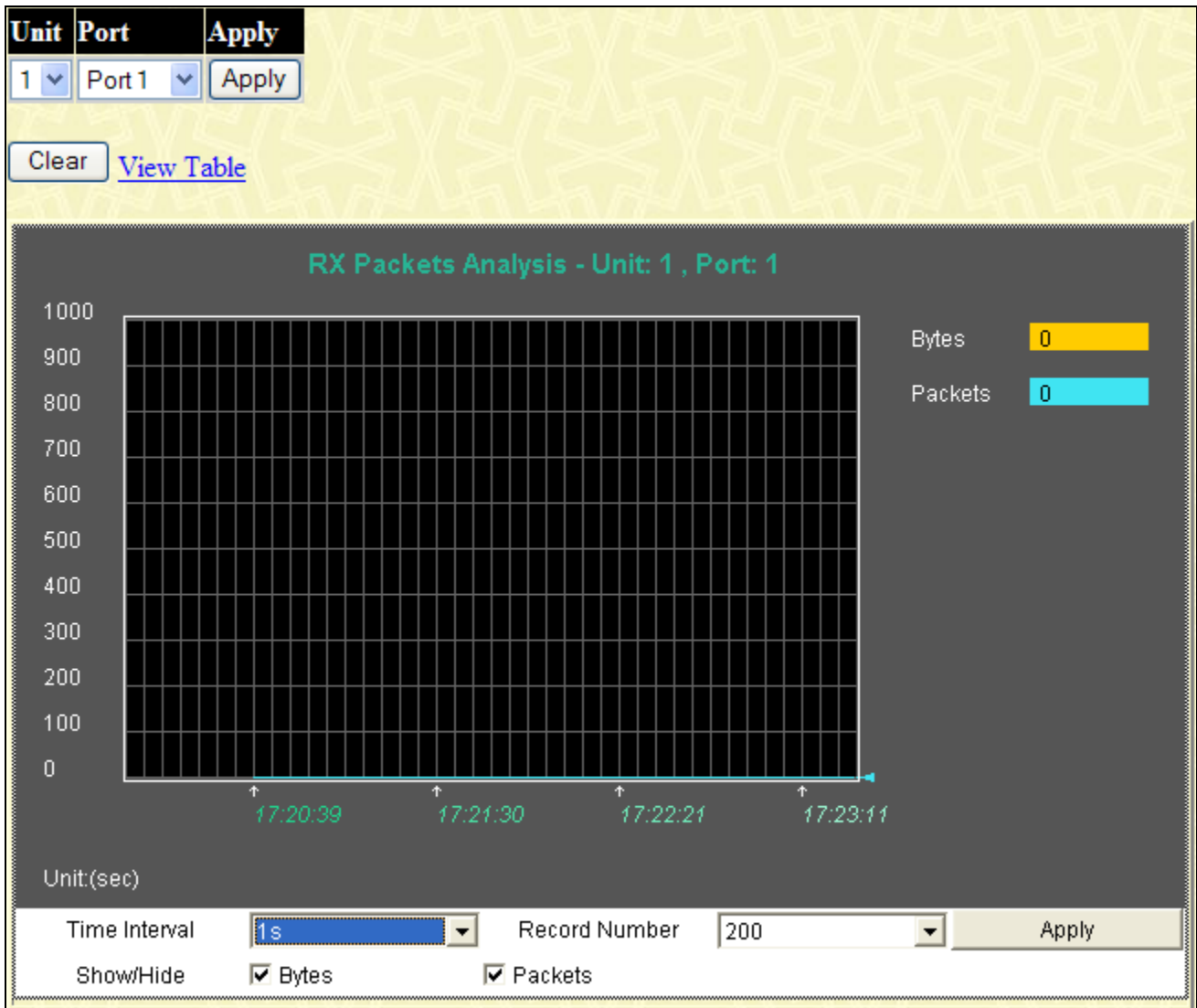


Figure 7 - 8 RX Packets Analysis (line graph for Bytes and Packets)

To view the **Received Packets Table** window, click the link [View Table](#).

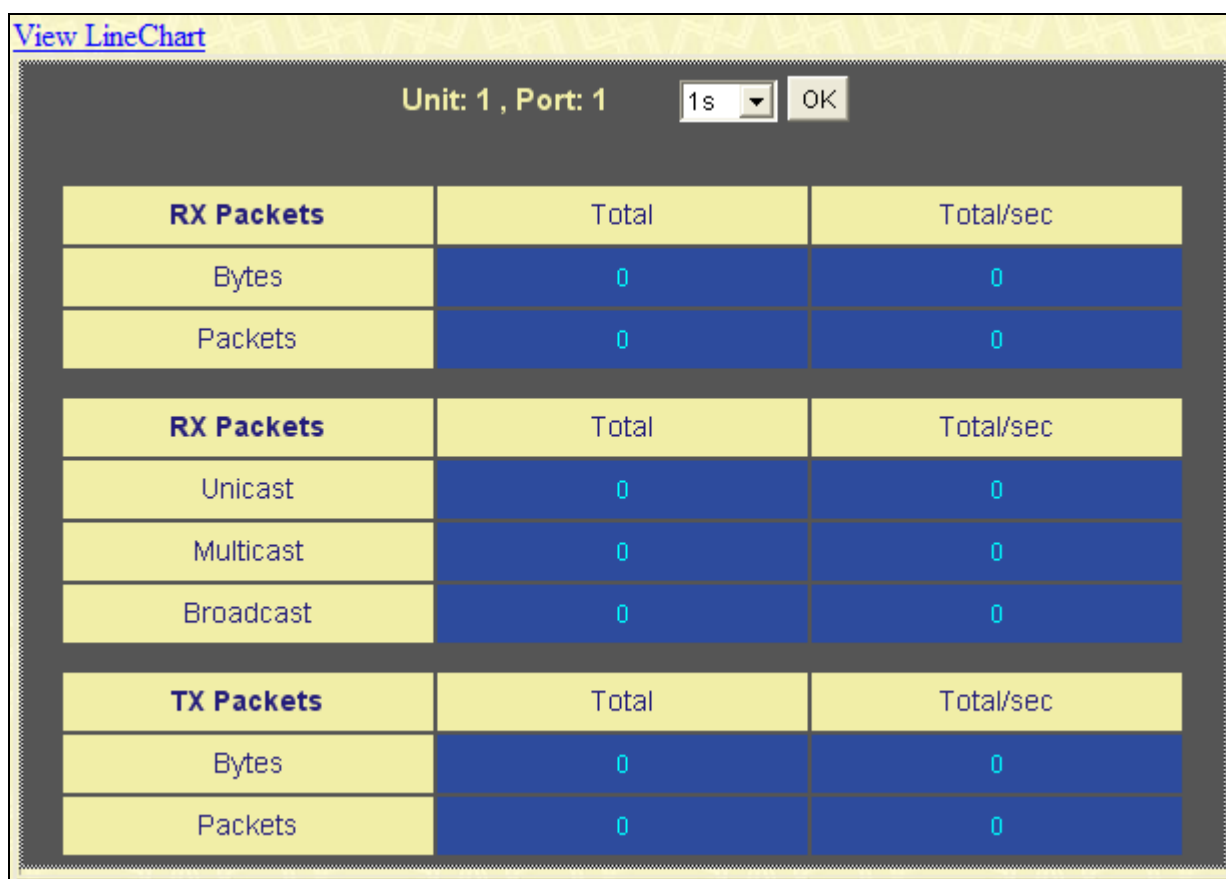


Figure 7 - 9 RX Packets Analysis Table window

The following fields may be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Bytes	Counts the number of bytes received on the port.
Packets	Counts the number of packets received on the port.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

UMB Cast (RX)

To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the window by simply clicking on a port.

To view this window, click **Monitoring > Packets > UMB_cast (RX)**, as shown below.

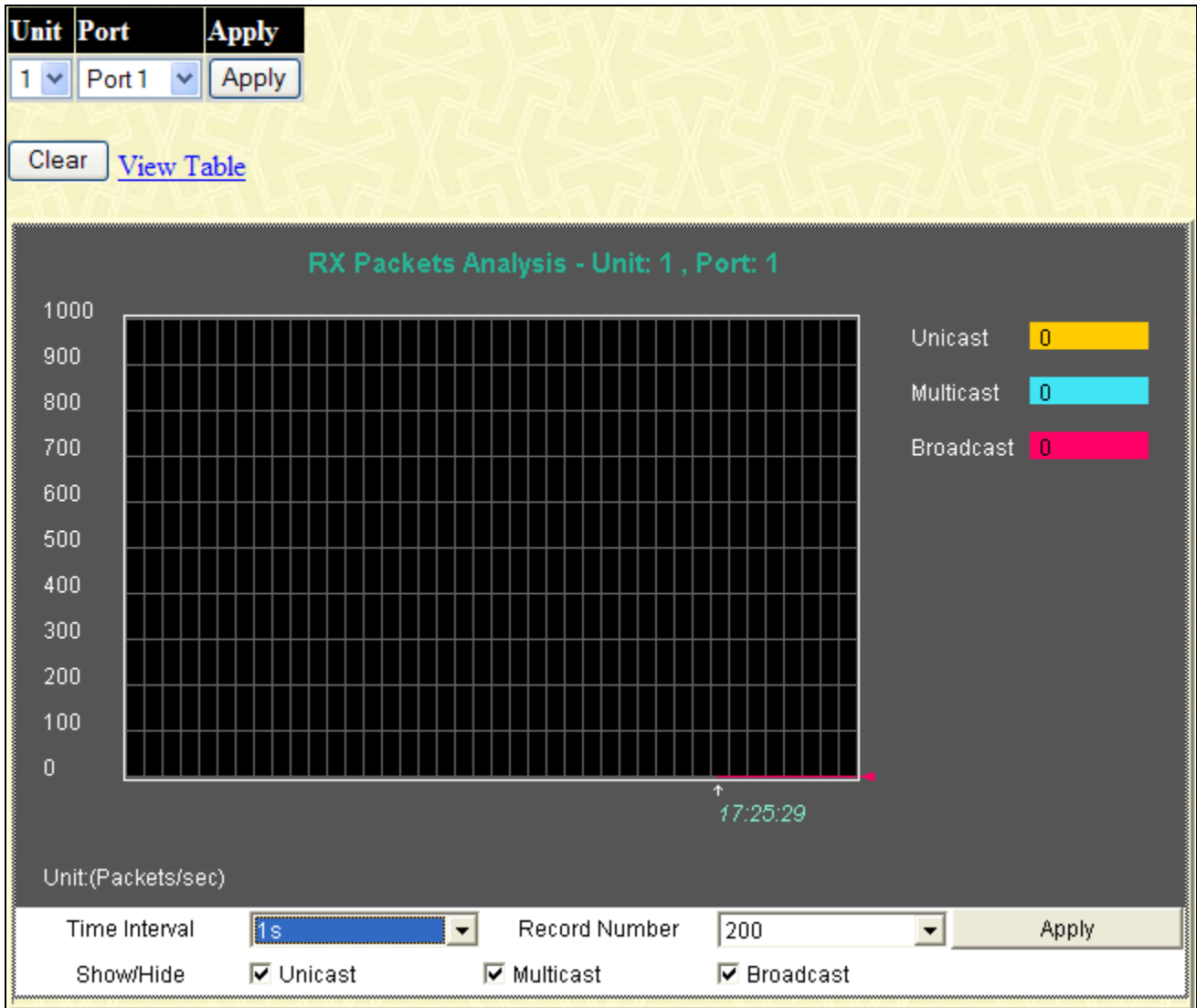


Figure 7 - 10 Packets Analysis (line graph for Unicast, Multicast, and Broadcast Packets)

To view the **UMB Cast Table** window, click the [View Table](#) link.

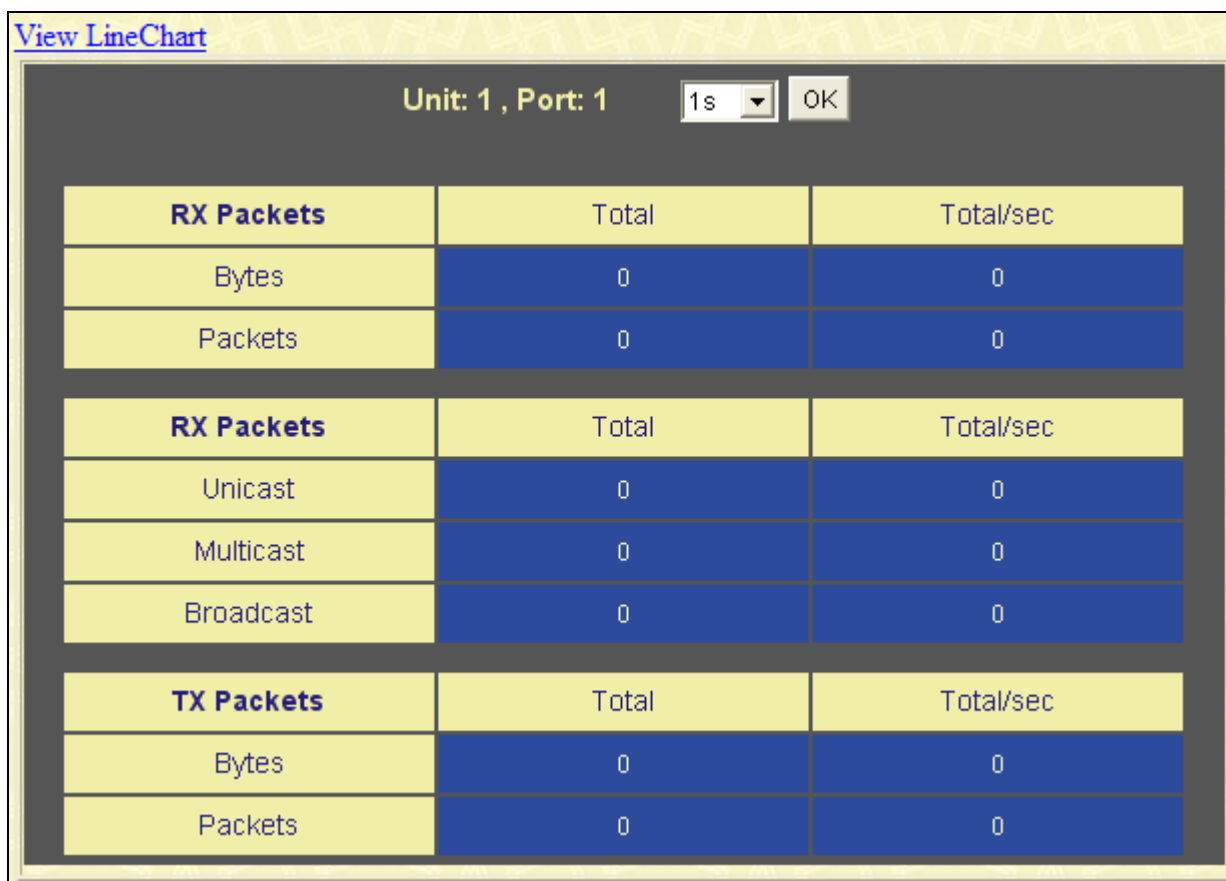


Figure 7 - 11 RX Packets Analysis window (table for Unicast, Multicast, and Broadcast Packets)

The following fields may be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Unicast	Counts the total number of good packets that were received by a unicast address.
Multicast	Counts the total number of good packets that were received by a multicast address.
Broadcast	Counts the total number of good packets that were received by a broadcast address.
Show/Hide	Check whether or not to display Multicast, Broadcast, and Unicast Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Packets > Transmitted (TX)**, as shown below.

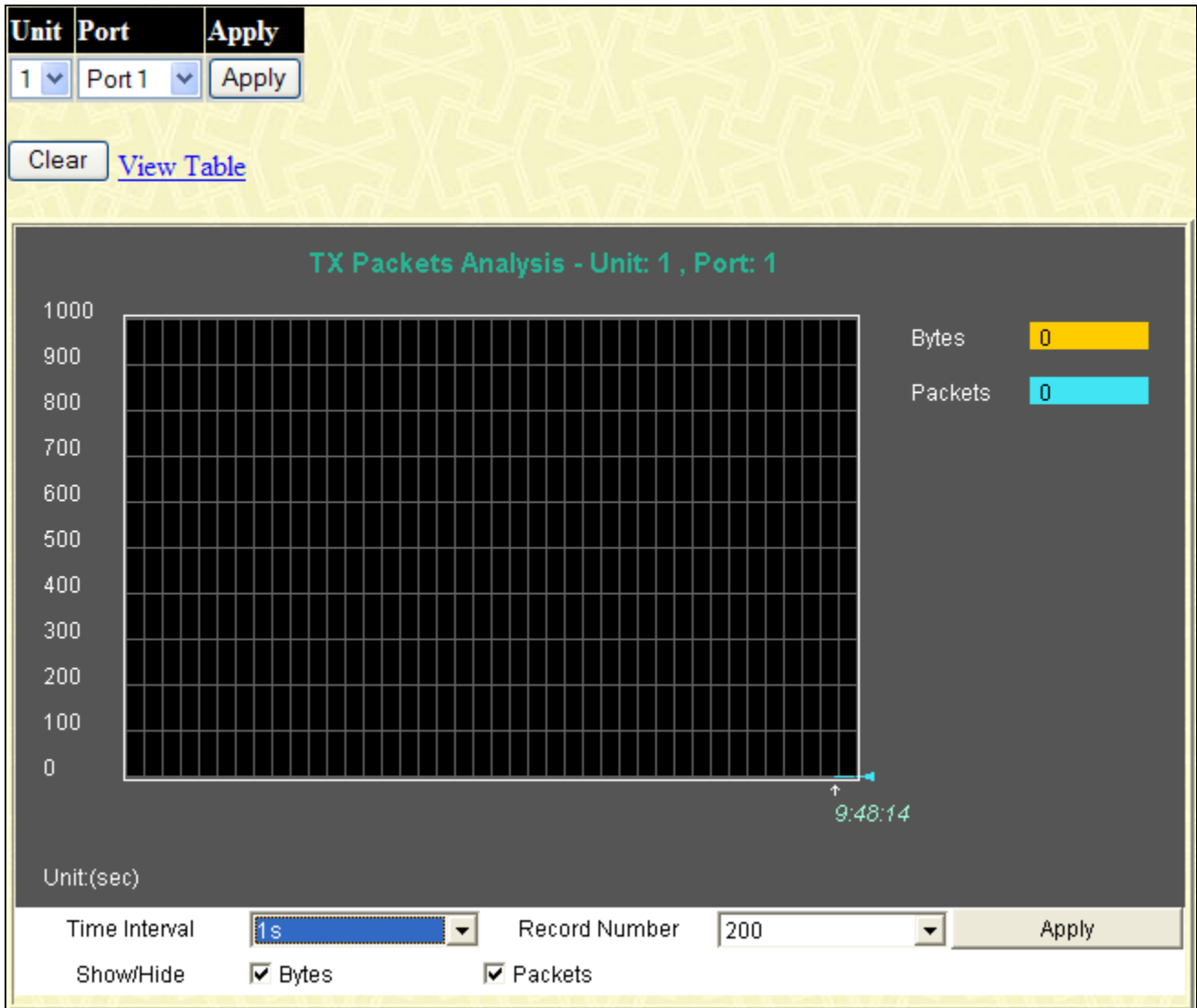


Figure 7 - 12 TX Packets Analysis window (line graph for Bytes and Packets)

To view the **Transmitted (TX) Table** window, click the link [View Table](#).

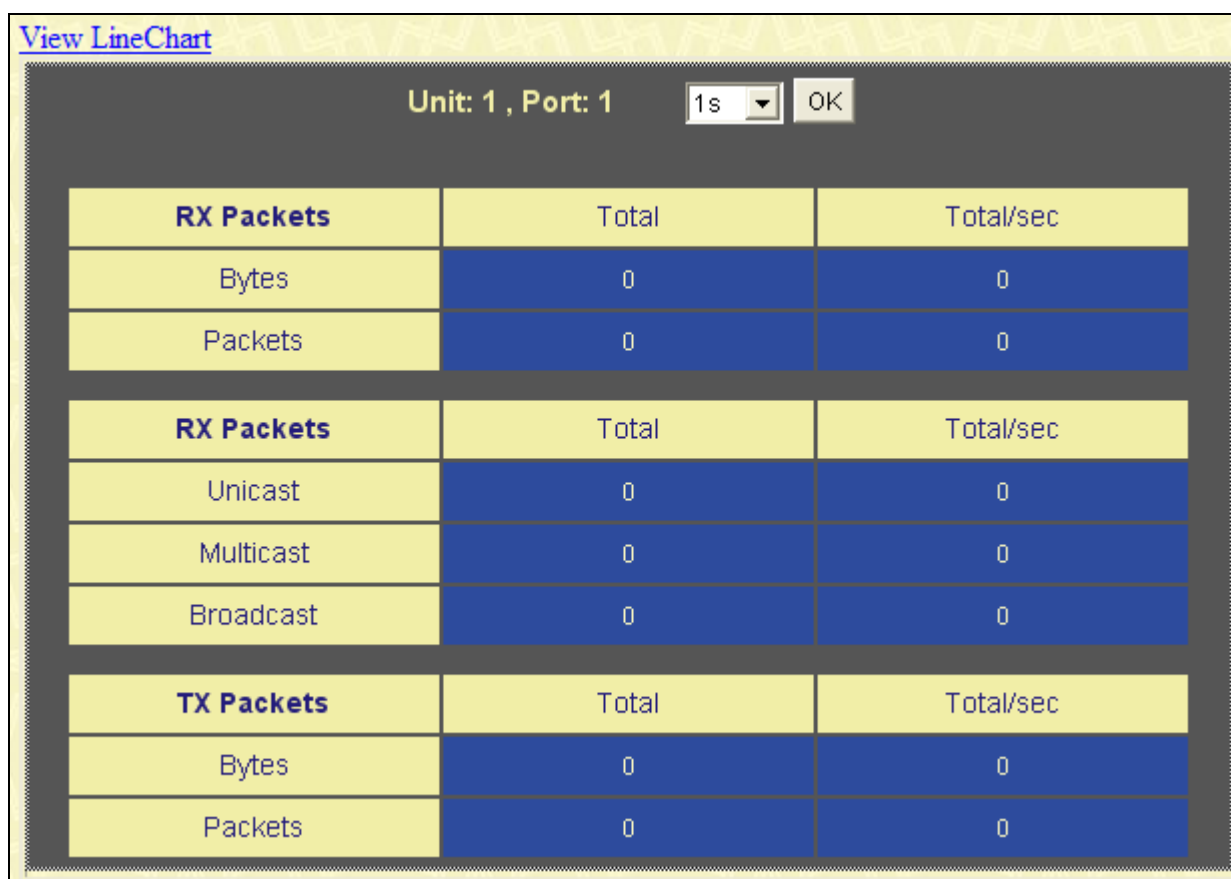


Figure 7 - 13 TX Packets Analysis window (table for Bytes and Packets)

The following fields may be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Bytes	Counts the number of bytes successfully sent on the port.
Packets	Counts the number of packets successfully sent on the port.
Unicast	Counts the total number of good packets that were transmitted by a unicast address.
Multicast	Counts the total number of good packets that were transmitted by a multicast address.
Broadcast	Counts the total number of good packets that were transmitted by a broadcast address.
Show/Hide	Check whether or not to display Bytes and Packets.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Errors

The Web Manager allows port error statistics compiled by the Switch's management agent to be viewed as either a line graph or a table. Four windows are offered.

Received (RX)

To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull-down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the window by simply clicking on a port.

To view this window, click **Monitoring > Errors > Received (RX)**, as shown below.

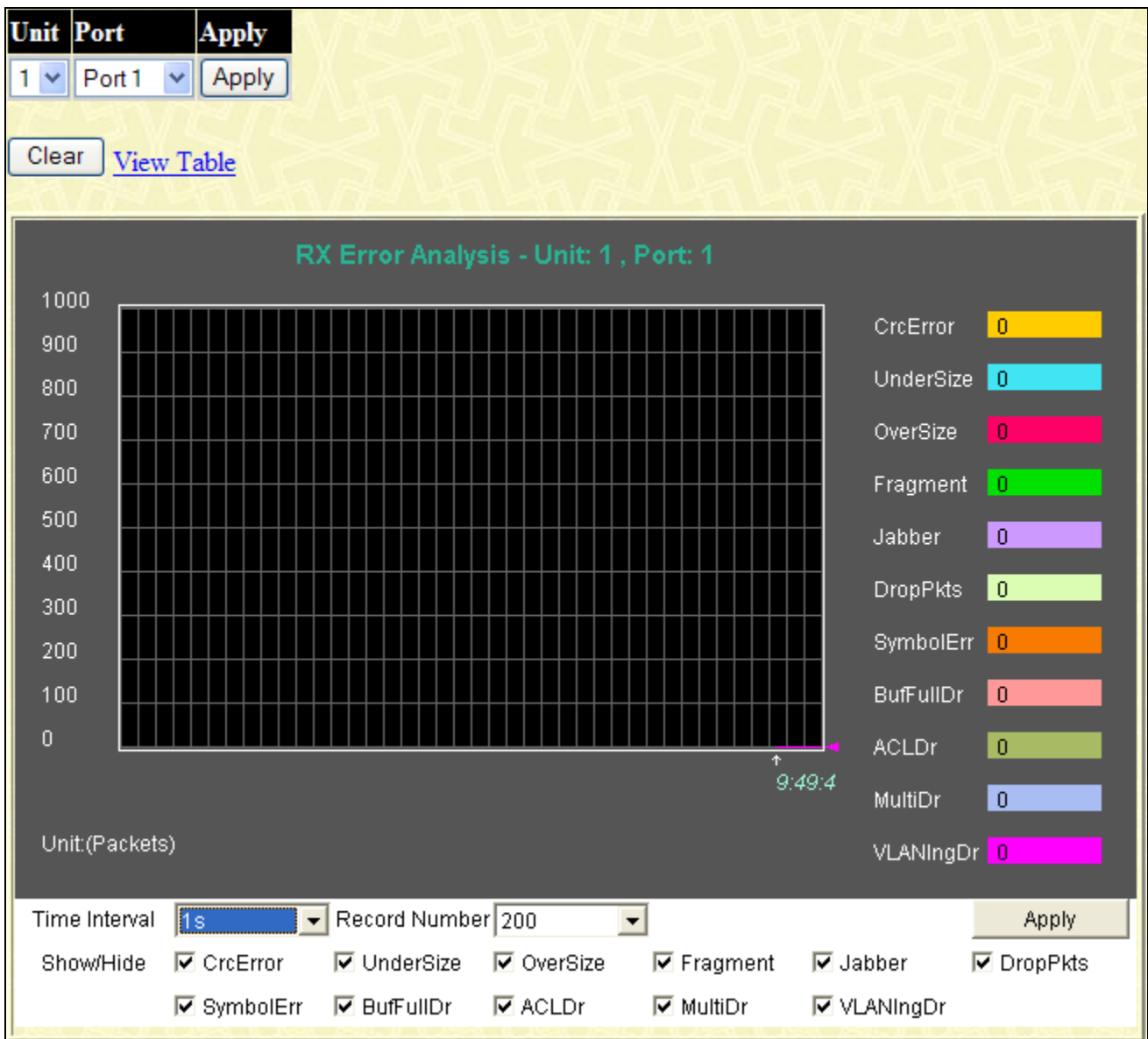


Figure 7 - 14 RX Error Analysis window (line graph)

To view the **Received Error Packets Table** window, click the link [View Table](#), which will show the following table:

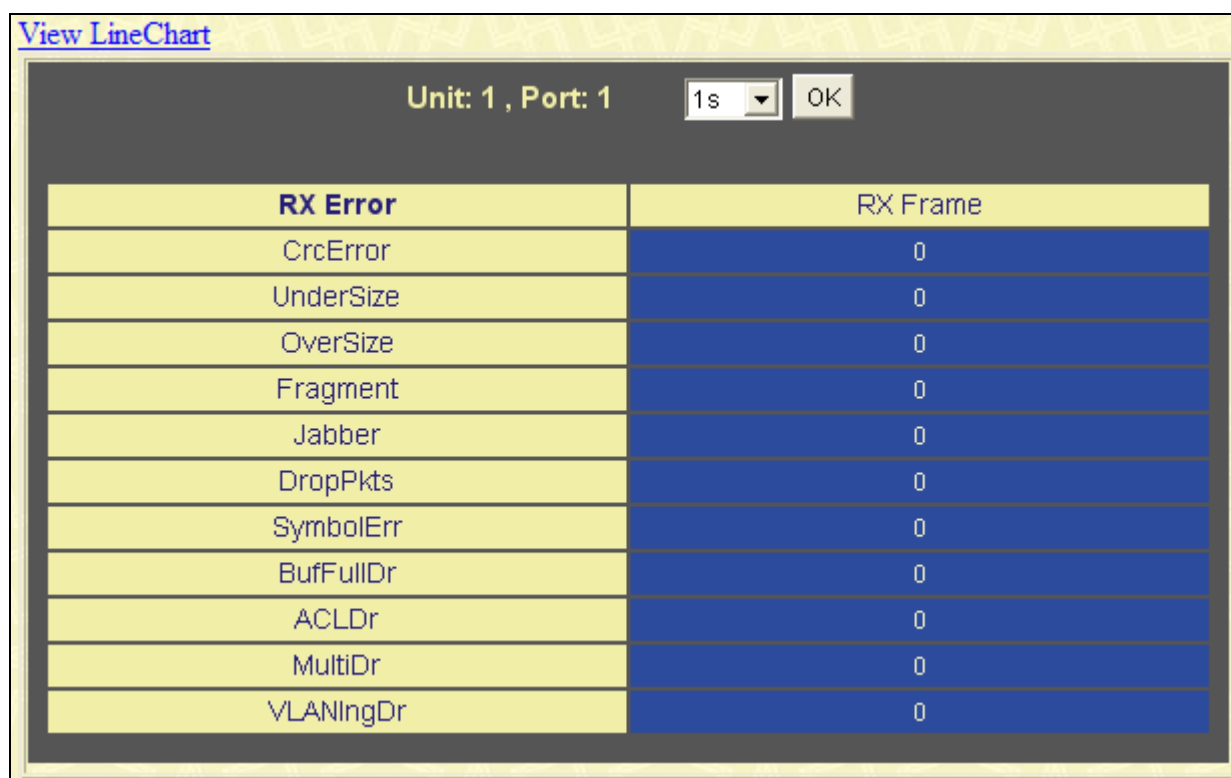


Figure 7 - 15 RX Error Analysis window (table)

The following fields can be set:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
Crc Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
UnderSize	The number of packets detected that are less than the minimum permitted packets size of 64 bytes and have a good CRC. Undersize packets usually indicate collision fragments, a normal network occurrence.
OverSize	Counts valid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
Fragment	The number of packets less than 64 bytes with either bad framing or an invalid CRC. These are normally the result of collisions.
Jabber	Counts invalid packets received that were longer than 1518 octets and less than the MAX_PKT_LEN. Internally, MAX_PKT_LEN is equal to 1536.
DropPkts	The number of packets that are dropped by this port since the last Switch reboot.
SymbolErr	Counts the number of packets received that have errors received in the symbol on the physical labor.
BufFullDr	Incremented for each packet that is discarded while buffer full.
ACLDr	Incremented for each packet that is discarded while buffer full.
MultiDr	Incremented for each multicast packet that is discarded.

VLANIngDr	Incremented for each packet that is discarded by VLAN ingress checking.
Show/Hide	Check whether or not to display CRC Error, Under Size, Over Size, Fragment, Jabber, and Drop errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Transmitted (TX)

To select a port to view these statistics for, first select the Switch in the switch stack by using the **Unit** pull-down menu and then select the port by using the **Port** pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Errors > Transmitted (TX)**, as shown below.



Figure 7 - 16 TX Error Analysis (line graph)

To view the **Transmitted Error Packets Table** window, click the link [View Table](#), which will show the following table:

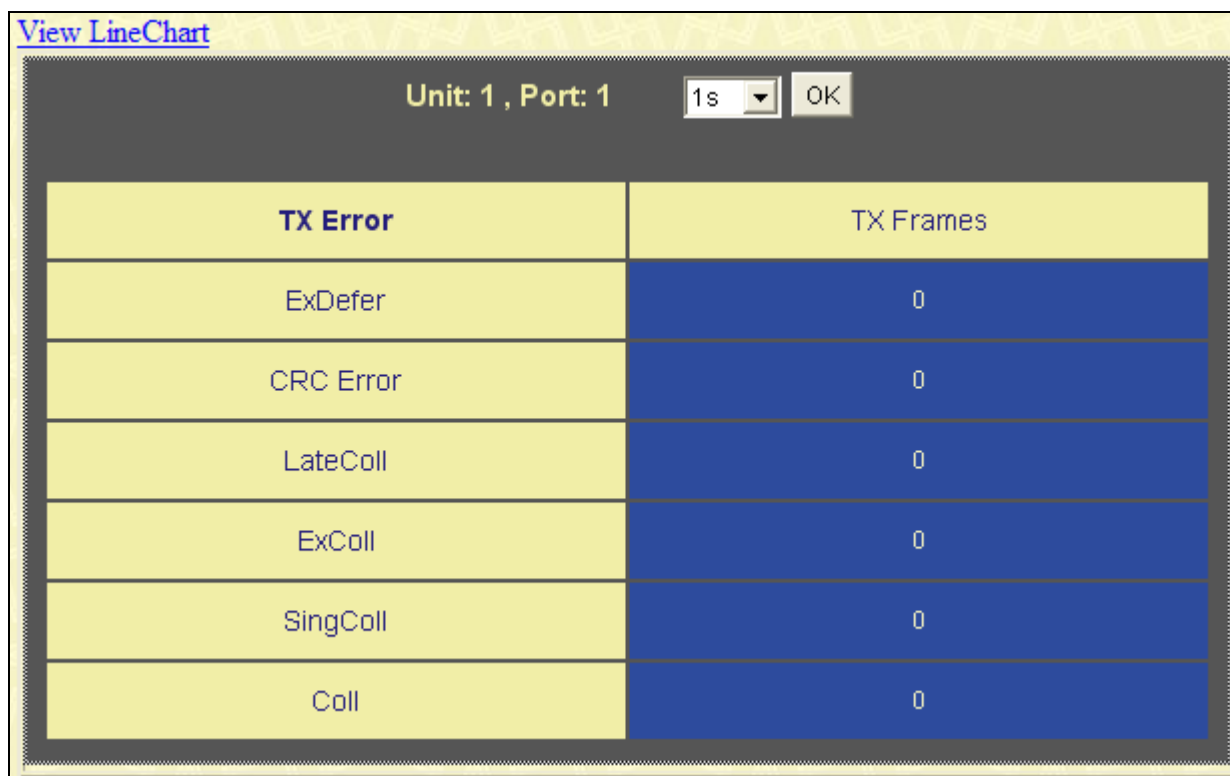


Figure 7 - 17 TX Error Analysis window (table)

The following fields may be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where "s" stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
ExDefer	Counts the number of packets for which the first transmission attempt on a particular interface was delayed because the medium was busy.
CRC Error	Counts otherwise valid packets that did not end on a byte (octet) boundary.
LateColl	Counts the number of times that a collision is detected later than 512 bit-times into the transmission of a packet.
ExColl	Excessive Collisions. The number of packets for which transmission failed due to excessive collisions.
SingColl	Single Collision Frames. The number of successfully transmitted packets for which transmission is inhibited by more than one collision.
Coll	An estimate of the total number of collisions on this network segment.
Show/Hide	Check whether or not to display ExDefer, LateColl, ExColl, SingColl, and Coll errors.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Packet Size

The Web Manager allows packets received by the Switch, arranged in six groups and classed by size, to be viewed as either a line graph or a table. Two windows are offered. To select a port to view these statistics for, first select the Switch in the switch stack by using the Unit pull-down menu and then select the port by using the Port pull down menu. The user may also use the real-time graphic of the Switch and/or switch stack at the top of the web page by simply clicking on a port.

To view this window, click **Monitoring > Packet Size**, as shown below.

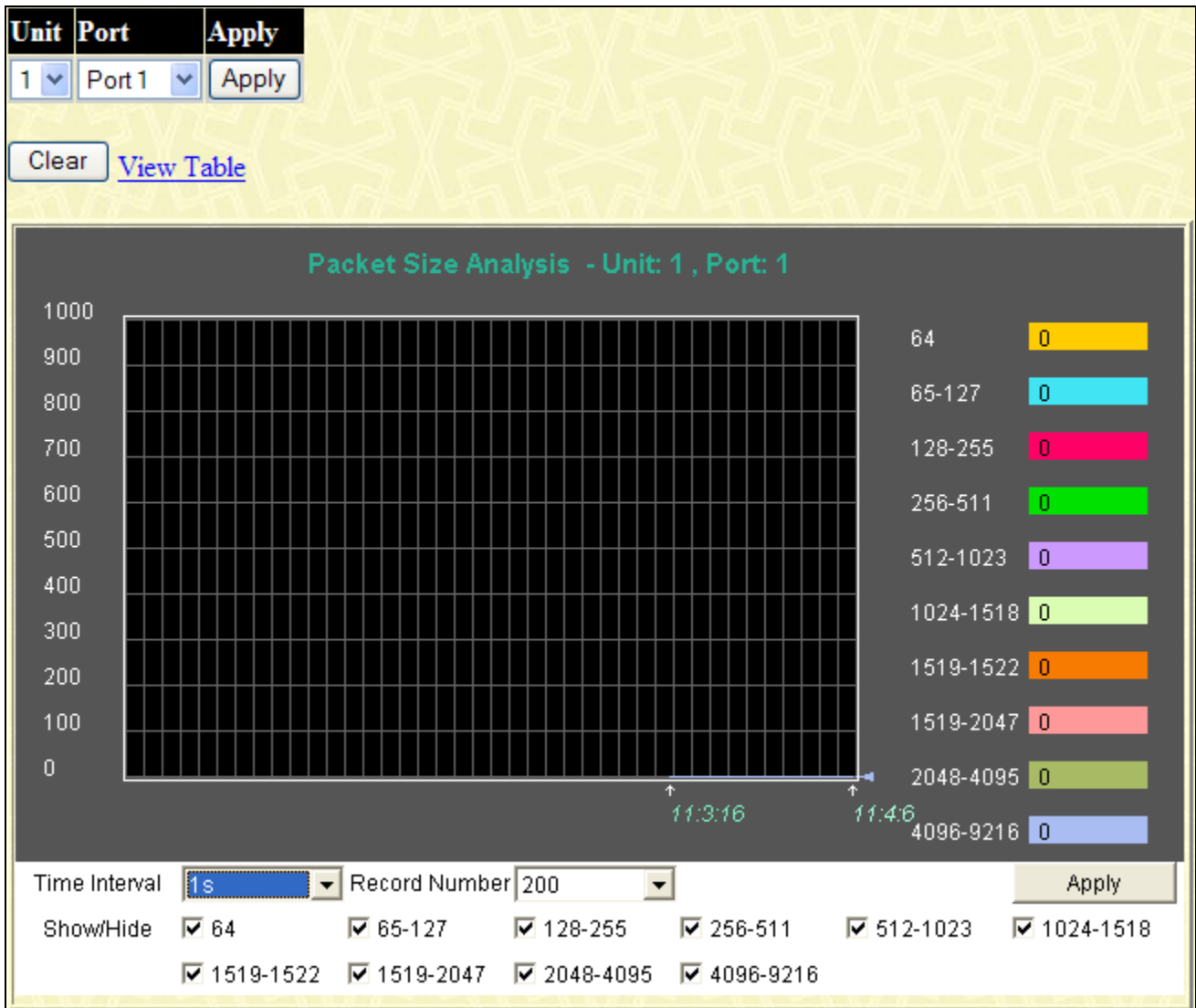


Figure 7 - 18 RX Size Analysis window (line graph)

To view the **Packet Size Analysis Table** window, click the link [View Table](#), which will show the following table:

[View Line Chart](#)

Unit: 1 , Port: 1 1s OK

Frame Size	Frame Counts	Frames/sec
64	0	0
65-127	0	0
128-255	0	0
256-511	0	0
512-1023	0	0
1024-1518	0	0
1519-1522	0	0
1519-2047	0	0
2048-4095	0	0
4096-9216	0	0

Figure 7 - 19 RX Size Analysis window (table)

The following fields can be set or viewed:

Parameter	Description
Time Interval	Select the desired setting between 1s and 60s, where “s” stands for seconds. The default value is one second.
Record Number	Select number of times the Switch will be polled between 20 and 200. The default value is 200.
64	The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).
65-127	The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).
128-255	The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).
256-511	The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

512-1023	The total number of packets (including bad packets) received that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).
1024-1518	The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).
Show/Hide	Check whether or not to display 64, 65-127, 128-255, 256-511, 512-1023, and 1024-1518 packets received.
Clear	Clicking this button clears all statistics counters on this window.
View Table	Clicking this button instructs the Switch to display a table rather than a line graph.
View Line Chart	Clicking this button instructs the Switch to display a line graph rather than a table.

Browse Router Port

This displays which of the Switch's ports are currently configured as router ports. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D and a Forbidden port is designated by F. To search for a specific VLAN enter the VLAN Name or VLAN ID and click **Find**.

To view this window, click **Monitoring > Browse Router Port**, as shown below.

VLAN Name

VLAN ID (1-4094)

Browse Router Port

VLAN ID	VLAN Name																								
1	default																								
Unit	Ports																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1																									

Figure 7 - 20 Browse IGMP Snooping Router Port window

Browse MLD Router Port

This displays which of the Switch's ports are currently configured as router ports in IPv6. A router port configured by a user (using the console or Web-based management interfaces) is displayed as a static router port, designated by S. A router port that is dynamically configured by the Switch is designated by D and a Forbidden port is designated by F. To search for a specific VLAN enter the VLAN Name or VLAN ID and click **Find**.

To view this window, click **Monitoring > Browse MLD Router Port**, as shown below.

VLAN Name	<input type="text"/>	<input type="button" value="Find"/>																							
VLAN ID (1-4094)	<input type="text"/>	<input type="button" value="Find"/>																							
Browse MLD Snooping Router Port																									
VLAN ID	VLAN Name																								
1	default																								
Unit	Ports																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1																									

Figure 7 - 21 Browse MLD Snooping Router Port window

VLAN Status

This allows the VLAN status for each of the Switch's ports to be viewed by VLAN. This window displays the ports on the Switch that are currently Egress (E) or Tag (T) ports. To search for a specific VLAN enter the VLAN Name or VLAN ID and click **Find**.

To view this window, click **Monitoring > VLAN Status**, as shown below.

VLAN Name	<input type="text"/>	<input type="button" value="Find"/>																							
VLAN ID (1-4094)	<input type="text"/>	<input type="button" value="Find"/>																							
Total VLAN Entries: 1																									
VLAN Status																									
VLAN ID	VLAN Name	Status	Advertisement																						
1	default	Static	Enabled																						
Unit	Ports																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
1	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E

Figure 7 - 22 VLAN Status window

VLAN Status Port

This window allows the VLAN status for each of the Switch's ports to be viewed. To view settings for a particular port, enter the port number and click **Find**.

To view this window, click **Monitoring > VLAN Status Port**, as shown below.

VLAN Status Port					
Port ID	VID	Untagged	Tagged	Forbidden	Dynamic
1 : 1	1	X	-	-	-
Total Entries:1					

Figure 7 - 23 VLAN Status Port window

Port Access Control

The following screens are used to monitor 802.1X statistics of the Switch, on a per port basis. To view the **Port Access Control** windows, open the monitoring folder and click the **Port Access Control** folder. There are six windows to monitor.



NOTE: The Authenticator State cannot be viewed on the Switch unless 802.1X is enabled by port or by MAC address. To enable 802.1X, go to the DGS-3400 Web Management Tool window.

Authenticator State

The following section describes the 802.1X Authenticator State on the Switch. This window displays the Authenticator State for individual ports on a selected device. In Port-based mode if one of the attached hosts is successfully authorized, all hosts on the same port will be granted access to the network. If the port authorization fails, the specified port(s) will continue authenticating. In Host-based mode each user can individually authenticate and access the network.

To view this window, click **Monitoring > Port Access Control > Authenticator State**, as shown below.

802.1X Authenticator State Table Settings						
Port List		<input type="text"/>	<input type="checkbox"/> All Ports			
						<input type="button" value="Search"/>
802.1X Authenticator State Table						
Port	MAC Address	PAE State	Backend State	Status	VID	Assigned Priority
Total Authenticating Hosts: 0						
Total Authenticated Hosts: 0						
Show All 802.1X Authenticator State Table Entries						

Figure 7 - 24 Authenticator State window

The user may also view this window if any port/host is authenticated.

Parameter	Description
Port List	Enter the port list you wish to find. To view all ports tick the Select All Ports check box.

MAC Address	Displays the MAC address of the client that is present when configured in mac based mode. It displays “-p” when configured in port based mode.
State	The Authenticator State value can be: Authenticated, Authenticating, or blocked.
VID	Displays the assigned VLAN ID. If a port/host is authenticated and the authorization Network is enabled, the assigned VLAN is determined by the VLAN assigned from RADIUS server. If there is no target VLAN information or invalid VLAN information embedded in RADIUS message it will be ignored.
Assigned Priority	Displays the assigned priority. If a port is authenticated and the authorization is enabled, the 802.1p default priority can be controlled by the RADIUS server via the passing value. The value of 802.1p comes from when the RADIUS server overwrites the locally configured ports. If the assigned priority is not valid (less than 0 or greater than 7) it will be ignored. In this case, the switch still adopts the local setting. The default priority is used to classify the priority for untagged packets. The 802.1p priority is on per port basis. However, for host-based authentication mode, the assigned 802.1p will be assigned for each host (MAC).

Authenticator Statistics

This table contains the statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. Enter the ports you wish to view and click **Search**.

To view the Authenticator Statistics, click **Monitoring > Port Access Control > Authenticator Statistics**, as shown below.

Authenticator Statistics Table Settings

Port List All Ports Search

Total Entries: 0

Authenticator Statistics Table

Port	MAC Address	View
------	-------------	------

Figure 7 - 25 Authenticator Statistics window

Authenticator Session Statistics

This table contains the session statistics objects for the Authenticator PAE associated with each port. An entry appears in this table for each port that supports the Authenticator function. Enter the ports you wish to view and click **Search**.

To view this window, click **Monitoring > Port Access Control > Authenticator Session Statistics**, as shown below.

Authenticator Session Statistics Table Settings

Port List All Ports Search

Total Entries: 0

Authenticator Session Statistics Table

Port	MAC Address	View
------	-------------	------

Figure 7 - 26 Authenticator Session Statistics window

Authenticator Diagnostics

This table contains the diagnostic information regarding the operation of the Authenticator associated with each port. An entry appears in this table for each port that supports the Authenticator function. Enter the ports you wish to view and click **Search**.

To view this window, click **Monitoring > Port Access Control > Authenticator Diagnostics**, as shown below.

Authenticator Diagnostics Table Settings

Port List All Ports Search

Total Entries: 0

Authentication Diagnostics Table

Port	MAC Address	View
------	-------------	------

Figure 7 - 27 Authenticator Diagnostics window

RADIUS Authentication

This table contains information concerning the activity of the RADIUS authentication client on the client side of the RADIUS authentication protocol.

To view this window, click **Monitoring > Port Access Control > RADIUS Authentication**, as shown below.

RADIUS Authentication Time Interval: 1s

ServerIndex	InvalidServerAddr	Identifier	AuthServerAddr	ServerPortNumber	RoundTripTime	AccessRequests	AccessRefrans	AccessAccepts	AccessRejects	AccessChallenges	AccessResponses	BasAuthenticators	PendingRequests	Timeouts	UnknownTypes	PacketsDropped
1	0	D-Link	0000	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	D-Link	0000	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	D-Link	0000	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 7 - 28 RADIUS Authentication information window

RADIUS Account Client

This window shows managed objects used for managing RADIUS accounting clients, and the current statistics associated with them.

To view this window, click **Monitoring > Port Access Control > RADIUS Account Client**, as shown below.

RADIUS Account Client Time Interval: 1s

ServerIndex	InvalidServerAddr	Identifier	ServerAddr	ServerPortNumber	RoundTripTime	Requests	Retransmissions	Responses	MulticastResponses	BasAuthenticators	PendingRequests	Timeouts	UnknownTypes	PacketsDropped
1	0	D-Link	0000	0	0	0	0	0	0	0	0	0	0	0
2	0	D-Link	0000	0	0	0	0	0	0	0	0	0	0	0
3	0	D-Link	0000	0	0	0	0	0	0	0	0	0	0	0

Figure 7 - 29 RADIUS Account Client information

The user may also select the desired time interval to update the statistics, between 1s and 60s, where “s” stands for seconds. The default value is one second. To clear the current statistics shown, click the *Clear* button in the top left hand corner.

The following information is displayed:

Parameter	Description
InvalidServerAddresses	The number of RADIUS Accounting-Response packets received from unknown addresses.
Identifier	The NAS-Identifier of the RADIUS accounting client. (This is not necessarily the same as sysName in MIB II.)
ServerAddr	The (conceptual) table listing the RADIUS accounting servers with which the client shares a secret.
ServerPortNumber	The UDP port the client is using to send requests to this server.
RoundTripTime	The time interval between the most recent Accounting-Response and the Accounting-Request that matched it from this RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Responses	The number of RADIUS packets received on the accounting port from this server.
MalformedResponses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
BadAuthenticators	The number of RADIUS Accounting-Response packets, which contained invalid authenticators, received from this server.
PendingRequests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response. This variable is incremented when an Accounting-Request is sent and decremented due to receipt of an Accounting-Response, a timeout or a retransmission.
Timeouts	The number of accounting timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as an Accounting-Request as well as a timeout.
UnknownTypes	The number of RADIUS packets of unknown type which were received from this server on the accounting port.
PacketsDropped	The number of RADIUS packets, which were received from this server on the accounting port and dropped for some other reason.



NOTE: To configure 802.1X features for the xStack® switch, go to **Security > 802.1X**.

MAC Address Table

This allows the Switch's dynamic MAC address forwarding table to be viewed. When the Switch learns an association between a MAC address and a port number, it makes an entry into its forwarding table. These entries are then used to forward packets through the Switch.

To view this window, click **Monitoring > MAC Address Table**, as shown below.

VLAN Name	<input type="text"/>	<input type="button" value="Find"/>	<input type="button" value="Clear Dynamic Entries"/>		
VID (1-4094)	<input type="text"/>	<input type="button" value="Find"/>			
MAC Address	<input type="text" value="00-00-00-00-00-00"/>	<input type="button" value="Find"/>			
Unit - Port	<input type="text" value="1"/> <input type="text" value="Port 1"/>	<input type="button" value="Find"/>	<input type="button" value="Clear Dynamic Entries"/>		
		<input type="button" value="View All Entries"/>	<input type="button" value="Clear All Entries"/>		
MAC Address Table					
VID	VLAN Name	MAC Address	Unit	Port	Type
1	default	00-0C-6E-AA-B9-C0	1	3	Dynamic
1	default	00-21-91-53-3E-C8	CPU		Self
Total Entries: 2					

Figure 7 - 30 MAC Address Table window

The functions are used in the MAC address table:

Parameter	Description
VLAN Name	Enter a VLAN Name for the forwarding table to be browsed by.
VID (1-4094)	Enter a VLAN ID for the forwarding table to be browsed by.
MAC Address	Enter a MAC address for the forwarding table to be browsed by.
Unit - Port	Select the unit of the switch in the switch stack, and a port on that switch, where to find the MAC address.
Find	Allows the user to move to a sector of the database corresponding to a user defined port, VLAN, or MAC address.
VID	The VLAN ID of the VLAN of which the port is a member.
VLAN Name	The VLAN Name of the VLAN of which the port is a member.
MAC Address	The MAC address entered into the address table.
Unit - Port	The unit and port to which the MAC address above corresponds.
Type	Describes the method which the Switch discovered the MAC address. The possible entries are Dynamic, Self, and Static.
Next	Click this button to view the next page of the address table.
View All Entries	Clicking this button will allow the user to view all entries of the address table.
Clear All Entries	Clicking this button will allow the user to delete all entries of the address table.

IGMP Snooping Group

This window allows the Switch's IGMP Snooping Group Table to be viewed. IGMP Snooping allows the Switch to read the Multicast Group IP address and the corresponding MAC address from IGMP packets that pass through the Switch.

To view this window, click **Monitoring > IGMP Snooping Group**, as shown below.

VID	VLAN Name	Source	Group	Member Ports	Filter Mode
-----	-----------	--------	-------	--------------	-------------

Figure 7 - 31 IGMP Snooping Group Table window

The user may search the IGMP Snooping Group Table by VLAN name by entering it in the top left hand corner and clicking **Find**. To view all entries click **View All Entry**.



NOTE: To configure IGMP snooping for the xStack® DGS-3400 Series switch, go to the **L2 Features** folder and select **IGMP Snooping**. Configuration and other information concerning IGMP snooping may be found in Section 7 of this manual under **IGMP Snooping**.

IGMP Snooping Data Driven Group

The dynamic IP Multicast Learning function is to forward un-registered IP multicast data packets to router ports without any clients report on the IP multicast group.

To view this window, click **Monitoring > IGMP Snooping Data Driven Group**, as shown below.

VID	VLAN Name	Source	Group	Member Ports	Router Ports	Filter Mode
-----	-----------	--------	-------	--------------	--------------	-------------

Figure 7 - 32 IGMP Snooping Data Driven Group Table window

The functions are used in the MAC address table:

Parameter	Description
VLAN Name	Enter a VLAN Name to be browsed by or to be deleted.
VID List	Enter a list of VLAN ID to be browsed by or to be deleted.
IP Address	Enter a IP address to be browsed by or to be deleted.

To search for IGMP snooping data driven group, click **Find**. To view all entries, click **View All Entries**. To delete an entry, enter the information and click **Clear**. To remove all entries, click **Clear All Entries**.

MLD Snooping Group

The following window allows the user to view MLD Snooping Groups present on the Switch. MLD Snooping is an IPv6 function comparable to IGMP Snooping for IPv4. The user may browse this table by VLAN Name present in the switch by entering that VLAN Name in the empty field shown below, and clicking the Search button.

To view this window, click **Monitoring > MLD Snooping Group**, as shown below.

VID	VLAN Name	Source	Group	Member Ports	Filter Mode
-----	-----------	--------	-------	--------------	-------------

Figure 7 - 33 MLD Snooping Group Table

The user may search the MLD Snooping Group Table by VLAN name by entering it in the top left hand corner and clicking **Find**. To view all entries click **View All Entry**.



NOTE: To configure MLD snooping for the xStack® DGS-3400 Series switch, go to the **L2 Features** folder and select **MLD Snooping**. Configuration and other information concerning MLD snooping may be found in Section 7 of this manual under **MLD Snooping**.

MLD Snooping Data Driven Group

To view this window, click **Monitoring > MLD Snooping Data Driven Group**, as shown below.

VID	VLAN Name	Source	Group	Member Ports	Router Ports	Filter Mode
-----	-----------	--------	-------	--------------	--------------	-------------

Figure 7 - 34 MLD Snooping Data Driven Group Table window

The functions are used in the MAC address table:

Parameter	Description
VLAN Name	Enter a VLAN Name to be browsed by or to be deleted.
VID List	Enter a list of VLAN ID to be browsed by or to be deleted.
IP Address	Enter a IP address to be browsed by or to be deleted.

To search for MLD snooping data driven group, click **Find**. To view all entries, click **View All Entries**. To delete an entry, enter the information and click **Clear**. To remove all entries, click **Clear All Entries**.

Trace Route

The following window will aid the user in back tracing the route taken by a packet before arriving at the Switch. When initiated, the Trace Route program will display the IP addresses of the previous hops a packet takes from the Target IP Address entered in the window, until it reaches the Switch.

Trace IPv4 Route

To view this window, click **Monitoring > Trace Route > Trace IPv4 Route**, as shown below.

Figure 7 - 35 Trace IPv4 Route window

The following parameter can be configured:

Parameter	Description
Target IP Address	Click the radio button to enter the IP address of the computer to be traced.
Domain Name	Enter the domain name of the host.
TTL (1-60)	The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices.
Port (30000-64900)	The virtual port number. The port number must be above 1024. The value range is from 30000 to 64900.
Timeout (1-65535)	Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between 1 and 65535 seconds.
Probe (1-9)	The probe value is the number of times the Switch will send probe packets to the next hop on the intended traceroute path. The default is 1.

Click **Start** to trace the route of a packet.

Trace IPv6 Route

To view this window, click **Monitoring > Trace Route > Trace IPv6 Route**, as shown below.

Figure 7 - 36 Trace IPv6 Route window

The following parameter can be configured:

Parameter	Description
Target IPv6 Address	Enter the IP address of the computer to be traced.
TTL (1-60)	The time to live value of the trace route request. This is the maximum number of routers the traceroute command will cross while seeking the network path between two devices.
Port (30000-64900)	The virtual port number. The port number must be above 1024. The value range is from 30000 to 64900.
Timeout (1-65535)	Defines the time-out period while waiting for a response from the remote device. The user may choose an entry between 1 and 65535 seconds.
Probe (1-9)	The probe value is the number of times the Switch will send probe packets to the next hop on the intended traceroute path. The default is 1.

Click **Start** to trace the route of a packet.

Switch Logs

The Web manager allows the Switch's history log, as compiled by the Switch's management agent, to be viewed.

To view this window, click **Monitoring > Switch Log**, as shown below.

Log Type Selection			
Type	Unit	Severity	Apply
Regular Log	1	<input type="checkbox"/> Emergency <input type="checkbox"/> Alert <input type="checkbox"/> Critical <input type="checkbox"/> Error <input type="checkbox"/> Warning <input type="checkbox"/> Notice <input type="checkbox"/> Informational <input type="checkbox"/> Debug	Apply

Switch History Logs			
Sequence	Time	Level	Log Text
5	2010-05-18, 14:27:20	INFO (6)	Successful login through Web (Username: Anonymous)
4	2010-05-18, 14:26:07	INFO (6)	Stacking topology is Chain. Master(Unit 1, MAC:00-21-91-53-3E-C8).
3	2010-05-18, 14:26:07	INFO (6)	Port 1:3 link up, 100Mbps FULL duplex
2	2010-05-18, 14:26:07	INFO (6)	Spanning Tree MST configuration ID name and revision level change (name:00:21:91:53:3E:C8 revision level:0)
1	2010-05-18, 14:26:07	CRIT (2)	Unit 1, System cold start

Clear

Figure 7 - 37 Switch History Logs window

The information in the table is categorized as:

Parameter	Description
Type	Choose the type of log to view. There are two choices: <i>Regular Log</i> – Choose this option to view regular switch log entries, such as logins or firmware transfers. <i>Attack Log</i> – Choose this option to view attack log files, such as spoofing attacks.
Unit	Choose the Unit ID of the switch in the switch stack for which to view the switch log.
Severity	Tick the check boxes to specify the severity to be displayed.
Sequence	A counter incremented whenever an entry to the Switch's history log is made. The table displays the last entry (highest sequence number) first.
Time	Displays the time in days, hours, and minutes since the Switch was last restarted.
Log Text	Displays text describing the event that triggered the history log entry.

The Switch can record event information in its own logs, to designated SNMP trap receiving stations, and to the PC connected to the console manager. Click **Next** to go to the next page of the **Switch History Log**. Click **Clear** will allow the user to clear the Switch History Log.

Browse ARP Table

This window will show current ARP entries on the Switch. To search a specific ARP entry, enter an interface name into the Interface Name, an IP Address or a MAC Address, and click **Find**. To clear the ARP Table, click **Clear All**.

To view this table, click **Monitoring > Browse ARP Table**, as shown below.

Interface Name	<input type="text"/>		
IP Address	<input type="text"/>		
MAC Address	<input type="text"/>		
State	<input type="checkbox"/> Static	<input type="button" value="Find"/>	<input type="button" value="Clear All"/>
<input type="button" value="View All"/>			
Total Entries: 4			
ARP Table			
Interface Name	IP Address	MAC Address	Type
System	10.0.0.0	FF-FF-FF-FF-FF-FF	Local/Broadcast
System	10.90.90.10	00-0C-6E-AA-B9-C0	Dynamic
System	10.90.90.90	00-21-91-53-3E-C8	Local
System	10.255.255.255	FF-FF-FF-FF-FF-FF	Local/Broadcast

Figure 7 - 38 ARP Table window

Session Table

This window is used to display the current session table.

To view this window, click **Monitoring > Session Table**, as shown below.

<input type="button" value="Reload"/>				
Total Entries :1				
Current Session Table				
ID	Live Time	From	Level	Name
8	00:07:13.860	Serial Port	1	Anonymous

Figure 7 - 39 Current Session Table window

IP Forwarding Table

The IP Forwarding Table window is read-only where the user may view IP addresses discovered by the Switch. To search a specific IP address, enter it into the field labeled IP Address at the top of the window and click **Find** to begin your search.

To view this window, click **Monitoring > IP Forwarding Table**, as shown below.

IP Address	<input type="text" value="0.0.0.0"/>	<input type="button" value="Find"/>	
IP Forwarding Table			
Interface	IP Address	Port	Learned
System	10.90.90.10	1:3	Dynamic
Total Entries: 1			

Figure 7 - 40 IP Forwarding Table window

Routing Table

Browse Routing Table

This window shows the current IP routing table of the Switch. To find a specific IP route, enter an IP address along with a proper subnet mask in the two fields offered and click **Find**.

To view this window, click **Monitoring > Routing Table > Browse Routing Table**, as shown below.

IP Address	<input type="text"/>	<input type="button" value="Find"/>			
Netmask	<input type="text"/>				
Total Entries: 1					
Routing Table					
IP Address	Netmask	Gateway	Interface	Cost	Protocol
10.0.0.0	255.0.0.0	0.0.0.0	System	1	Local

Figure 7 - 41 Routing Table window

Browse IPv6 Routing Table

To view this window, click **Monitoring > Routing Table > Browse IPv6 Routing Table**, as shown below.

IPv6 Address/PrefixLen

Type RIPng

Total Entries: 0

IPv6 Routing Table

IPv6 Prefix	Protocol	Metric	Next Hop	IPIF
-------------	----------	--------	----------	------

Figure 7 - 42 IPv6 Routing Table window

MAC-based Access Control Authentication Status

To clear MAC-based Access Control Authentication entries enter the appropriate information and click **Delete**.

To view this table, click **Monitoring > MAC Based Access Control Authentication Status**, as shown below.

MAC-based Access Control Authentication State Table Settings

Port List Select All Ports

MAC-based Access Control Authentication State Table

Port	MAC Address	State	VID	Priority	Aging Time/ Block Time	Delete
------	-------------	-------	-----	----------	------------------------	--------

Total Authenticating Hosts: 0
 Total Authenticated Hosts: 0
 Total Blocked Hosts: 0

[Show All MAC-based Access Control Authentication State Table Entries](#)

Figure 7 - 43 MAC-based Access Control Authentication State Table Settings window

Section 8

Save, Reset and Reboot

- Reset*
- Reboot System*
- Save Services*
- Logout*

Reset

The Reset function has several options when resetting the Switch. Some of the current configuration parameters can be retained while resetting all other configuration parameters to their factory defaults.



NOTE: Only the Reset System option will enter the factory default parameters into the Switch's non-volatile RAM, and then restart the Switch. All other options enter the factory defaults into the current configuration, but do not save this configuration. Reset System will return the Switch's configuration to the default factory settings.

Reset	
Reset	<input type="radio"/> Proceed with system reset except stacking, IP address, log, user account and banner.
Reset Config	<input type="radio"/> Proceed with system reset except stacking.
Reset System	<input checked="" type="radio"/> Proceed with system reset (reset all, save, reboot). <input type="checkbox"/> Reset Stack
<input type="button" value="Apply"/>	

Figure 8 - 1 Reset window

Reboot System

The following menu is used to restart the Switch.

Reboot System

If you do not save the settings, all changes made in this session will be lost.

Do you want to save the settings? **Yes** **No**

Figure 8 - 2 Reboot System window

Click the **Yes** radio button, and the Switch saves the current configuration to non-volatile RAM before restarting the Switch.

Click the **No** radio button for not saving the current configuration before restarting the Switch. All of the configuration information entered from the last time Save Changes was executed will be lost.

Click the **Restart** button to restart the Switch.

Save Services

The following three windows will aid the user in saving configurations to the Switch's memory.

Save Changes

The Switch has two levels of memory, normal RAM and non-volatile or NV-RAM. Configuration changes are made effective clicking the **Save** button. When this is done, the settings will be immediately applied to the switching software in RAM, and will immediately take effect.

Some settings, though, require you to restart the Switch before they will take effect. Restarting the Switch erases all settings in RAM and reloads the stored settings from the NV-RAM. Thus, it is necessary to save all setting changes to NV-RAM before rebooting the switch.

The save options allow one alternative configuration image to be stored.

To view this window, click **Save Services > Save Changes**, as shown below.

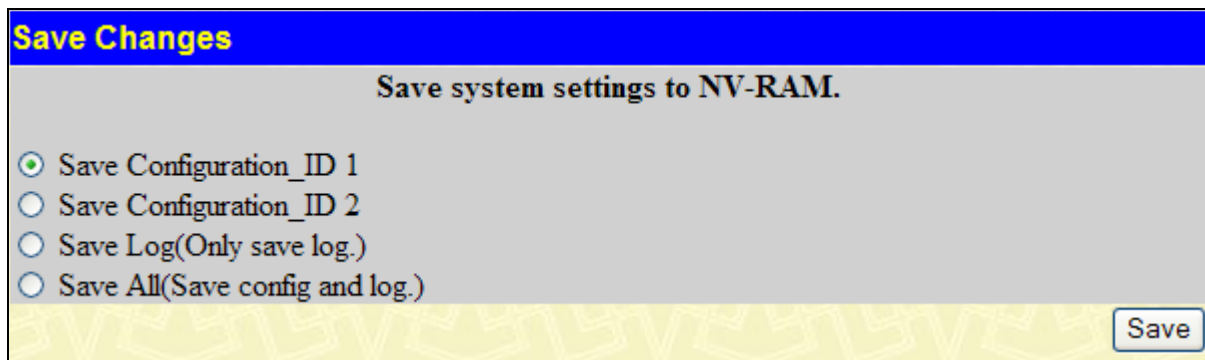


Figure 8 - 3 Save Changes window

The Save Changes options include:

- **Save Configuration_ID_1** to save the configuration file indexed as Image file 1. To use this file for configuration it must be designated as the *Boot* configuration using the **Config Current Setting** menu (**Save Services > Config Current Setting**)
- **Save Configuration_ID_2** to save the configuration file indexed as Image file 2. To use this file for configuration it must be designated as the *Boot* configuration using the **Config Current Setting** menu (**Save Services > Config Current Setting**)
- **Save Log** to save only the current log.
- **Save All** to save the current configuration file indexed as Image file 1 and save the current log.

Configuration Information

The following window is used to view information regarding configuration files saved in the Switch. The Switch can hold two configuration files in its memory. Configuration Files can be uploaded to the Switch using the TFTP services located in the Administration folder.

To view this window, click **Save Services > Configure Information**, as shown below.

Configuration Information						
ID	Version	Size (B)	Update Time	From	User	Boot
*1	2.70.B43	15898	2010/04/12 09:43:16	Local save(W)	admin	*
2	(empty)					

Note : * indicates the currently actived configuration

(R) means configuration update through Serial Port (RS232)

(T) means configuration update through Telnet

(S) means configuration update through SNMP

(W) means configuration update through Web

(SIM) means configuration update through Single IP Management

Figure 8 - 4 Configuration Information window

This window holds the following information:

Parameter	Description
ID	States the image ID number of the configuration file in the Switch's memory. The Switch can store 2 configuration files for use. Image ID 1 will be the default boot up configuration file for the Switch unless otherwise configured by the user.
Version	States the firmware version.
Size	States the size of the corresponding configuration file, in bytes.
Update Time	States the specific time the configuration file was downloaded to the Switch.
From	States the origin of the firmware. There are five ways configuration files may be uploaded to the Switch. R – If the IP address has this letter attached to it, it denotes a configuration file upgrade through the Console Serial Port (RS-232). T – If the IP address has this letter attached to it, it denotes a configuration file upgrade through Telnet. S – If the IP address has this letter attached to it, it denotes a configuration file upgrade through the Simple Network Management Protocol (SNMP). W – If the IP address has this letter attached to it, it denotes a configuration file upgrade through the web-based management interface. SIM – If the IP address has this letter attached to it, it denotes a configuration file upgrade through the Single IP Management feature.
User	States the user who uploaded the configuration file. This field may read "Anonymous" or "Unknown" for users that are not identified.
Boot	If this field reads an asterisk (*), then this configuration file is the boot up configuration file for the Switch.

Current Configuration Settings

The following window is used to select one of the two possible configuration files that can be stored in the Switch as a boot up configuration file, or to select it for deletion from the Switch's memory.

To view this window, click **Save Services > Current Configuration Settings**, as shown below.

Figure 8 - 5 Configuration Settings window

This window holds the following information to be configured:

Parameter	Description
Configuration ID	Select the configuration file ID to be configured using the pull-down menu. The Switch allows two configuration file ID's to be stored in the Switch's memory.
Action	<p>This field has three options for configuration.</p> <ul style="list-style-type: none"> • <i>Delete</i> – Select this option to delete the configuration file ID specified in the Configuration ID field above. • <i>Boot_up</i> – Select this option to set the configuration file ID specified above as the boot up configuration file ID for the Switch. This firmware will be set as the boot up configuration file ID after a Switch reboot has been performed. The default setting has Configuration ID 1 as the boot up firmware image for the Switch unless specified here. • <i>Active</i> – Select this option to set the configuration file ID specified above as the file to be immediately implemented. Once selected and Apply is clicked, the Switch will upload this Configuration file for current use.

Click **Apply** to implement the changes.

Logout

Use the **Logout** page to logout of the Switch's Web-based management agent by clicking on the **Logout** button.

Figure 8 - 6 Logout window

Appendix A

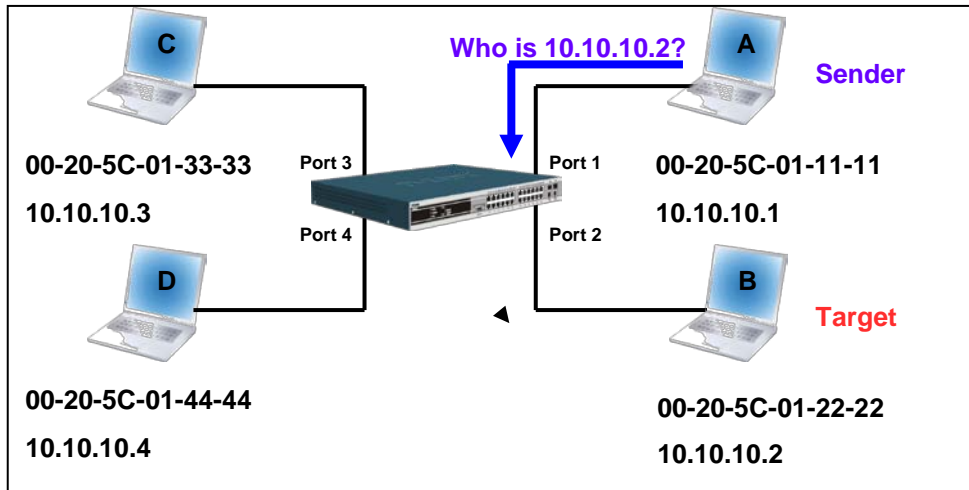
Mitigating ARP Spoofing Attacks Using Packet Content ACL

How Address Resolution Protocol works

Address Resolution Protocol (ARP) is the standard method for finding a host’s hardware address (MAC address) when only its IP address is known. However, this protocol is vulnerable because crackers can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This document is intended to introduce the ARP protocol, ARP spoofing attacks, and the countermeasures brought by D-Link’s switches to thwart ARP spoofing attacks.

In the process of ARP, PC A will first issue an ARP request to query PC B’s MAC address. The network structure is shown in Figure 1.

Figure 1



In the meantime, PC A’s MAC address will be written into the “Sender H/W Address” and its IP address will be written into the “Sender Protocol Address” in the ARP payload. As PC B’s MAC address is unknown, the “Target H/W Address” will be “00-00-00-00-00-00,” while PC B’s IP address will be written into the “Target Protocol Address,” shown in Table 1.

Table 1. ARP Payload

H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
				ARP request	00-20-5C-01-11-11	10.10.10.1	00-00-00-00-00-00	10.10.10.2

The ARP request will be encapsulated into an Ethernet frame and sent out. As can be seen in Table 2, the “Source Address” in the Ethernet frame will be PC A’s MAC address. Since an ARP request is sent via broadcast, the “Destination address” is in a format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Table 2. Ethernet Frame Format

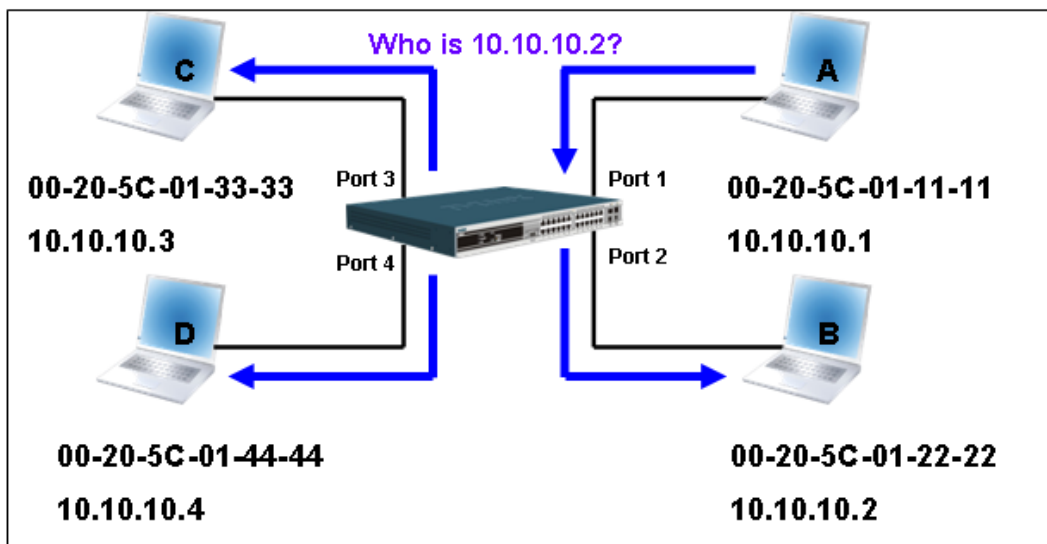
Destination Address	Source Address	Ether-Type	ARP	FCS
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11			

When the switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the switch will learn PC A’s MAC and the associated port into its Forwarding Table.



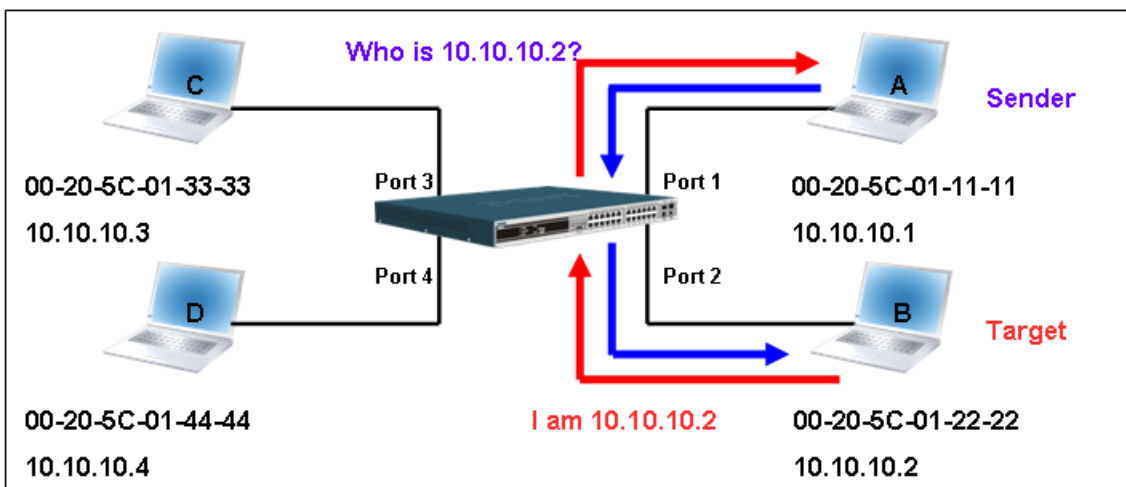
In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure 2).

Figure 2



When the switch floods the frame of ARP request to the network, all PCs will receive and examine the frame but only PC B will reply the query as the destination IP matched (see Figure 3).

Figure 3



When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload shown in Table 3. The ARP reply will be then encapsulated into an Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

Table 3. ARP Payload

H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
				ARP reply	00-20-5C-01-11-11	10.10.10.1	00-20-5C-01-22-22	10.10.10.2

When PC B replies to the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Table 4).

Table 4. Ethernet Frame Format

Destination Address	Source Address	Ether-Type	ARP	FCS
00-20-5C-01-11-11	00-20-5C-01-22-22			

The switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B’s MAC and update its Forwarding Table.

Forwarding Table

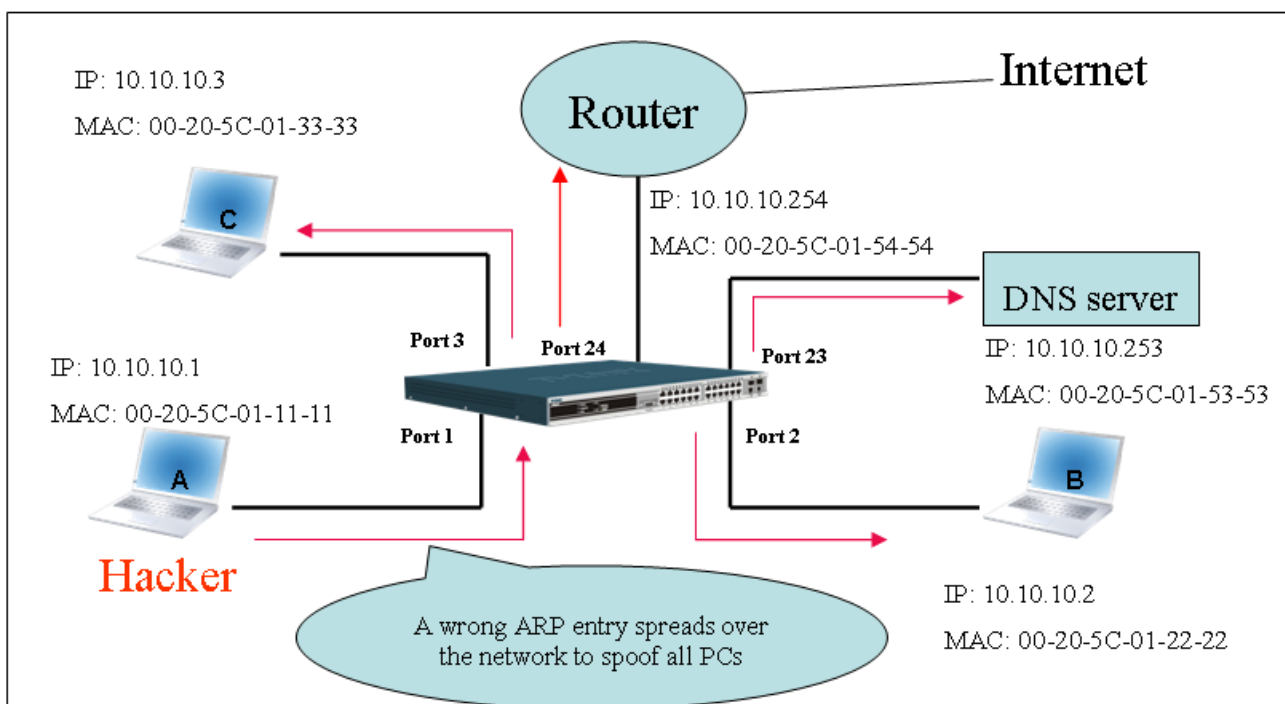
Port1 00-20-5C-01-11-11
Port2 00-20-5C-01-22-22

How ARP Spoofing Attacks a Network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service – DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

Figure 4



In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address itself. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is shown in the following table.

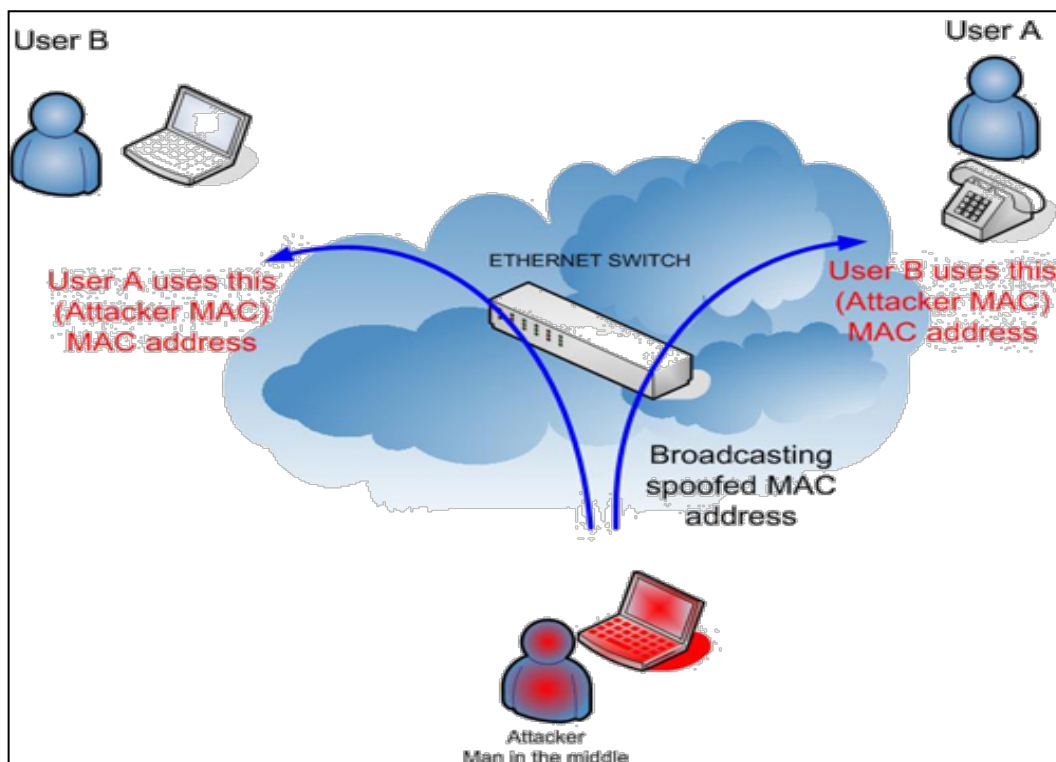
Table 5 **Gratuitous ARP**
Ethernet Header

Destination Address	Source Address	Ethernet Type	H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
(6-byte) FF-FF-FF-FF-FF-FF	(6-byte) 00-20-5C-01-11-11	(2-byte) 0806	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte) ARP relay	(6-byte) 00-20-5C-01-11-11	(4-byte) 10.10.10.254	(6-byte) 00-20-5C-01-11-11	(4-byte) 10.10.10.254

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim PC that it is a router and cheats the router that it is the victim. As can be seen in Figure 5 all traffic will be then sniffed by the hacker but the users will not discover.

Figure 5

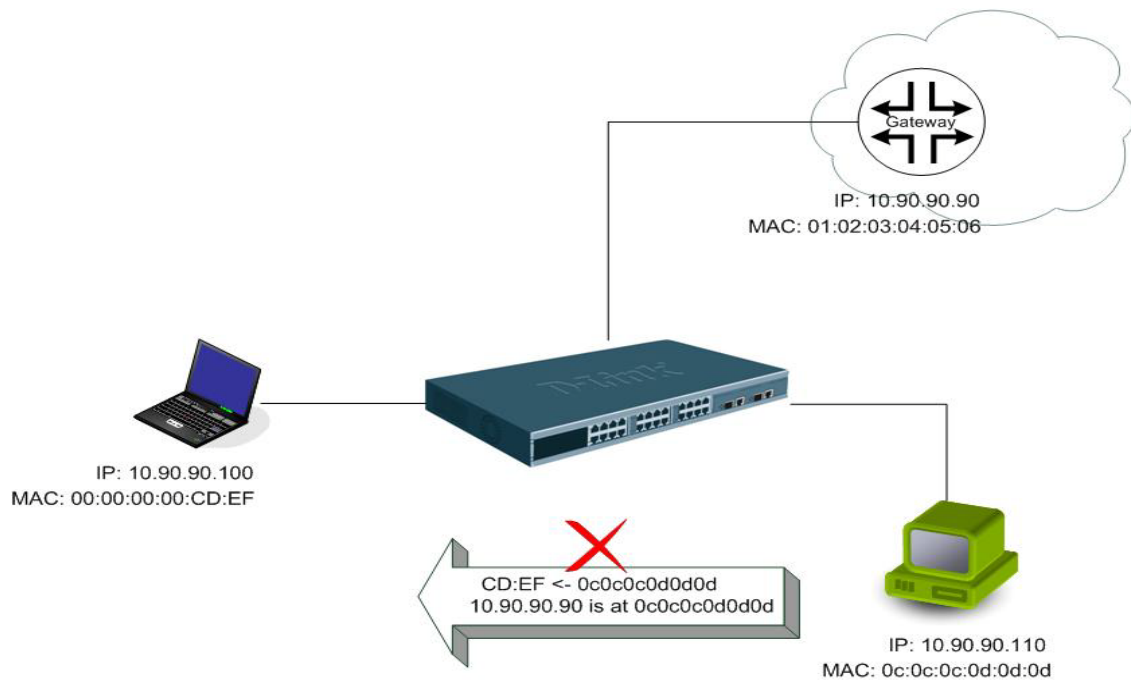


Prevent ARP Spoofing via Packet Content ACL

D-Link managed switches can effectively mitigate common DoS attacks caused by ARP spoofing via a unique Package Content ACL.

For the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source, and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here via using Packet Content ACL on the Switch to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

Example topology



Configuration

The configuration logic is as follows:

1. Only if the ARP matches Source MAC address in Ethernet, Sender MAC address and Sender IP address in ARP protocol can pass through the switch. (In this example, it is the gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL on the Switch enables users to inspect any offset chunk. An offset chunk is a 4-byte block in a HEX format, which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of four offset chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset chunks can be applied to each profile and a switch. Therefore, a careful consideration is needed for planning and configuration of the valuable offset chunks.

In Table 6, you will notice that the Offset_Chunk0 starts from the 127th byte and ends at the 128th byte. It also can be found that the offset chunk is scratched from 1 but not zero.

Table 6. Chunk and Packet Offset

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30	Offset Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

The following table indicates a completed ARP packet contained in Ethernet frame which is the pattern for the calculation of packet offset.

Table 7. A Completed ARP Packet Contained in an Ethernet Frame

Ethernet Header				ARP							
Destination Address	Source Address	Ethernet Type	H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
	01 02 03 04 05 06	0806							0a5a5a5a		
									(10.90.90.90)		

	command	description
Step1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	- Create access profile 1 To match Ethernet Type and Source MAC address.
Step2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-12 permit	- Config access profile 1 - Only if the gateway's ARP packet that contain the correct Source MAC address in the Ethernet frame can pass through the switch
Step3	create access_profile profile_id 2 packet_content_mask offset_chunk_1 3 0x0000 FFFF Ethernet Type(2-byte) offset_chunk_2 7 0x0000 FFFF SdrIP(Frist 2-byte) offset_chunk_3 8 0xFFFF 0000 SdrIP(Last 2-byte)	- Create access profile 2 - The frist Chunk starts from Chunk 3:mask for Ethernet Type (Bule in Table-6:13 th &14 th bytes) - The second Chunk stars from Chunk 7:mask for Sender IP (Frist 2-byte) in ARP packet (green in Table-6:29 th & 30 th bytes) - The third Chunk starts from Chunk 8:mask for Sender IP (Last 2-byte) in ARP packe (green in Table-6:31 th & 32 th bytes)
Step4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x0000 0806 Ethernet Type(2-byte):ARP offset_chunk_2 0x0000 0A5A SdrIP(Frist 2-byte):10.90 offset_chunk_3 0x 5A5A 0000 SdrIP(Last 2-byte):90.90 port1-12 deny	- Config access profile 2 - The rest ARP packet whose Sender IP claim they are the gateway's IP will be dropped.
Step5	save	- Save config

Appendix B

Switch Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

Category	Event Description	Log Information	Severity	Remark
system	System warm start	Unit <unitID>, System warm start	Critical	Unit ID only appears when stacking mode is enabled.
	System cold start	Unit <unitID>, System cold start	Critical	
	Configuration saved to flash	Unit <unitID>, Configuration saved to flash (Username: <username>)	Informational	
	System log saved to flash	Unit <unitID>, System log saved to flash (Username: <username>)	Informational	
	Configuration and log saved to flash	Unit <unitID>, Configuration and log saved to flash by console (Username: <username>)	Informational	
	Internal Power failed	Unit <unitID>, Internal Power failed	Critical	
	Internal Power is recovered	Unit <unitID>, Internal Power is recovered	Critical	
	Redundant Power failed	Unit <unitID>, Redundant Power failed	Critical	
	Redundant Power is working	Unit <unitID>, Redundant Power is working	Critical	
	Side Fan failed	Unit <unitID>, Side Fan failed	Critical	
	Side Fan recovered	Unit <unitID>, Side Fan recovered	Critical	
	Back Fan failed	Unit <unitID>, Back Fan failed	Critical	
	Back Fan recovered	Unit <unitID>, Back Fan recovered	Critical	
up/download	Firmware upgraded successfully	Unit <unitID>, Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgrade was unsuccessful	Unit <unitID>, Firmware upgrade by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging

	Configuration successfully downloaded	Configuration successfully downloaded by console (Username: <username>, IP: <ipaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration download was unsuccessful	Configuration download by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully uploaded	Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration upload was unsuccessful	Configuration upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message successfully uploaded	Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message upload was unsuccessful	Log message upload by console was unsuccessful! (Username: <username>, IP: <ipaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
Interface	Port link up	Port <unitID:portNum> link up, <link state>	Informational	link state, for ex: 100Mbps Full duplex
	Port link down	Port <unitID:portNum> link down	Informational	
	Port GBIC module occur errors	Port <unitID:portNum> GBIC module is abnormal	Warning	
Stacking	Hot insert	Unit <unitID>, MAC: <macaddr> Hot insert	Informational	
	Hot remove	Unit <unitID>, MAC: <macaddr> Hot remove	Informational	
	Firmware upgraded to slave successfully	Firmware upgraded by console successfully (Username: <username>, IP: <ipaddr>)	Informational	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgraded to slave unsuccessfully	Firmware upgraded by console unsuccessfully (Username: <username>, IP: <ipaddr>)	Warning	by console and "IP: <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console,

				will no IP and MAC information for logging
Console	Successful login through Console	Unit <unitID>, Successful login through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console	Unit <unitID>, Login failed through Console (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Logout through Console	Unit <unitID>, Logout through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Console session timed out	Unit <unitID>, Console session timed out (Username: <username>)	Informational	There are no IP and MAC if login by console.
Web	Successful login through Web	Successful login through Web (Username: <username>)	Informational	
	Login failed through Web	Login failed through Web (Username: <username>)	Warning	
	Logout through Web	Logout through Web (Username: <username>)	Informational	
	Web session timed out	Web session timed out (Username: <username>)	Informational	
	Successful login through Web (SSL)	Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	Login failed through Web (SSL)	Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	
	Logout through Web (SSL)	Logout through Web (SSL) (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
	Web (SSL) session timed out	Web (SSL) session timed out (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>)	Informational	
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>)	Informational	
SNMP	SNMP request received with invalid community string	SNMP request received from <ipaddress> with invalid community string	Informational	
STP	Topology changed	Topology changed (Instance: <instanceID>, Port:	Informational	

		<unitID:portNum>		
	CIST New Root selected	CIST New Root bridge selected (MAC: <macaddr>, Priority: <int>)	Informational	
	MSTI Root Selected	MSTI Regional New Root bridge selected (Instance: <instanceID>, MAC: <macaddr>, Priority: <int>)	Informational	
	BPDU Loop Back on port	BPDU Loop Back on Ports <unitID:portNum>	Warning	
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational	
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational	
DoS	Spoofing attack	Possible spoofing attack from IP <ipaddr> MAC <macAddress> port <portNum>	Critical	
SSH	Successful login through SSH	Successful login through SSH (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational	
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational	
	SSH server is enabled	SSH server is enabled	Informational	
	SSH server is disabled	SSH server is disabled	Informational	
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational	
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational	
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA local method	Successful login through Web from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Web authenticated by AAA local	Login failed through Web from <userIP> authenticated by AAA local method (Username: <username>)	Warning	

	method	<username>		
	Successful login through Web (SSL) authenticated by AAA local method	Successful login through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Web (SSL) authenticated by AAA local method	Login failed through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web (SSL) authenticated by AAA none method	Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	There are no IP and MAC if login by console.

	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Web (SSL) authenticated by AAA server	Successful login through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Web (SSL) authenticated by AAA server	Login failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web (SSL) due to AAA server timeout or improper configuration	Login failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Telnet due to AAA server timeout or improper configuration	Login failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through SSH authenticated by AAA server	Login failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through SSH due to AAA server timeout or improper	Login failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username:	Warning	

	configuration	<username>		
	Successful Enable Admin through Console authenticated by AAA local_enable method	Successful Enable Admin through Console authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Web(SSL) authenticated by AAA local_enable method	Successful Enable Admin through Web(SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Web (SSL) authenticated by AAA local_enable method	Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Telnet authenticated by AAA local_enable method	Enable Admin failed through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through SSH authenticated by AAA local_enable method	Enable Admin failed through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	

	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Web (SSL) authenticated by AAA none method	Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web due to AAA server timeout or improper configuration	Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Web (SSL) authenticated by AAA server	Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	

		<username>		
	Enable Admin failed through Web (SSL) authenticated by AAA server	Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web (SSL) due to AAA server timeout or improper configuration	Enable Admin failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Telnet due to AAA server timeout or improper configuration	Enable Admin failed through Telnet from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	AAA server timed out	AAA server <serverIP> (Protocol: <protocol>) connection failed	Warning	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
	AAA server ACK error	AAA server <serverIP> (Protocol: <protocol>) response is wrong	Warning	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
	AAA does not support this functionality	AAA doesn't support this functionality	Informational	
IP-MAC-Port Binding	Unauthenticated IP address encountered and discarded by ip IP-MAC port binding	Unauthenticated IP-MAC address and discarded by IP-MAC port binding (IP: <ipaddr>, MAC: <macaddr>, Port: <unitID:portNum>)	Warning	

	Dynamic IMPB entry is in conflict with static ARP	Dynamic IMPB entry is conflict with static ARP(IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>)	Warning	
	Dynamic IMPB entry conflicts with static IMPB	Dynamic IMPB entry conflicts with static IMPB: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>	Warning	
	IMPB entry cannot be created in ACL mode due to no ACL rules	IMPB entry cannot be created in ACL mode due to no ACL rules: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>	Warning	
	Port enter stop learning state	Port <> IMPB stop learning state	Warning	
	Port recover normal state	Port <> IMPB normal state	Warning	
IP and Password Changed	IP Address change activity	Unit <unitID>, Management IP address was changed by (Username: <username>,IP:<ipaddr>,MAC:<macaddr>)	Informational	
	Password change activity	Unit <unitID>, Password was changed by (Username: <username>,IP:<ipaddr>,MAC:<macaddr>)	Informational	
Dual Configuration	Execution error encountered during system boot-up	Configuration had <int> syntax error and <int> execute error	Warning	
Safeguard Engine	Safeguard Engine is in normal mode	Unit <unitID>, Safeguard Engine enters NORMAL mode	Informational	
	Safeguard Engine is in filtering packet mode	Unit < unitID>, Safeguard Engine enters EXHAUSTED mode	Warning	
Packet Storm	Broadcast storm occurrence	Port <unitID:portNum> Broadcast storm is occurring	Warning	
	Broadcast storm cleared	Port <unitID:portNum> Broadcast storm has cleared	Informational	
	Multicast storm occurrence	Port <unitID:portNum> Multicast storm is occurring	Warning	
	Multicast storm cleared	Port <unitID:portNum> Multicast storm has cleared	Informational	
	Port shut down due to a packet storm	Port <unitID:portNum> is currently shut down due to a packet storm	Warning	
MAC-based Access Control	A host failed to pass uthentication.	MBAC unauthenticated host(MAC: <macaddr>, Port <[unitID:]portNum>, VID: <vid>)	Critical	

	The authorized number of users on a port has reached the maximum user limit.	Port < [unitID:]portNum> enters MBAC stop learning state.	Warning	
	The authorized number of users on a port is below the maximum user limit in a time interval (interval is project dependent).	Port <[unitID:]portNum> recovers from MBAC stop learning state.	Warning	
	The authorized number of users on the whole device has reached the maximum user limit.	MBAC enters stop learning state.	Warning	
	The authorized number of users on the whole device is below the maximum user limit in a time interval (interval is project depended).	MBAC recovers from stop learning state.	Warning	
JWAC	When a client host authenticated successful.	JWAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Warning	
	When a client host fails to authenticate.	JWAC unauthenticated user (User Name: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Warning	
	This log will be triggered when the number of authorized users reaches the maximum user limit on the whole device.	JWAC enters stop learning state.	Warning	
	This log will be triggered when the number of authorized users is below the maximum user limit on the whole device in a time interval (The interval is project dependent).	JWAC recovered from stop learning state.	Warning	
WAC	When a client host fail to authenticate.	WAC unauthenticated user (User Name: <string>, IP: <ipaddr ipv6address>, MAC: <macaddr>, Port: <[unitID:]portNum>)	Warning	
	This log will be triggered when the authorized user number reaches the max user limit on	WAC enters stop learning state.	Warning	

	whole device.			
	This log will be triggered when the authorized user number is below the max user limit on whole device in a time interval (interval is project depended)	WAC recovers from stop learning state.	Warning	

Appendix C

Trap Logs

This table lists the trap logs found on the DGS-3400 Series Switches.

MACNotifyTrap	This trap indicates the MAC address variations in the address table.	1.3.6.1.4.1.171.11.70.1.2.16.1.2.0.1 1.3.6.1.4.1.171.11.70.2.2.16.1.2.0.1 1.3.6.1.4.1.171.11.70.3.2.16.1.2.0.1 1.3.6.1.4.1.171.11.70.7.2.16.1.2.0.1
PortLoopOccurredTrap	This trap is sent when a Port loop occurs.	1.3.6.1.4.1.171.11.70.1.2.16.1.2.0.0.3 1.3.6.1.4.1.171.11.70.2.2.16.1.2.0.0.3 1.3.6.1.4.1.171.11.70.3.2.16.1.2.0.0.3 1.3.6.1.4.1.171.11.70.7.2.16.1.2.0.0.3
PortLoopRestart	This trap is sent when a Port loop restarts after the interval time.	1.3.6.1.4.1.171.11.70.1.2.16.1.2.0.0.4 1.3.6.1.4.1.171.11.70.2.2.16.1.2.0.0.4 1.3.6.1.4.1.171.11.70.3.2.16.1.2.0.0.4 1.3.6.1.4.1.171.11.70.7.2.16.1.2.0.0.4
VlanLoopOccurred	This trap is sent when a Port with a VID loop occurs.	1.3.6.1.4.1.171.11.70.1.2.16.1.2.0.0.5 1.3.6.1.4.1.171.11.70.2.2.16.1.2.0.0.5 1.3.6.1.4.1.171.11.70.3.2.16.1.2.0.0.5 1.3.6.1.4.1.171.11.70.7.2.16.1.2.0.0.5

VlanLoopRestart	This trap is sent when a Port with a VID loop restarts after the interval time.	1.3.6.1.4.1.171.11.70.1.2.16.1.2.0.0.6 1.3.6.1.4.1.171.11.70.2.2.16.1.2.0.0.6 1.3.6.1.4.1.171.11.70.3.2.16.1.2.0.0.6 1.3.6.1.4.1.171.11.70.7.2.16.1.2.0.0.6
CpuProtectChgToExhausted	This trap indicates System change operation mode from normal to exhausted.	1.3.6.1.4.1.171.12.19.4.1.0.1
SafeGuardChgToNormal	This trap indicates System change operation mode from exhausted to normal.	1.3.6.1.4.1.171.12.19.4.1.0.2
PktStormOccurred	This trap is sent when a packet storm is detected by the packet storm mechanism and takes shutdown as an action.	1.3.6.1.4.1.171.12.25.5.0.1
PktStormCleared	This trap is sent when the packet storm is cleared by the packet storm mechanism.	1.3.6.1.4.1.171.12.25.5.0.2
IpMACBindTrap	When the IP-MAC Binding trap is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out.	1.3.6.1.4.1.171.12.23.5.0.1
MacBasedAuthLoggedSuccess	This trap is sent when a MAC-based access control host is successfully logged in.	1.3.6.1.4.1.171.12.35.11.1.0.1
MacBasedAuthLoggedFail	This trap is sent when a MAC-based access control host login fails.	1.3.6.1.4.1.171.12.35.11.1.0.2
MacBasedAuthAgesOut	This trap is sent when a MAC-based access control host ages out.	1.3.6.1.4.1.171.12.35.11.1.0.3
FilterDetectedTrap	This trap is sent when an illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration.	1.3.6.1.4.1.171.12.37.100.0.1
SingleIPMSColdStart	Commander switch will send swSingleIPMSColdStart notification to indicated host when its Member generate cold start notification.	1.3.6.1.4.1.171.12.8.6.0.11
SingleIPMSWarmStart	The commander switch will send swSingleIPMSWarmStart notification to the indicated host when its member generates a warm start notification.	1.3.6.1.4.1.171.12.8.6.0.12
SingleIPMSLinkDown	The commander switch will send swSingleIPMSLinkDown notification to the indicated host when its member generates a link down notification.	1.3.6.1.4.1.171.12.8.6.0.13
SingleIPMSLinkUp	The commander switch will send swSingleIPMSLinkUp notification to the indicated host when its member generates a link up notification.	1.3.6.1.4.1.171.12.8.6.0.14

SingleIPMSAuthFail	The commander switch will send swSingleIPMSAuthFail notification to the indicated host when its member generates an authentication failure notification	1.3.6.1.4.1.171.12.8.6.0.15
SingleIPMSnewRoot	The commander switch will send swSingleIPMSnewRoot notification to the indicated host when its member generates a new root notification.	1.3.6.1.4.1.171.12.8.6.0.16
SingleIPMSTopologyChange	The commander switch will send swSingleIPMSTopologyChange notification to the indicated host when its member generates a topology change notification.	1.3.6.1.4.1.171.12.8.6.0.17
PowerStatusChg	<p>Power Status change notification. The notification is issued when the swPowerStatus changes in the following cases:</p> <p>lowVoltage -> overCurrent. owVoltage -> working. lowVoltage -> disconnect. lowVoltage -> connect. overCurrent -> lowVoltage. overCurrent -> working. overCurrent -> disconnect. overCurrent -> connect. working -> lowVoltage. working -> overCurrent. working -> connect. working -> disconnect. fail -> connect. fail -> disconnect. connect -> lowVoltage. connect -> overCurrent. connect -> working. connect -> disconnect. disconnect -> lowVoltage. disconnect -> overCurrent. disconnect -> working. disconnect -> connect.</p>	1.3.6.1.4.1.171.12.11.2.2.2.0.1
PowerFailure	<p>Power Failure notification. The notification is issued when the swPowerStatus changes in the following cases:</p> <p>lowVoltage -> fail. overCurrent -> fail. working -> fail. connect -> fail. disconnect -> fail.</p>	1.3.6.1.4.1.171.12.11.2.2.2.0.2

PowerRecover	Power Recover notification. The notification is issued when the swPowerStatus changes in the following cases: fail -> lowVoltage. fail -> overCurrent. fail -> working.	1.3.6.1.4.1.171.12.11.2.2.2.0.3
agentGratuitousARPTrap	This trap is sent when there is an IP address conflict.	1.3.6.1.4.1.171.12.1.7.2.0.5
FanFailure	Fan Failure notification.	1.3.6.1.4.1.171.12.11.2.2.3.0.1
FanRecover	Fan Recover notification.	1.3.6.1.4.1.171.12.11.2.2.3.0.2
coldStart	A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.	1.3.6.1.6.3.1.1.5.1
warmStart	A warmStart trap signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is altered.	1.3.6.1.6.3.1.1.5.2
linkDown	A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.	1.3.6.1.6.3.1.1.5.3
linkUp	A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.	1.3.6.1.6.3.1.1.5.4
authenticationFailure	An authenticationFailure trap signifies that the sending protocol entity is the address of a protocol message that is not properly authenticated. While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation- specific mechanism.	1.3.6.1.6.3.1.1.5.5
RisingAlarmTrap	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps.	1.3.6.1.2.1.16.0.1
FallingAlarmTrap	The SNMP trap that is generated when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps.	1.3.6.1.2.1.16.0.2
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon action of the Topology Change Timer immediately subsequent to	1.3.6.1.2.1.17.0.1

	its election. Implementation of this trap is optional.	
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.2
IldpRemTablesChange	A IldpRemTablesChange notification is sent when the value of IldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls.	1.0.8802.1.1.2.0.0.1

Glossary

1000BASE-SX: A short laser wavelength on multimode fiber optic cable for a maximum length of 550 meters

1000BASE-LX: A long wavelength for a “long haul” fiber optic cable for a maximum length of 10 kilometers

100BASE-FX: 100Mbps Ethernet implementation over fiber.

100BASE-TX: 100Mbps Ethernet implementation over Category 5 and Type 1 Twisted Pair cabling.

10BASE-T: The IEEE 802.3 specification for Ethernet over Unshielded Twisted Pair (UTP) cabling.

aging: The automatic removal of dynamic entries from the Switch Database which have timed-out and are no longer valid.

ATM: Asynchronous Transfer Mode. A connection oriented transmission protocol based on fixed length cells (packets). ATM is designed to carry a complete range of user traffic, including voice, data and video signals.

auto-negotiation: A feature on a port which allows it to advertise its capabilities for speed, duplex and flow control. When connected to an end station that also supports auto-negotiation, the link can self-detect its optimum operating setup.

backbone port: A port which does not learn device addresses, and which receives all frames with an unknown address. Backbone ports are normally used to connect the Switch to the backbone of your network. Note that backbone ports were formerly known as designated downlink ports.

backbone: The part of a network used as the primary path for transporting traffic between network segments.

bandwidth: Information capacity, measured in bits per second, that a channel can transmit. The bandwidth of Ethernet is 10Mbps, the bandwidth of Fast Ethernet is 100Mbps.

baud rate: The switching speed of a line. Also known as line speed between network segments.

BOOTP: The BOOTP protocol allows automatic mapping of an IP address to a given MAC address each time a device is started. In addition, the protocol can assign the subnet mask and default gateway to a device.

bridge: A device that interconnects local or remote networks no matter what higher level protocols are involved. Bridges form a single logical network, centralizing network administration.

broadcast: A message sent to all destination devices on the network.

broadcast storm: Multiple simultaneous broadcasts that typically absorb available network bandwidth and can cause network failure.

console port: The port on the Switch accepting a terminal or modem connector. It changes the parallel arrangement of data within computers to the serial form used on data transmission links. This port is most often used for dedicated local management.

CSMA/CD: Channel access method used by Ethernet and IEEE 802.3 standards in which devices transmit only after finding the data channel clear for some period of time. When two devices transmit simultaneously, a collision occurs and the colliding devices delay their retransmissions for a random amount of time.

data center switching: The point of aggregation within a corporate network where a switch provides high-performance access to server farms, a high-speed backbone connection and a control point for network management and security.

Ethernet: A LAN specification developed jointly by Xerox, Intel and Digital Equipment Corporation. Ethernet networks operate at 10Mbps using CSMA/CD to run over cabling.

Fast Ethernet: 100Mbps technology based on the CSMA/CD network access method.

Flow Control: (IEEE 802.3X) A means of holding packets back at the transmit port of the connected end station. Prevents packet loss at a congested switch port.

forwarding: The process of sending a packet toward its destination by an internetworking device.

full duplex: A system that allows packets to be transmitted and received at the same time and, in effect, doubles the potential throughput of a link.

half duplex: A system that allows packets to be transmitted and received, but not at the same time. Contrast with full duplex.

IP address: Internet Protocol address. A unique identifier for a device attached to a network using TCP/IP. The address is written as four octets separated with full-stops (periods), and is made up of a network section, an optional subnet section and a host section.

IPX: Internetwork Packet Exchange. A protocol allowing communication in a NetWare network.

LAN - Local Area Network: A network of connected computing resources (such as PCs, printers, servers) covering a relatively small geographic area (usually not larger than a floor or building). Characterized by high data rates and low error rates.

latency: The delay between the time a device receives a packet and the time the packet is forwarded out of the destination port.

line speed: See baud rate.

main port: The port in a resilient link that carries data traffic in normal operating conditions.

MDI - Medium Dependent Interface: An Ethernet port connection where the transmitter of one device is connected to the receiver of another device.

MDI-X - Medium Dependent Interface Cross-over: An Ethernet port connection where the internal transmit and receive lines are crossed.

MIB - Management Information Base: Stores a device's management characteristics and parameters. MIBs are used by the Simple Network Management Protocol (SNMP) to contain attributes of their managed systems. The Switch contains its own internal MIB.

multicast: Single packets copied to a specific subset of network addresses. These addresses are specified in the destination-address field of the packet.

protocol: A set of rules for communication between devices on a network. The rules dictate format, timing, sequencing and error control.

resilient link: A pair of ports that can be configured so that one will take over data transmission should the other fail. See also main port and standby port.

RJ-45: Standard 8-wire connectors for IEEE 802.3 10BASE-T networks.

RMON: Remote Monitoring. A subset of SNMP MIB II that allows monitoring and management capabilities by addressing up to ten different groups of information.

RPS - Redundant Power System: A device that provides a backup source of power when connected to the Switch.

server farm: A cluster of servers in a centralized location serving a large user population.

SLIP - Serial Line Internet Protocol: A protocol which allows IP to run over a serial line connection.

SNMP - Simple Network Management Protocol: A protocol originally designed to be used in managing TCP/IP internets. SNMP is presently implemented on a wide range of computers and networking equipment and may be used to manage many aspects of network and end station operation.

Spanning Tree Protocol (STP): A bridge-based system for providing fault tolerance on networks. STP works by allowing the user to implement parallel paths for network traffic, and ensure that redundant paths are disabled when the main paths are operational and enabled if the main paths fail.

Stack: A group of network devices that are integrated to form a single logical device.

standby port: The port in a resilient link that will take over data transmission if the main port in the link fails.

switch: A device which filters, forwards and floods packets based on the packet's destination address. The switch learns the addresses associated with each switch port and builds tables based on this information to be used for the switching decision.

TCP/IP: A layered set of communications protocols providing Telnet terminal emulation, FTP file transfer, and other services for communication among a wide range of computer equipment.

Telnet: A TCP/IP application protocol that provides virtual terminal service, letting a user log in to another computer system and access a host as if the user were connected directly to the host.

TFTP - Trivial File Transfer Protocol: Allows the user to transfer files (such as software upgrades) from a remote device using your switch's local management capabilities.

UDP - User Datagram Protocol: An Internet standard protocol that allows an application program on one device to send a datagram to an application program on another device.

VLAN - Virtual LAN: A group of location- and topology-independent devices that communicate as if they are on a common physical LAN.

VLT - Virtual LAN Trunk: A Switch-to-Switch link which carries traffic for all the VLANs on each Switch.

VT100: A type of terminal that uses ASCII characters. VT100 screens have a text-based appearance.