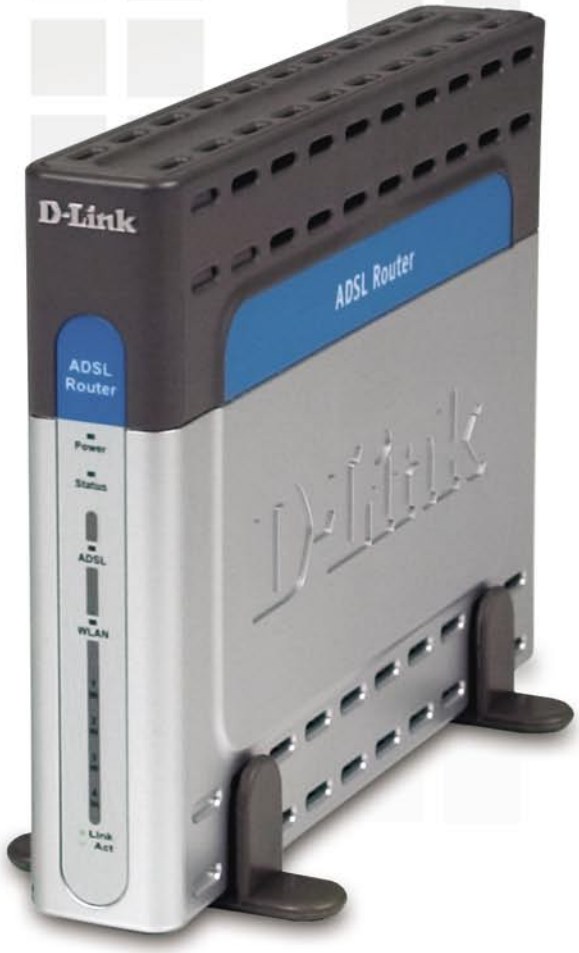
D-Link®
Building Networks for People



Manual

Version 1.0

DSL-504T

ADSL Router

Table of Contents

Table of Contents 2
Package Contents 4
Installation Overview 5
Installation Requirements 6
Information you will need from your ADSL service provider 8
Information you will need about your DSL-504T ADSL service router 9
Information you will need about your LAN or computer 10
Introduction 11
Features and Benefits 12
Standards Compatibility & Compliance 14
Front Panel Display 16
Rear Panel Connections 17
Hardware Installation 18
Power ON Router 19
Network Connections 20
Basic Router Configuration 22
Access the Configuration Manager 29
Login to the Home Page 30
Configure the Router 31
Using the Setup Wizard 33
Configuring the WAN connection 46
LAN IP Settings 55
DHCP Server Settings 56
DNS Server Settings 58

Advanced Settings 60
Tools 72
Status 79
Multiple Virtual Connections 83
Technical Specifications 85
Appendix A: IP Address Setup 87
Appendix B: IP Concepts 90
Appendix C: Microfilters & Splitters 93
Contacting Technical Support 95
Warranty 96
Registration 99

Package Contents

- **D-Link DSL-504T**
  ADSL Ethernet Router
- One twisted-pair telephone cable used for ADSL connection
- One straight-through Ethernet cable
- Manual on CD
- Quick Installation Guide
- One AC power adapter

If any of the above items are missing, please contact your reseller.

Installation Overview

The procedure to install the Router can be described in general terms in the following steps:

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.
2. Install the hardware, that is, connect the cables (Ethernet and telephone) to the device and connect the power adapter.
3. Check the IP settings on your computer and change them if necessary so the computer can access the web-based software built into the Router.
4. Use the web-based management software to configure the device to suit the requirements of your ADSL account.

Installation Requirements

In order to establish a connection to the Internet it will be necessary to provide information to the Router that will be stored in its memory. For some users, only their account information (Username and Password) is required. For others, various parameters that control and define the Internet connection will be required. You can print out the two pages below and use the tables to list this information. This way you have a hard copy of all the information needed to setup the Router. If it is necessary to reconfigure the device, all the necessary information can be easily accessed. Be sure to keep this information safe and private.

Low Pass Filters

Since ADSL and telephone services share the same copper wiring to carry their respective signals, a filtering mechanism may be necessary to avoid mutual interference. A low pass filter device can be installed for each telephone that shares the line with the ADSL line. These filters are easy to install passive devices that connect to the ADSL device and/or telephone using standard telephone cable. Ask your service provider for more information about the use of low pass filters with your installation.

Operating Systems

The DSL-504T uses an HTML-based web interface for setup and management. The web configuration manager may be accessed using any operating system capable of running web browser software, including Windows 98 SE, Windows ME, Windows 2000, and Windows XP.

Web Browser

Any common Web browser can be used to configure the Router using the web configuration management software. The program is designed to work best with more recently released browsers such as Opera, Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)

Any computer that uses the router must be able to connect to it through the Ethernet port on the Router. This connection is an Ethernet connection and therefore requires that your computer be equipped with an Ethernet port as well. Most notebook computers are now sold with an Ethernet port already installed. Likewise, most fully assembled desktop computers come with an Ethernet NIC adapter as standard equipment. If your computer does not have an Ethernet port, you must install an Ethernet NIC adapter before you can use the Router. If you must install an adapter, follow the installation instructions that come with the Ethernet NIC adapter.

Additional Software

It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using the device a simple bridge. For a bridged connection, the information needed to make and maintain the Internet connection is stored on another computer or gateway device, not in the Router itself.

If your ADSL service is delivered through a Dynamic, PPPoE/PPPoA, Static, or Bridge connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

All connections to the Internet require a unique global IP address. For bridged connections, the global IP settings must reside in a TCP/IP enabled device on the LAN side of the bridge, such as a PC, a server, a gateway device such as a router or similar firewall hardware. The IP address can be assigned in a number of ways. Your network service provider will give you instructions about any additional connection software or NIC configuration that may be required.

Information you will need from your ADSL service provider

Username This is the Username used to log on to your ADSL service provider's network. It is commonly in the form - user@isp.com. Your ADSL service provider uses this to identify your account.

Password This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account.

Connection Protocol This is the method your ADSL service provider uses to send and receive data between the Internet and your computer. Your Modem supports the following connection protocols: Dynamic, PPPoE/PPPoA, Static, or Bridge.

Protocol This is the method your ADSL service provider will use to verify your Username and Password when you log on to their network. Your Modem supports the PAP and CHAP protocols.

VPI This is the Virtual Path Identifier (VPI). It is used in conjunction with the Virtual Channel Identifier (VCI) below, to identify the data path between your ADSL service provider's network and your computer.

VCI This is the Virtual Channel Identifier (VCI). It is used in conjunction with the VPI above to identify the data path between your ADSL service

Information you will need about your DSL-504T ADSL router

Username This is the Username needed access the Modem's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Modem is **admin**. This is a default setting and can NOT be changed.

Password This is the Password you will be prompted to enter when you access the Modem's management interface. The default Password is **admin**. This may be changed by the user.

LAN IP addresses for the DSL-504T This is the IP address you will enter into the Address field of your web browser to access the Modem's configuration graphical user interface (GUI) using a web browser. The default IP address is 192.168.1.1 and it is referred to as the "Management IP" address in this User's Manual. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled.

LAN Subnet Mask for the This is the subnet mask used by the DSL-504T, and will be used throughout your LAN. The default subnet mask is **255.255.255.0**. This can be changed later.

Information you will need about your LAN or computer

Ethernet NIC If your computer has an Ethernet NIC, you can connect the DSL-504T to this Ethernet port using an Ethernet cable. You can also use the Ethernet port on the DSL-504T to connect to other Ethernet devices, such as a Wireless Access Point.

DHCP Client status Your DSL-504T ADSL Modem is configured, by default, to be a DHCP server. This means that it can assign an IP address, subnet mask, and a default gateway address to computers on your LAN. The default range of IP addresses the DSL-504T will assign are from **192.168.1.2** to **192.168.1.254**. Your computer (or computers) needs to be configured to **Obtain an IP address automatically** (that is, they need to be configured as

It is recommended that your collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your DSL-504T ADSL Router.

The Modem may be reset to its factory default settings by performing a Restore settings operation within the management interface (see System Commands). If you cannot gain access to the management interface, you may opt to use the Reset button on the rear panel of the device).

Introduction

Router Description and Operation

The DSL-504T ADSL Router is designed to provide a simple and cost-effective ADSL Internet connection for individual computers through the Ethernet ports, or use it to bridge your Ethernet LAN to the Internet. The DSL-504T combines the benefits of high-speed ADSL technology and LAN IP management in one compact and convenient package. ADSL technology enables many interactive multi-media applications such as video conferencing and collaborative computing.

The Router is easy to install and use. The DSL-504T connects to computers or an Ethernet LAN via a standard Ethernet interface. The ADSL connection is made using ordinary twisted-pair telephone line with standard connectors. Multiple PCs can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address.

The Router supports transparent bridging and can be used for IP packet routing over the Internet. Cost saving features of the Router such as NAT (Network Address Translator) and DHCP (Dynamic Host Configuration Protocol) improve administration efficiency and improve security for your private network. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

What is ADSL?

Asymmetric Digital Subscriber Line (ADSL) is an access technology that utilizes ordinary copper telephone lines to enable broadband high-speed digital data transmission and interactive multimedia applications for business and residential customers.

ADSL greatly increases the signal carrying capacity of copper telephone lines without interfering with regular telephone services. For the ADSL user, this means faster downloads and more reliable connectivity. ADSL devices make it possible to enjoy benefits such as high-speed Internet access without experiencing any loss of quality or disruption of voice/fax telephone capabilities.

ADSL provides a dedicated service over a single telephone line operating at speeds of up to 8 Mbps downstream and up to 640 Kbps upstream, depending on local telephone line conditions. A secure point-to-point connection is established between the user and the central office of the service provider.

D-Link ADSL devices incorporate the recommendations of the ADSL Forum regarding framing, data format, and upper layer protocols.

Features and Benefits

The DSL-504T ADSL Router utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. DSL-504T advantages include:

- **PPP (Point-to-Point Protocol) Security –** The DSL-504T ADSL Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.
- **DHCP Support –** Dynamic Host Configuration Protocol automatically and dynamically assigns all LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT) –** For small office environments, the DSL-504T allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user.

  NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.
- **TCP/IP (Transfer Control Protocol/Internet Protocol) –** The DSL-504T supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.
- **RIP-1/RIP-2 –** The DSL-504T supports both RIP1 and RIP-2 exchanges with other routers. Using both versions allows the Router to communicate with all RIP enabled devices
- **Static Routing –** This allows you to select a data path to a particular network destination that will remain in the routing table and never "age out". If you wish to define a specific route that will always be used for data traffic from your LAN to a specific destination within your LAN (for example to another router or a server) or outside your network (to a ISP defined default gateway for instance).
- **Default Routing –** This allows you to choose a default path for incoming data packets for which the destination address is unknown. This is particularly useful when the Router functions as the sole connection to the Internet.
- **ATM (Asynchronous Transfer Mode) –** The DSL-504T supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577) and PPP over ATM (RFC 2364).

- **Precise ATM Traffic Shaping –** Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer
- **G.hs (Auto-handshake) –** This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.
- **High Performance –** Very high rates of data transfer are possible with the Router. Up to eight Mbps downstream bit rate using the G.dmt standard.
- **Full Network Management –** The DSL-504T incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via Telnet connection.
- **Telnet Connection –** Telnet enables a network manager to access the Router's management software remotely.
- **Easy Installation –** The DSL-504T uses a web-based graphical user interface program for convenient management access and easy set up. Any Web browser, that meets the minimum requirements, can be used to manage the Router.

Standards Compatibility & Compli-

The DSL-504T complies with or is compatible with the following standards as recognized by their respective agencies.

- ITU G.992.2 (G.lite, "splitterless ADSL") compliant
- ITU-T Rec. I.361 compliant
- RFC 791 Internet Protocol compliant
- RFC 792 UDP compliant
- RFC 826 Address Resolution Protocol compliant (ARP) compliant
- RFC 1058 Routing Information Protocol (RIP) compliant
- RFC 1213 MIB II for IP compliant
- RFC 1334 PPP Authentication Protocol compliant
- RFC 1389 Routing Information Protocol 2 (RIP2) compliant
- RFC 1483 IP over AAL5/ Bridged Ethernet over AAL5 compliant
- RFC 1557 Classical IP over ATM (IPoA) compliant
- RFC 1661 Point to Point Protocol (PPP) compliant
- RFC 1877 Automatic IP assignment compliant
- RFC 1994 Challenge Handshake Authentication Protocol compliant
- Supports RFC 2131 and RFC 2132 DHCP functions including: automatic assignment of IP address, use of subnet mask and default gateway and provision of DNS server address for all hosts
- RFC 2364 PPP over ATM compliant (PPPoA) compliant
- RFC 2516 PPP over Ethernet compliant (PPPoE) compliant
- RFC 2684 Bridged/Routed Ethernet over ATM compliant
- IEEE 802.3 compliant
- IEEE 802.3u compliant
- IEEE 802.1d compliant
- IEEE 802.3x compliant
- Embedded web server support
- Supports Dynamic Learning
- Supports Static Routing

- Supports NAPT for up to 4096 connections
- Supports DHCP for up to 253 hot connections
- Supports IGMP
- Supports ATM Forum UNI 3.1/4.0
- Supports ATM VCC (Virtual Channel Circuit) for up to eight sessions
- Supports TELNET and TFTP
- Supports back pressure for half-duplex

Front Panel Display

Place the Router in a location that permits an easy view of the LED indicators on the front panel.
The LED indicators on the front panel include the **Power**, **Status**, **ADSL** and **WLAN** and **Ethernet (1-4) Link/Act** indicators. The ADSL, WLAN and Ethernet indicators monitor link status and activity (Link/Act).

Power	A solid green light indicates the unit is powered on. When the device is powered off this remains off.
Status	Lights solid green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator light is off after the POST, the system has failed and the device should be rebooted.
ADSL (Link/Act)	A solid green light indicates a valid ADSL connection. A blinking green light indicates activity on the WAN (ADSL) interface.
Ethernet Ports (1-4):	A solid light indicates a connection on the associated port. A blinking light indicates activity on the associated port.

Rear Panel Connections

All cable connections to the Router are made at the rear panel. Connect the power adapter here to power on the Router. Use the Reset button to restore the settings to the factory default values. Please see the Hardware Installation section in this manual for more information about the Reset button.

ADSL Port
Use the ADSL cable to connect to the your telephone line (RJ-11 port)

Ethernet ports
Use the Ethernet ports to connect the Router to your Ethernet LAN or Ethernet devices

Reset button
To manually reset to the manufacturer's default setting, depress button with the power on for at least seven seconds

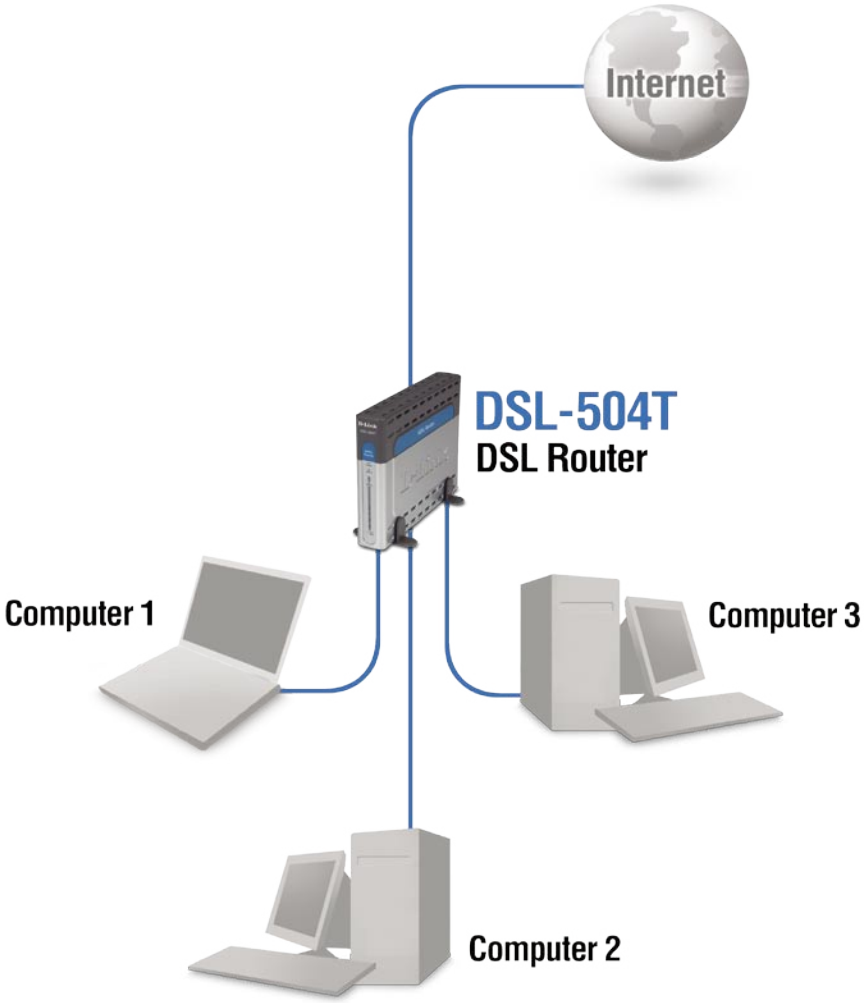
Power Insert
Use the adapter shipped with the Router to connect to power source

To manually reboot the Router, disconnect and then reconnect the power.

Hardware Installation

The DSL-504T maintains five separate interfaces, four Ethernet and one ADSL interface. Place the Router in a location where it can be safely connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety precautions.

The access point can be placed on a shelf or desktop, ideally you should be able to see the LED indicators on the front if you need to view them for troubleshooting.



Power On Router

CAUTION: The Router must be used with the power adapter included with the device.

To power on the Router:

1. Insert the AC Power Adapter cord into the power receptacle located on the rear panel of the Router and plug the adapter into a suitable nearby power source.
2. You should see the Power LED indicator light up and remain lit. The Status LED should light solid green and begin to blink after a few seconds.
3. If the Ethernet port is connected to a working device, check the Ethernet Link/Act LED indicators to make sure the connection is valid. The Router will attempt to establish the ADSL connection, if the ADSL line is connected and the Router is properly configured this should light up after several seconds. If this is the first time installing the device, some settings may need to be changed before the Router can establish a connection.

Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button for at least seven seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address 192.168.1.1 and the subnet mask is 255.255.255.0, the default management Username is **admin** and the default Password is **admin**.

Network Connections

Network connections are provided through the ADSL port and the four Ethernet ports on the back of the Router. See the Rear Panel diagram and the illustrations below for examples.

Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket or receptacle. Plug one end of the cable into the ADSL port (RJ-11 receptacle) on the rear panel of the Router and insert the other end into the RJ-11 wall socket. If you are using a low pass filter device, follow the instructions included with the device or given to you by your service provider. The ADSL connection represents the WAN interface, the connection to the Internet. It is the physical link to the service provider's network backbone and ultimately to the Internet.

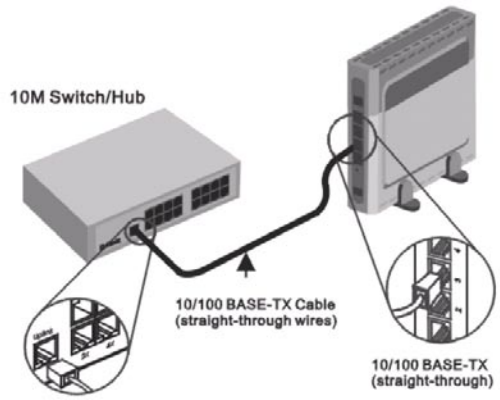
Connect Router to Ethernet

The Router may be connected to a single computer or Ethernet device through the 10/100 BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds between 0~100Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port.
Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch.

The rules governing Ethernet cable lengths apply to the LAN to Router connection. Be sure that the cable connecting the LAN to the Router does not exceed 100 meters.

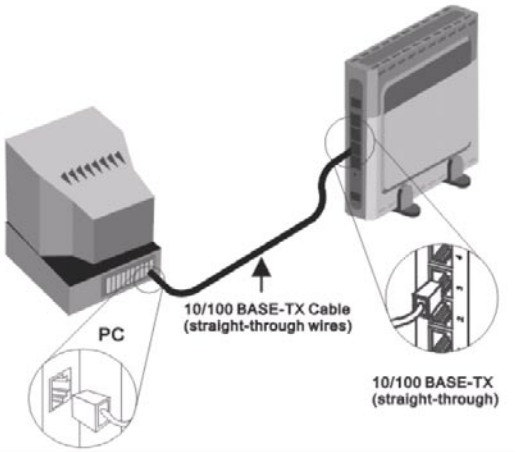
Hub or Switch to Router Connection

Connect the Router to an uplink port (MDI-II) on an Ethernet hub or switch with a straight-through cable as shown in the diagram below:



If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

Computer to Router Connection



You can connect the Router directly to a 10/100BASE-TX Ethernet adapter card (NIC) installed on a PC using the Ethernet cable provided as shown in this diagram.

Basic Router Configuration

The first time you setup the Router it is recommended that you configure the WAN connection using a single computer making sure that both the computer and the Router are not connected to the LAN. Once the WAN connection is functioning properly, you may continue to make changes to Router configuration including IP settings and DHCP setup. This chapter is concerned with using your computer to configure the WAN connection. The following chapter describes the various menus used to configure and monitor the Router including how to change IP settings and DHCP server setup.

Wan Configuration Summary

1. **Connect to the Router** To configure the WAN connection used by the Router it is first necessary to communicate with the Router through its management interface, which is HTML-based and can be accessed using a web browser. To access the management section, your computer must be able to "see" the Router. Your computer can see the Router if it is in the same "neighborhood" or subnet as the Router. This is accomplished by making sure your computer has IP settings that place it in the same subnet as the Router. The easiest way to make sure your computer has the correct IP settings is to configure it to use the DHCP server in the Router. The next section describes how to change the IP configuration for a computer running a Windows operating system to be a DHCP client.
2. **Configure the WAN Connection** Once you are able to access the configuration software you can proceed to change the settings required to establish the ADSL connection and connect to the service provider's network. There are different methods used to establish the connection to the service provider's network and ultimately to the Internet. You should know what Encapsulation and connection type you are required to use for your ADSL service. It is also possible that you must change the PVC settings used for the ADSL connection. Your service provider should provide all the information you need to configure the WAN connection.

Configuring IP Settings on Your Computer

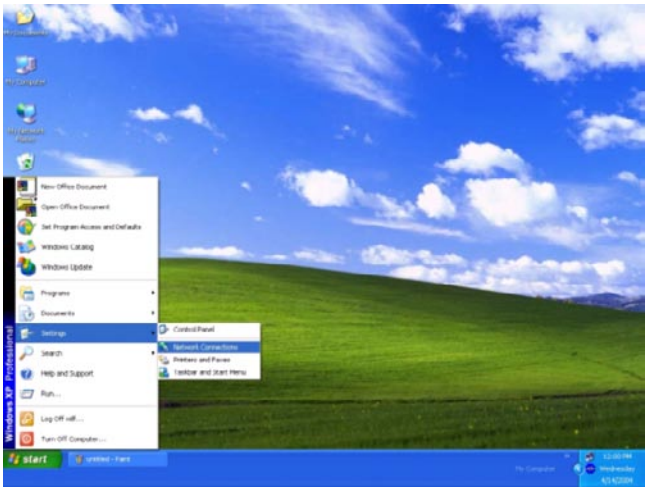
In order to configure your system to receive IP settings from the Router it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. On the following page is an illustrated example of how to configure a Windows XP system to automatically obtain IP settings from the Router. Following this example is a step-by-step description of the procedures used on the other Windows operating systems to first check if the TCP/IP protocol has been installed; if it is not, instructions are provided for installing it. Once the protocol has been installed you can configure the system to receive IP settings from the Router.
For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP address from the Router, that is,

If you are using this Router to provide Internet access for more than one computer, you can use these instructions later to change the IP settings for the other computers. However, you cannot use the same IP address since every computer must have its own IP address that is unique on the local network.

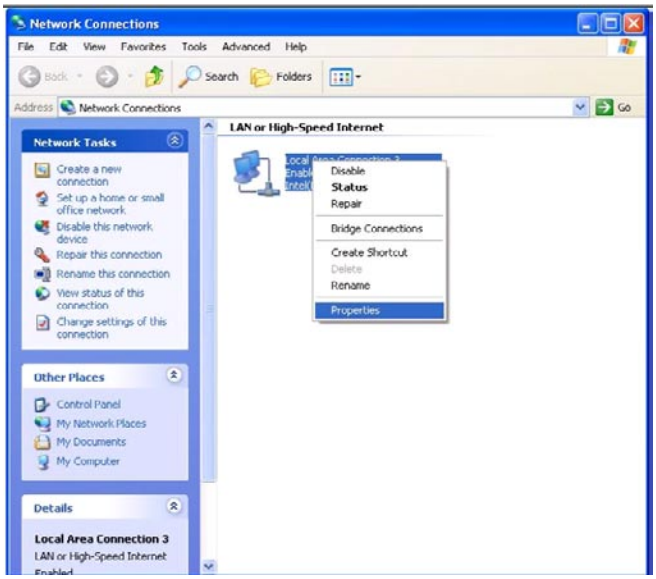
Configure Windows XP for DHCP

Use the following steps to configure a computer running Windows XP to be a DHCP client.

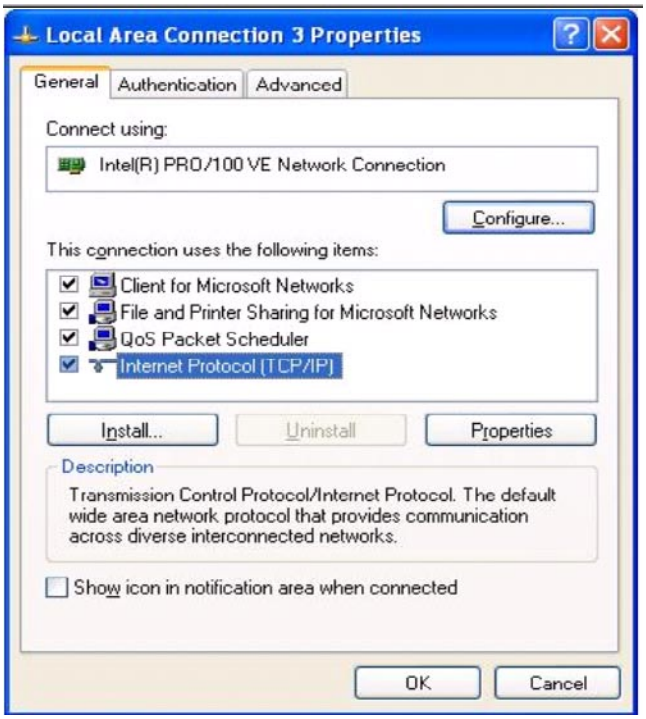
From the **Start** menu on your desktop, go to **Settings**, then click on **Network Connections.** If the network setting is not displayed, go to Start>Settings>Control Panel>Network Connections.



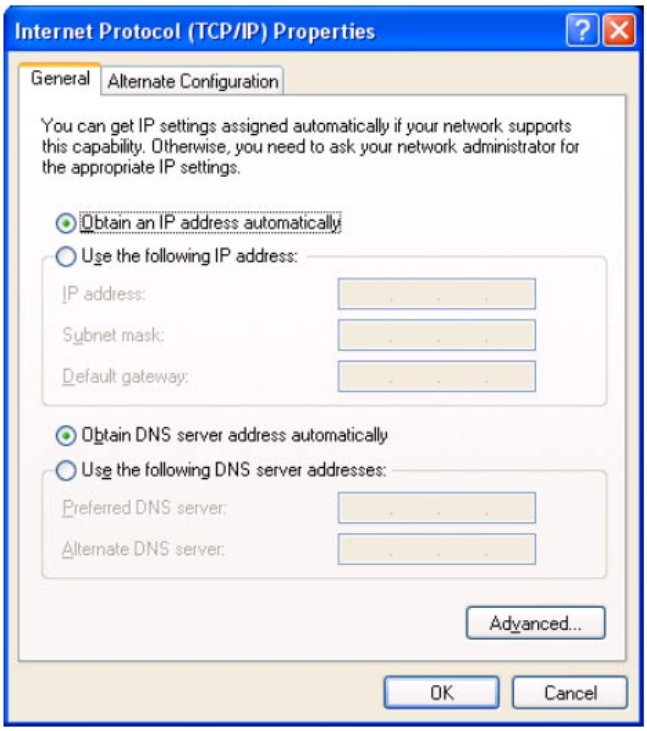
In the **Network Connections** window, right-click on **LAN** (Local Area Connection), then click **Properties**.



In the **General** tab of the **Local Area Connection Properties** menu, highlight **Internet Protocol (TCP/IP)** under "This connection uses the following items:" by clicking on it once. Click on the **Properties** button.



Select "Obtain an IP address automatically" by clicking once in the circle. Click the **OK** button.



Your computer is now ready to use the Router's DHCP server.

Windows 2000

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
4. The **Local Area Connection Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled, skip ahead to *Configure Windows 2000 for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Install**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
8. You may be prompted to install files from your Windows 2000 installation CD or other media. Follow the instructions to install the files.
9. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows 2000 for DHCP

1. In the Control Panel, double-click the **Network and Dial-up Connections** icon.
2. In **Network and Dial-up Connections** window, right-click the **Local Area Connection** icon, and then select **Properties**.
3. In the **Local Area Connection Properties** dialog box, select **Internet Protocol (TCP/IP)**, and then click **Properties**.
4. In the **Internet Protocol (TCP/IP) Properties** dialog box, click the button labeled **Obtain an IP address automatically**.
5. Double-click **OK** to confirm and save your changes, and then close the Control Panel.

Windows ME

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Star**t button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.
3. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
4. The **Network Properties** dialog box displays with a list of currently installed network components. If the list includes Internet Protocol (TCP/IP), then the protocol has already been enabled. Skip ahead to *Configure Windows ME for DHCP*.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click **Add**.
6. In the **Select Network Component Type** dialog box, select **Protocol**, and then click **Add**.
7. Select **Microsoft** in the Manufacturers box.
8. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click **OK**.
9. You may be prompted to install files from your Windows Me installation CD or other media. Follow the instructions to install the files.
10. If prompted, click **OK** to restart your computer with the new settings.

Configure Windows ME for DHCP

1. In the **Control Panel**, double-click the **Network and Dial-up Connections** icon.
2. In the **Network and Dial-up Connections** window, right-click the **Network** icon, and then select **Properties**.
3. In the **Network Properties** dialog box, select **TCP/IP**, and then click **Properties**.
4. In the **TCP/IP Settings** dialog box, click the **Obtain and IP address automatically** option.
5. Double-click **OK** twice to confirm and save your changes, and then close the Control Panel.

Your computer is now ready to use the Router's DHCP server.

Windows 98

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**. Double-click the **Network** icon.
2. The **Network** dialog box displays with a list of currently installed network components. If the list includes TCP/IP, and then the protocol has already been enabled, skip to *Configure IP Information Windows 95, 98*.
3. If TCP/IP does not display as an installed component, click **Add**. The **Select Network Component Type** dialog box displays.
4. Select **Protocol**, and then click **Add**. The **Select Network Protocol** dialog box displays.
5. Click on **Microsoft** in the Manufacturers list box, and then click **TCP/IP** in the Network Protocols list box.
6. Click **OK** to return to the Network dialog box, and then click **OK** again. You may be prompted to install files from your Windows 95/98 installation CD. Follow the instructions to install the files.
7. Click **OK** to restart the PC and complete the TCP/IP installation.

Configure Windows 98 for DHCP

1. Open the **Control Panel** window, and then click the **Network** icon.
2. Select the network component labeled TCP/IP, and then click **Properties**.
3. If you have multiple TCP/IP listings, select the listing associated with your network card or adapter.
4. In the **TCP/IP Properties** dialog box, click the **IP Address** tab.
5. Click the **Obtain an IP address automatically** option.
6. Double-click **OK** to confirm and save your changes. You will be prompted to restart Windows.
7. Click **Yes**.

When it has restarted, your computer is ready to use the Router's DHCP server.

Windows NT 4.0 Workstations

First, check for the IP protocol and, if necessary, install it:

1. In the **Windows NT** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. In the **Control Panel** window, double-click the **Network** icon.
3. In the **Network** dialog box, click the **Protocols** tab.
4. The **Protocols** tab displays a list of currently installed network protocols. If the list includes TCP/IP, then the protocol has already been enabled. Skip to "Configure IP Information"
5. If TCP/IP does not display as an installed component, click **Add**.
6. In the **Select Network Protocol** dialog box, select **TCP/IP**, and then click **OK**. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
7. After all files are installed, a window displays to inform you that a TCP/IP service called DHCP can be set up to dynamically assign IP information.
8. Click **Yes** to continue, and then click **OK** if prompted to restart your computer.

Configure Windows NT 4.0 for DHCP

1. Open the **Control Panel** window, and then double-click the **Network** icon.
2. In the **Network** dialog box, click the **Protocols** tab.
3. In the **Protocols** tab, select **TCP/IP**, and then click **Properties**.
4. In the **Microsoft TCP/IP Properties** dialog box, click the **Obtain an IP address automatically** option.
5. Click **OK** twice to confirm and save your changes, and then close the Control Panel.

Access the Configuration Manager

Now that your computer's IP settings allow it to communicate with the Router, you can access the configuration software.

Be sure that the web browser on your computer is not configured to use a proxy server in the Internet settings. In Windows Internet Explorer, you can check if a proxy server is enabled using the following procedure:

1. *In Windows, click on the **Start** button, go to **Settings** and choose **Control Panel**.*
2. *In the **Control Panel** window, double-click on the **Internet Options** icon.*
3. *Click the **Connections** tab and click on the **LAN Settings** button.*
4. *Verify that the "Use proxy server" option is NOT checked. If it is checked, click in the checked box to deselect the option and click OK.*

Alternatively, you can access this **Internet Options** menu using the **Tools**

Login to Home Page

To use the web-based management software, launch a suitable web browser and direct it to the IP address of the Router. Type in **http://** followed by the default IP address, **192.168.1.1** in the address bar of the browser. The URL in the address bar should read: **http://192.168.1.1**.

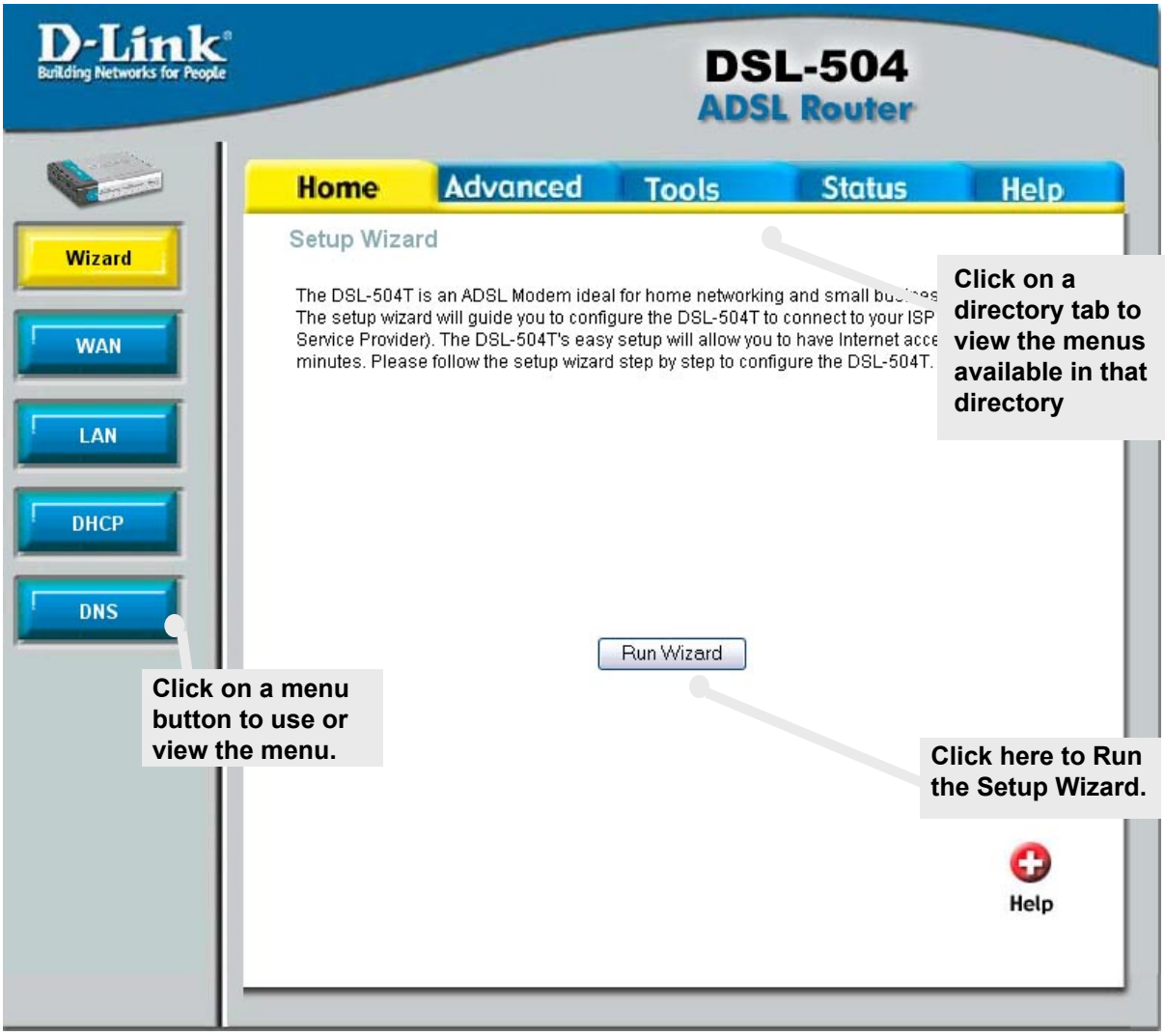
A dialog box prompts for the User Name and Password. Type in the default User Name **admin** and default Password **admin** and click the **OK** button to access the web-based manager.

You should change the web-based manager access user name and password once you have verified that a connection can be established. The user name and password allows any computer within the same subnet as the Router to access the web-based manger.

Do not confuse the user name and password used to access the web-based manager with the ADSL account user name and password needed for PPP connections to access the Internet.

Configure the Router

When you successfully connect to the Web manager, the **Home** directory tab will display the **Setup Wizard** menu. You can launch the Setup Wizard from this page or use the menu buttons located in the left panel of the web page to view other menus used for basic configuration. You may use the Setup Wizard if your Internet connection is a Dynamic IP, Static IP, PPPoE/PPPoA, and Bridge connection.



Web Manager – First Time Log On

All configuration and management of the Router is done using the web-based management interface pictured in the above example. The various menus are accessed by clicking on one of the directory tabs, Home, Advanced, Tools, Status and Help. Each tab displays menu buttons located in the left hand panel of the web interface. The table below lists the menus for each directory in the web manager.

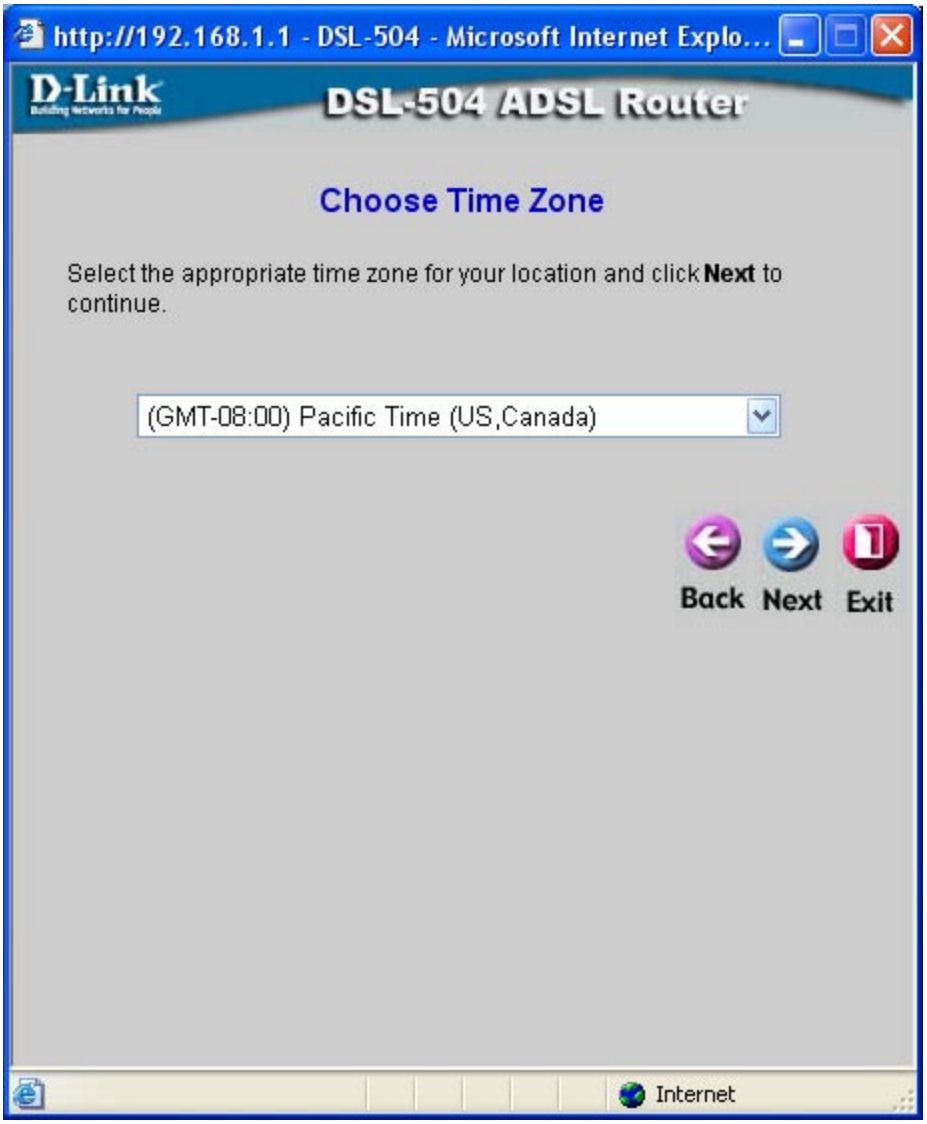
Directory	Configuration and Read-only Menus
Home	Click the Home tab to access the Setup Wizard, LAN setup, WAN Configuration, LAN IP Configuration, DHCP for the LAN Setup and DNS Configuration menus.
Advanced	Click the Advanced tab to access the Virtual Server, Filters, Routing, DMZ, Firewall, RIP, PPP, ADSL, ATM VCC menus.
Tools	Click the Tools tab to access the Administrator Settings (used to set the system user name and password), System Time Configuration, System Settings (load and save configuration files), Firmware Upgrade, Misc Settings (save & reboot) and Diagnostic Test menus.
Status	Click the Status tab to view the Device Information, Event Log, Traffic Statistics and ADSL Status information windows.
Help	The Help menu presents links to pages that explain various functions and services provided by the Router.

Using the Setup Wizard

To use the Setup Wizard, click the **Run Wizard** button in the first browser window and follow the instructions in the pop-up window that appears.

Set a password that is required to make changes to the configuration settings of the Router in the Advanced Configurations menus. Type in a password and verify it by typing a second time. Click **Next** to continue.

The default User Name **admin** used for Router management cannot be changed.

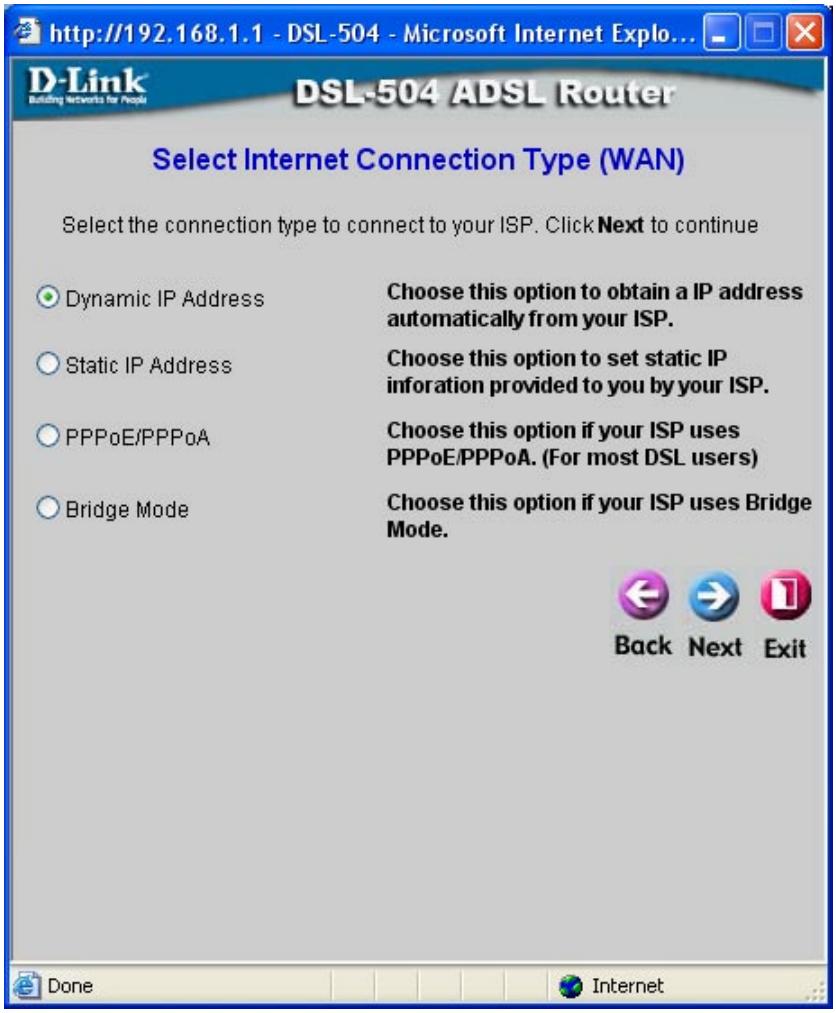


Set the system time of the Router. Choose the time zone you are in from the pull-down menu and click **Next**. If you wish to return to the previous menu during the setup process, click the **Back** button.

Dynamic IP Address

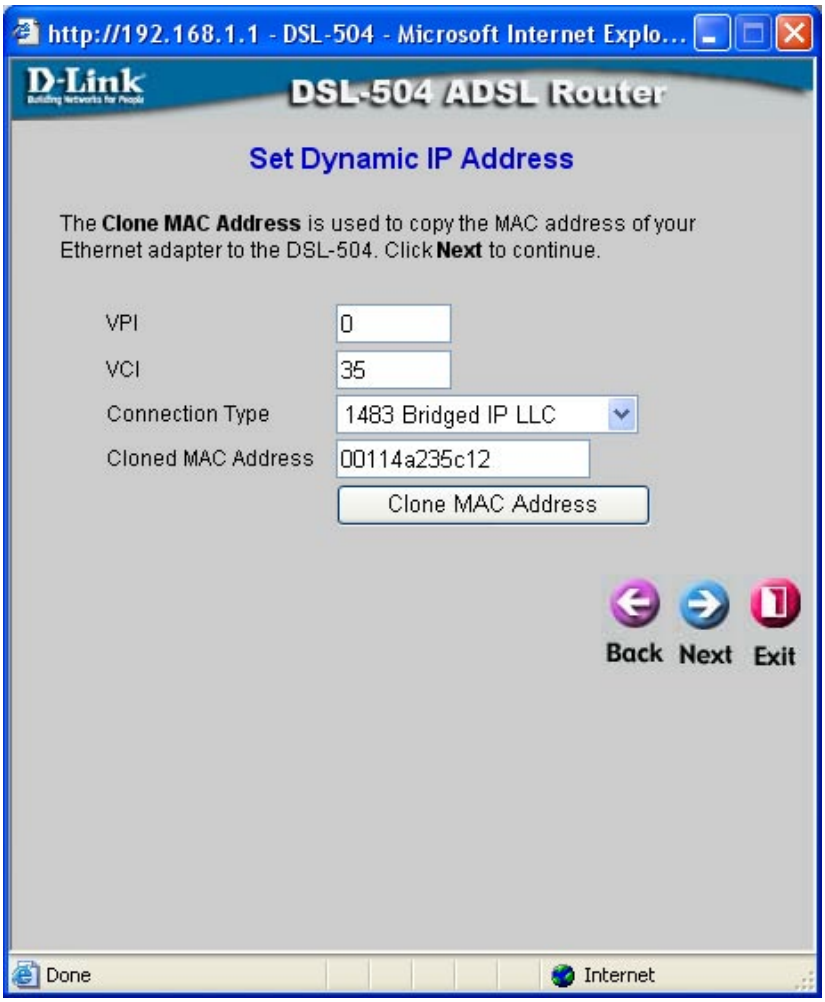
You will need to select the Internet Connection Type. If you are unsure which type of Internet Connection you have, please contact your Internet Service Provider. There are four connection modes and settings vary depending on the connection type.

1. Dynamic IP Address
2. Static IP Address
3. PPPoE/PPPoA
4. Bridge Mode



Connection Type:	Select the **Connection Type** for the Internet.
Next:	Click **Next** to proceed.

Dynamic IP Address (continued)



VPI or VCI: Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.

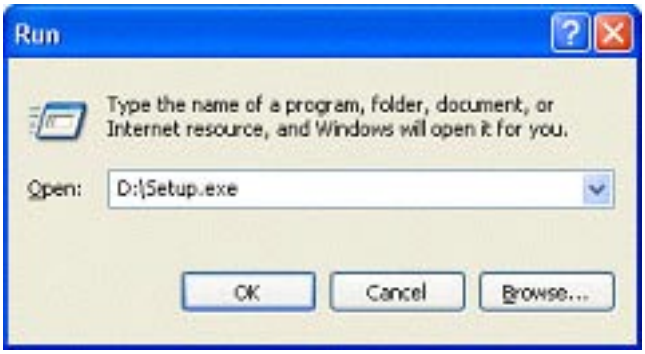
Connection Type: Under **Dynamic IP Address mode**, choose the **Connection Type** from the pull-down menu. For Dynamic IP mode connections the available encapsulation choices are *1483 Bridged IP LLC* and *1483 Bridged IP VCMux*.

Cloned MAC Address: Some ISP's may require you to use the original computer that was originally registered for the Internet service. To obtain the MAC address of the computer, click **Clone MAC Address**. If the MAC address does not appear, please follow the instructions on the next page of this manual (page 37).

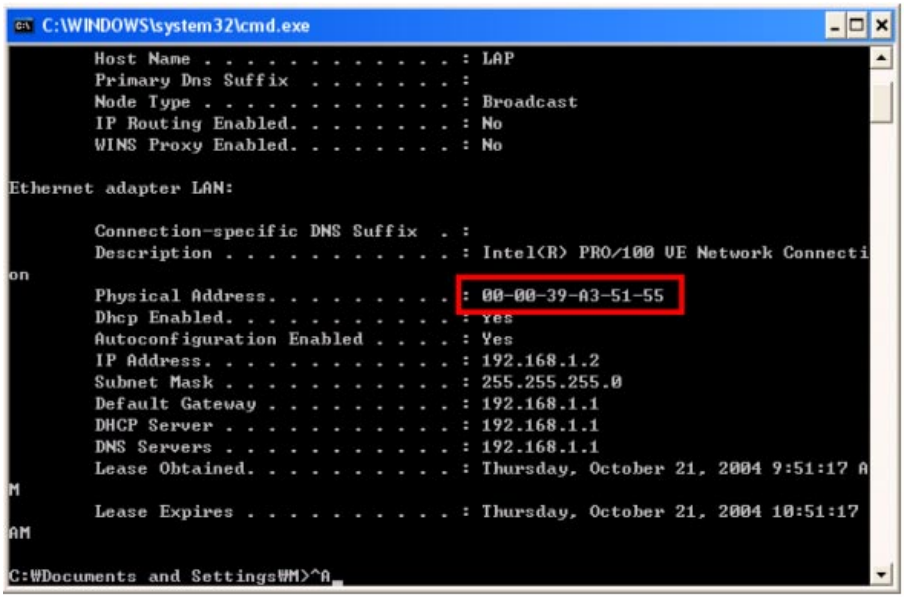
Next: Click **Next** to proceed to the next page.

Finding the MAC address

For Windows XP/2000: **Start**>**Run** >**cmd** >**OK**



In the command prompt, type in **ipconfig/all**. The physical address is the MAC address of the computer

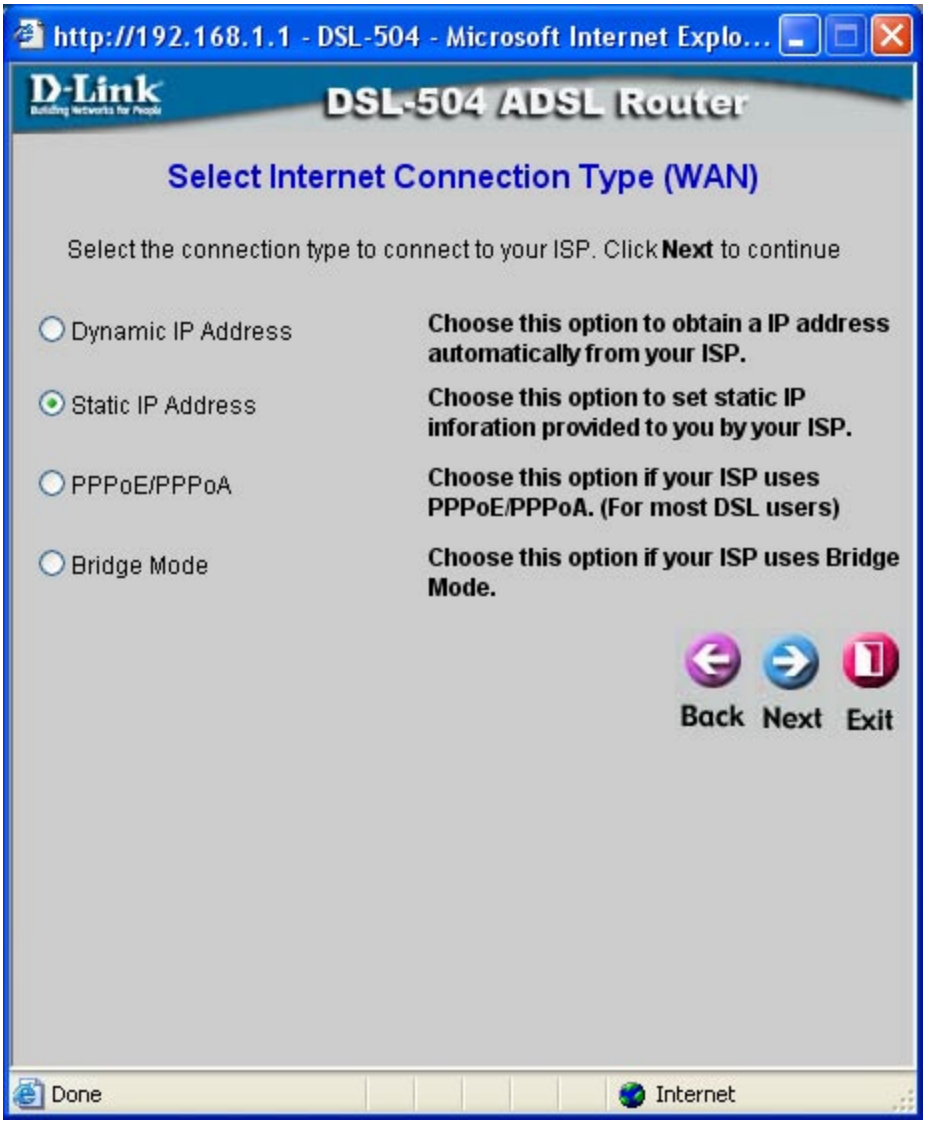


For Windows ME: **Start**>**Run**>**command**>**OK**
In the command prompt, type in **ipconfig/all**. The physical address is the MAC address of the computer.

For Windows 98: **Start**>**Run**>**command**>**OK**
In the command prompt, type in **winipcfg**. The physical address is the MAC address of the computer.

After you have obtained the MAC address, please type the MAC address into the **Cloned MAC Address** box (as shown on page 36 of this manual), and click **Clone MAC Address**. Then click **Next**.

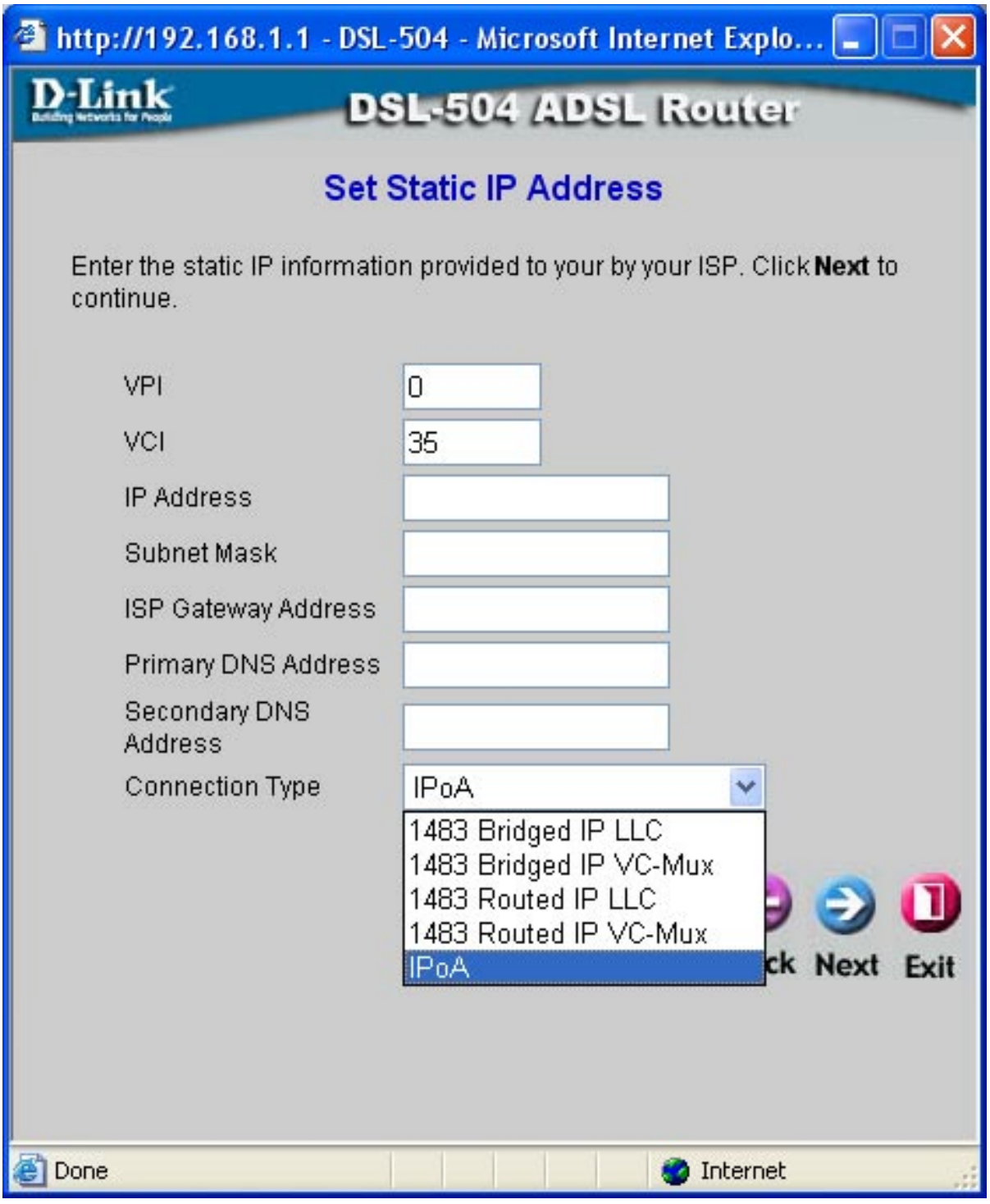
Static IP Address



Connection Type: Select the **Connection Type** for the Internet.

Next: Click **Next** to proceed.

Static IP Address (continued)



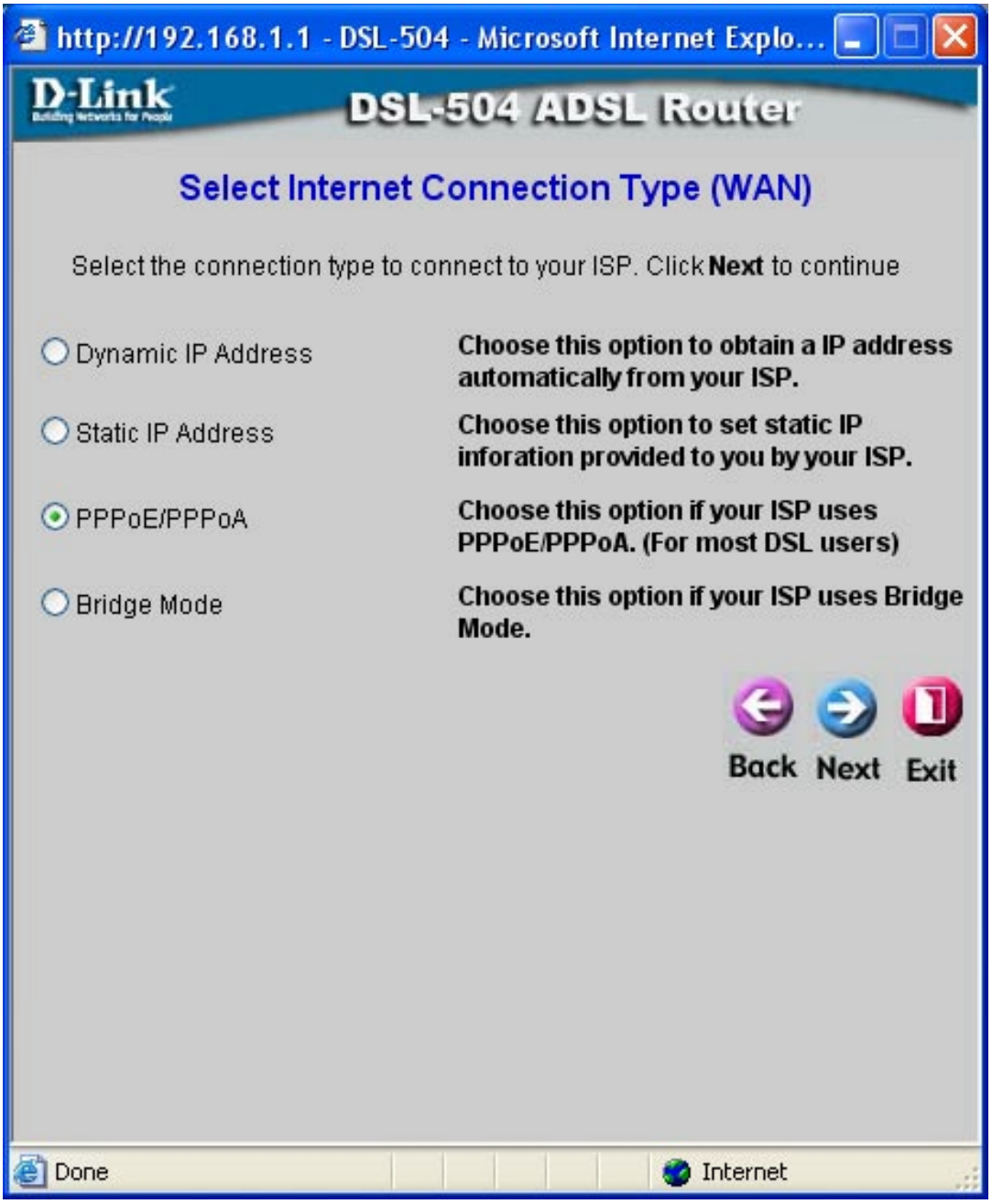
The addresses displayed in this window are only examples, your addresses may be different.

Please see the following page for an explanation of the fields shown on this screen.

Static IP Address (continued)

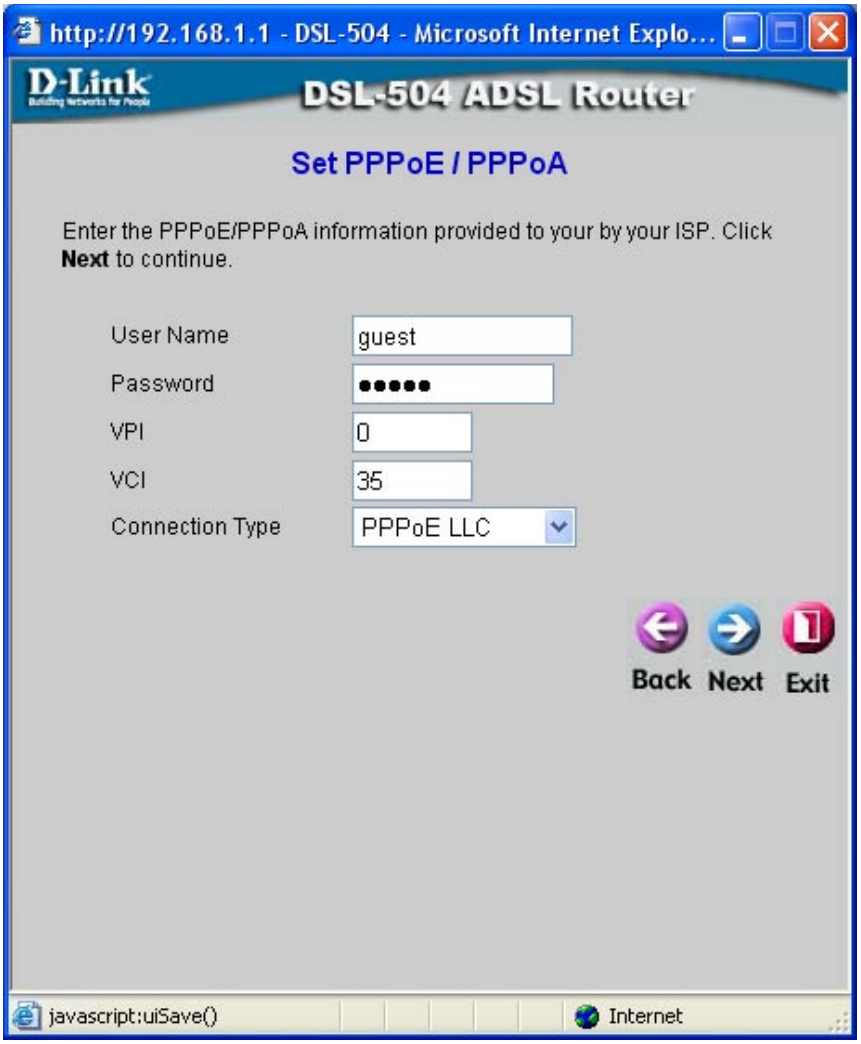
VPI or VCI:	Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.
IP Address:	Change the IP address as instructed by your ISP. Your ISP should have provided these IP settings to you.
Subnet Mask:	Change the subnet mask as instructed by your ISP. Your ISP should have provided these IP settings to you.
ISP Gateway Address:	Change the gateway address as instructed by your ISP. Your ISP should have provided these IP settings to you.
Primary DNS Address:	Change the primary DNS address as instructed by your ISP. Your ISP should have provided this setting to you.
Secondary DNS Address:	Change the secondary DNS address (if available) as instructed by your ISP. Your ISP should have provided this setting to you (if available).
Connection Type:	Select the connection type from the pull-down menu. Your ISP should provide this information to you. The available options are IPOA, 1483 Bridged VC-Mux, 1483 Bridged LLC, 1483 Routed LLC, and 1483 Routed VC-Mux. If you are unsure of the connection type, please contact your service provider for assistance.
Next:	Click Next to proceed to the next page.

PPPoE/PPPoA



Connection Type:	Select the **Connection Type** for the Internet.
Click Next:	Click **Next** to proceed.

PPPoE/PPPoA (continued)



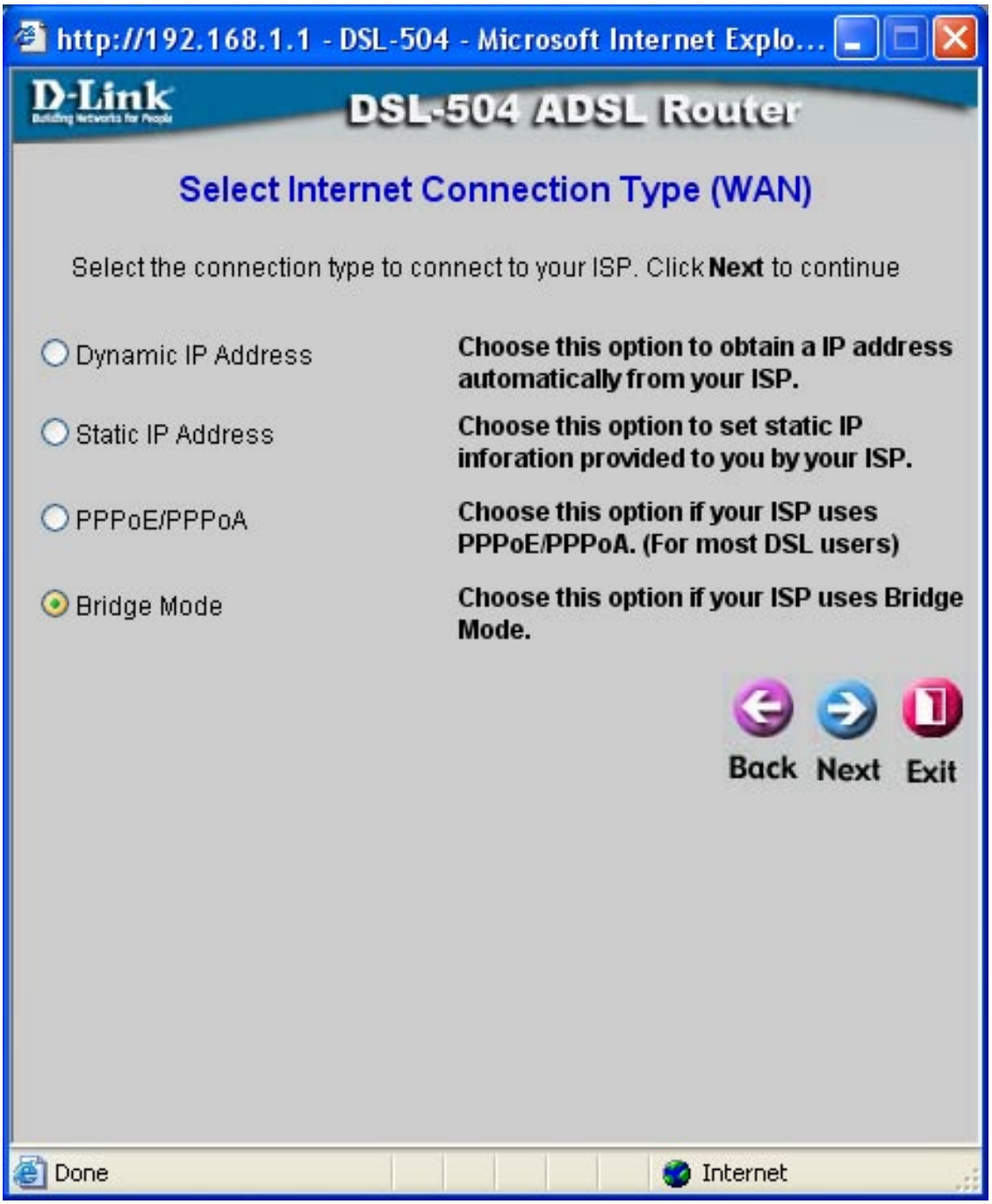
User Name & Password: Type in the account User Name and Password. Your ISP has given this information to you.

VPI or VCI: Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.

Connection Type: Choose the **Connection Type** from the pull-down menu. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoA VC-MUX, PPPoA LLC* and *PPPoE LLC.* If you have not been provided specific information for the Connection Type setting, leave the default

Next: Click **Next** to proceed to next page.

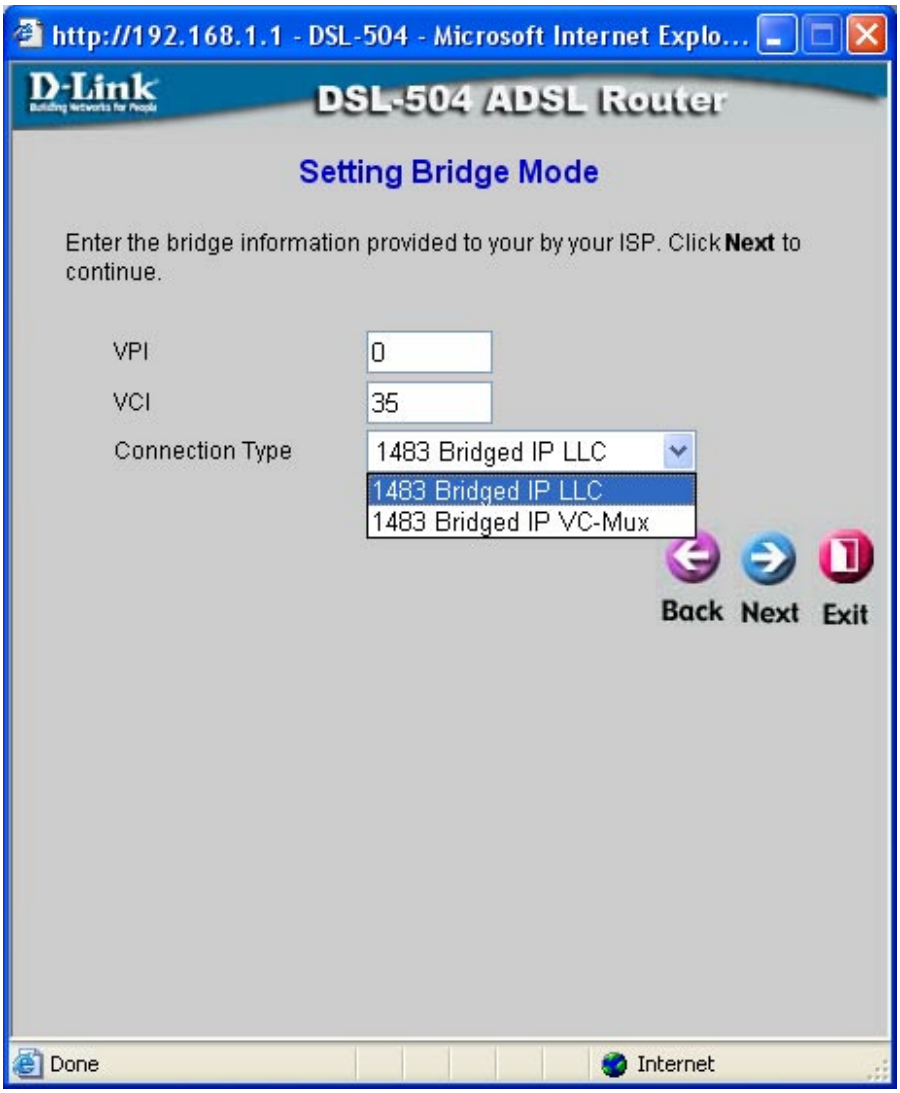
Bridge Mode



Connection Type: Select the **Connection Type** for the Internet.

Click Next: Click **Next** to proceed.

Bridge Mode (continued)

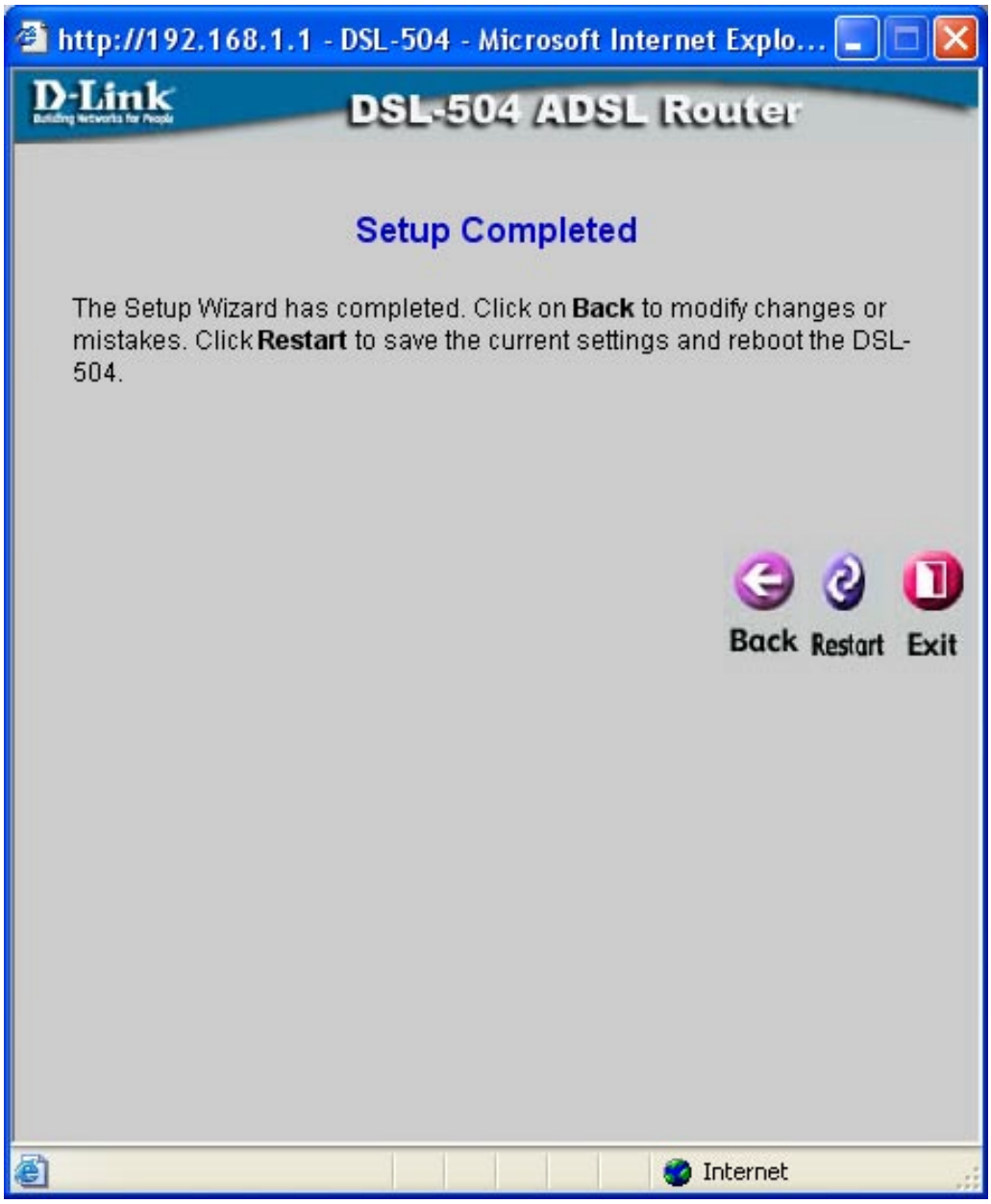


VPI or VCI: Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.

Connection Type: Choose the **Connection Type** from the pull-down menu. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoA VC-MUX, PPPoA LLC* and *PPPoE LLC.* If you have not been provided specific information for the Connection Type setting, leave the default

Next: Click **Next** to proceed to next page.

Completing the Setup Wizard



Restart: Click Restart to save the new configuration settings and restart the DSL-504T.

Back: If you need to change settings from a previous menu, click the Back button.

Exit: When the router has completed rebooting it will take you to the main page of the web management menu. Click Exit to close the window and continue to configure the router as desired.

Do not turn the Router off while it is restarting.

Configuring the WAN Connection

To configure the Router's basic configuration settings without running the Setup Wizard, you can access the menus used to configure WAN, LAN, DHCP and DNS settings directly from the **Home** directory. To access the WAN Settings menu, click on the **WAN** link button on the left side of the first window that appears when you successfully access the web manager.

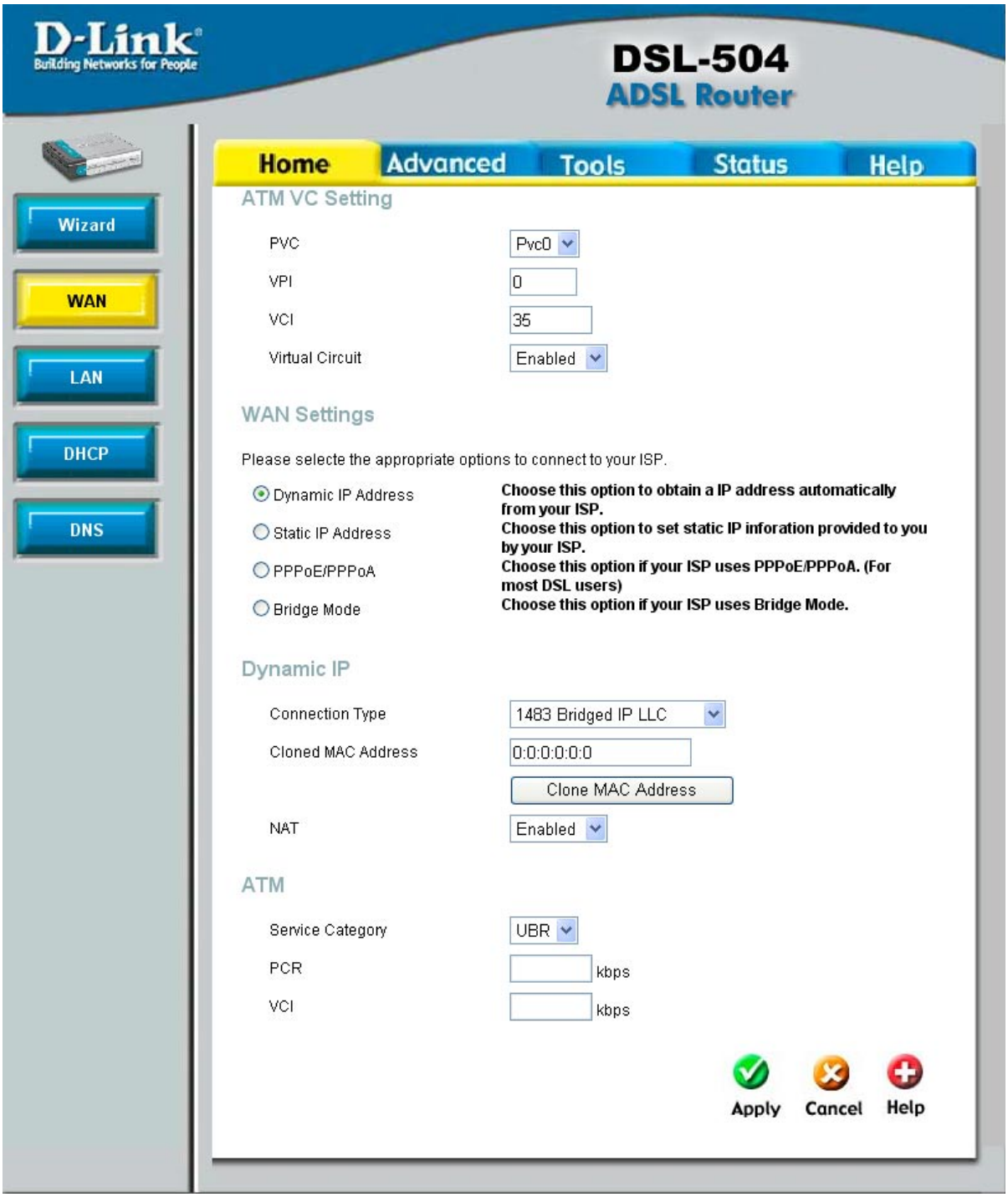
The WAN Settings menu is also used to configure the Router for multiple virtual connections (Multiple PVCs). This will be discussed later in this manual.

WAN Settings Menu

Select the connection type used for your account. The menu will display settings that are appropriate for the connection type you select. Follow the instructions on the following pages according to the type of connection you select in the WAN Settings menu.

Dynamic IP Address for WAN

Follow the instructions below to configure the Router to use a dynamic IP address for the Internet connection. Make sure you have all the necessary information before you configure the WAN connection.



Please see the following page for an explanation of the fields in this window.

Dynamic IP Address for WAN (continued)

ATM VC Settings:

The **ATM VC Settings** at the top of the menu should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account Leave the **PVC** and **Virtual Circuit** settings at their default (*Pcv0* and *Enabled*) values for now. These can be used later if you are configuring multiple virtual circuits for your ADSL service.

WAN Settings:

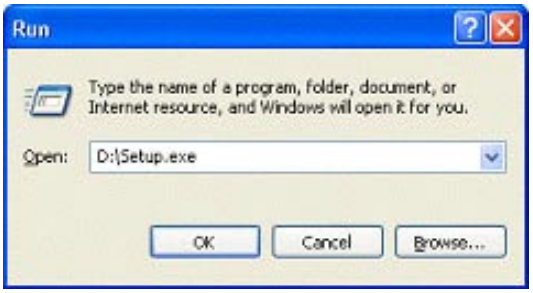
Dynamic IP Address is selected.

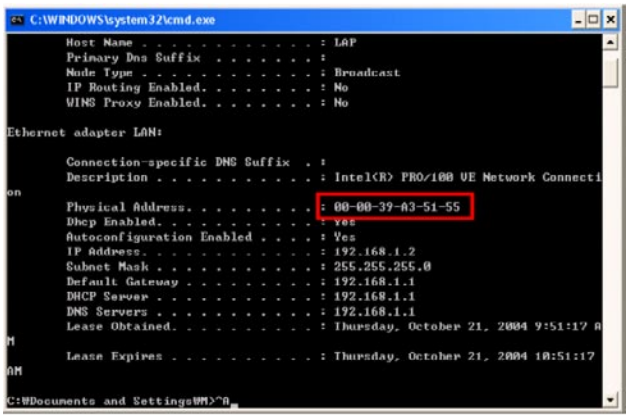
Dynamic IP-Connection Type:

Under **Dynamic IP section**, choose the **Connection Type** from the pull-down menu. For Dynamic IP mode connections the available encapsulation methods are *1483 Bridged IP LLC* and *1483 Bridged IP VCMux*.

Dynamic IP-Cloned MAC Address

Some ISP's may require you to use the original computer that was originally registered for the Internet service. In this case, type in the MAC address of the computer that was used. To obtain the MAC address of the computer, you can do the following:





For Windows XP/2000:

Start>Run>cmd>OK
In the command prompt, type in **ipconfig/all**. The physical address is the MAC address of the computer.

For Windows Me:

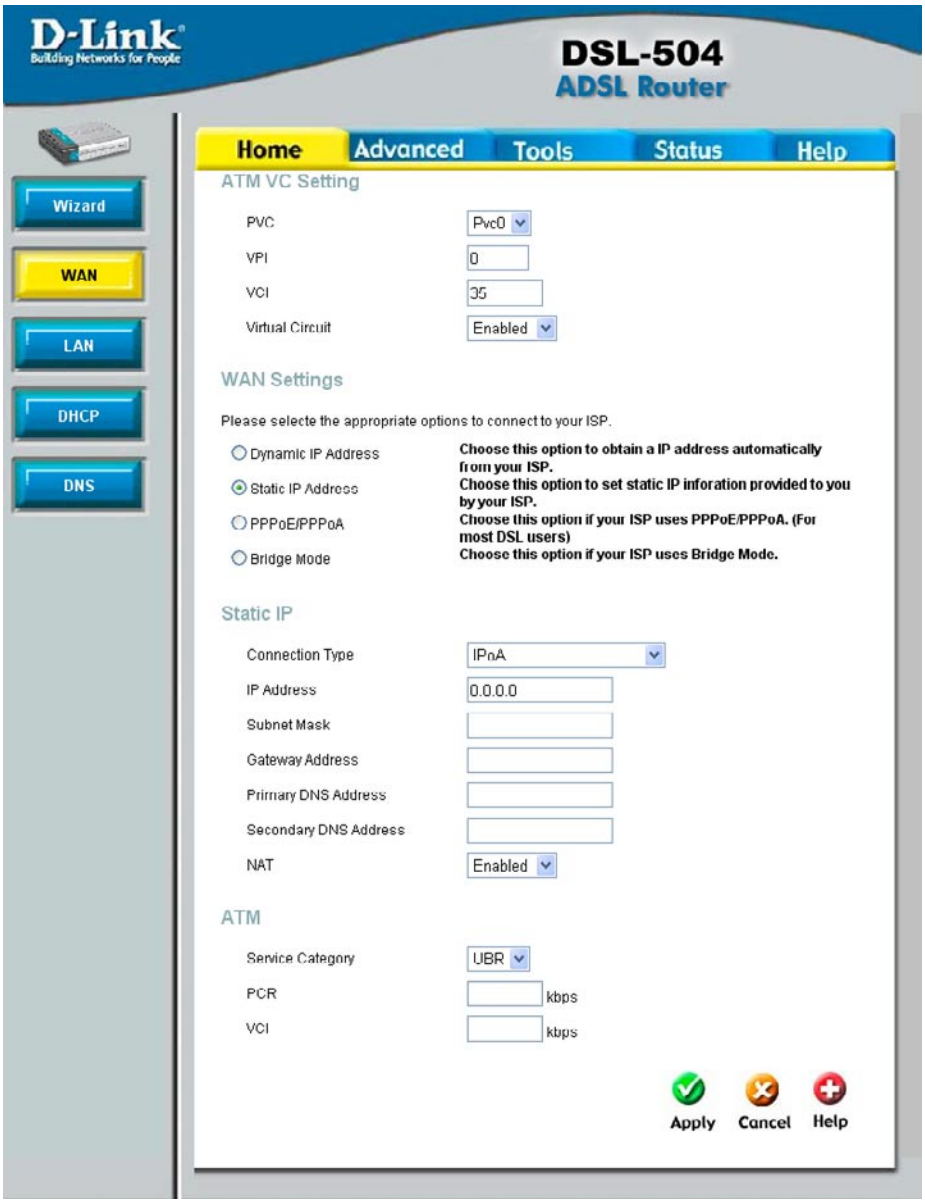
Start >Run >command >OK
In the command prompt, type in **ipconfig/all**. The physical address is the MAC address of the computer.

ATM:

If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **VCI** in Kbps.

Static IP Address for WAN

When the router is configured to use static IP address assignment for the WAN connection, you must manually assign a global IP address, subnet mask and gateway IP address used for the WAN connection. Most users will also configure DNS server IP settings in the DNS settings configuration menu (see below). Please see the following page for an explanation of the fields on this page.



ATM VC Setting-PVC: Do not change the **PVC** (*Pvc0*) index for the initial connection.

ATM VC Setting-VPI & VCI: Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.

Static IP Address for WAN (continued)

Virtual Circuit: Set the **Virtual Circuit** setting to *Enabled* in the pull-down menu if it is not already enabled.

WAN Settings: **Static IP Address** is selected.

Connection Type: Select the **Connection Type** from the pull-down menu under the **Static IP** heading. Your ISP should provide this information to you. The available options are *IPOA*, *1483 Bridged VC-Mux, 1483 Bridged LLC,1483 Routed LLC,* and *1483 Routed VC-Mux.* If you have not been provided specific information for the Connection Type setting, leave the default setting.

IP Address: Change the IP address as instructed by your ISP. Your ISP should have provided these IP settings to you.

Subnet Mask: Change the subnet mask as instructed by your ISP. Your ISP should have provided these IP settings to you.

Gateway Address: Change the gateway address as instructed by your ISP. Your ISP should have provided these IP settings to you.

Primary DNS Address: Change the primary DNS address as instructed by your ISP. Your ISP should have provided this setting to you.

Secondary DNS Address: Change the secondary DNS address (if available) as instructed by your ISP. Your ISP should have provided this setting to you (if available).

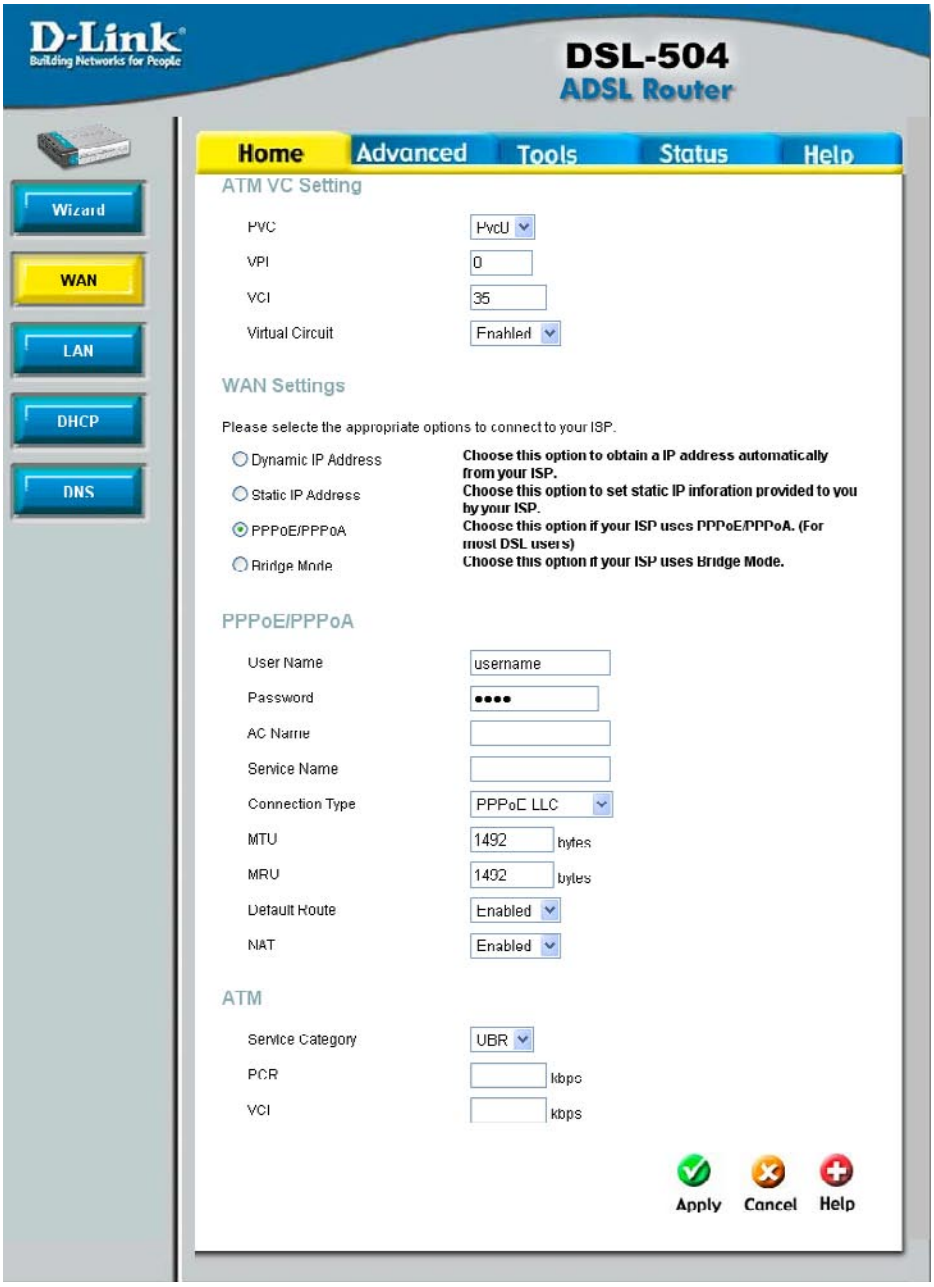
NAT: Set **NAT** to *Enabled* unless you have been told that NAT must be *Disabled* for your account.

ATM: If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the Service Category and type in the values for **PCR** and **VCI** in Kbps.

Apply: Click **Apply** when you have completed the configuration.

*The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** menu button. In the Misc Settings menu, click the **Reboot** button under **Force the DSL-504T to system restart**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection*

PPPoE and PPPoA Connection for WAN



Follow the instructions below and on the next page to configure the Router to use a PPPoE or PPPoA for the Internet connection. Make sure you have all the necessary information before you configure the WAN connection.

ATM VC Setting: The **ATM VC Settings** at the top of the menu should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** settings at their default (*Pcv0* and *Enabled*) values for now. These can be used later if you are configuring multiple virtual circuits for your ADSL service.

PPPoE and PPPoA Connection for WAN (continued)

WAN Settings: Click to select the **PPPoE/PPPoA** radio button in the **WAN Settings** options list. This is selected by default if you are configuring the Router for the first time. If it is not selected, click the **PPPoE/PPPoA** radio button located under the **WAN Settings** heading

PPPoE/PPPoA: User Name & Password Under the **PPPoE/PPPoA** heading, type the **User Name** and **Password** used for your ADSL account. A typical User Name will be in the form user@isp.com.au, the Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP.

AC Name: Check with your ISP.

Service Name: Check with your ISP.

PPPoE/PPPoA: Connection Type Choose the **Connection Type** from the pull-down menu located under the User Name and Password entry fields. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoA VC-MUX, PPPoA LLC* and *PPPoE LLC.* If you have not been provided specific information for the Connection Type setting, leave the default setting.

PPPoE/PPPoA: MTU/MRU Leave the **MTU/MRU** value at the default setting (default = 1492) unless you have been instructed to change this.

PPPoE/PPPoA: Default Route If you are instructed to use enable **Default Route**, this setting specifies that the Router be used to define the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer.

PPPoE/PPPoA: NAT Set **NAT** to *Enabled* unless you have been told that NAT must be *Disabled* for your account.

ATM: If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **VCI** in Kbps.

Apply: Click **Apply** when you have completed the configuration.

*The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** menu button. In the Misc Settings menu, click the **Reboot** button under **Force the DSL-504T to system restart**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection*

Bridged Connection for WAN

For Bridged connections it will be necessary for most users to install additional software on any computer that will connect to the Router for Internet access. The additional software is used for the purpose of identifying and verifying your account, and then granting Internet access to the computer requesting the connection. The connection software requires the user to enter the User Name and Password for the ISP account. This information is stored on the computer, not in the Router.

Follow the instructions on the next page to configure a Bridged connection for the WAN interface.

Bridged Connection for WAN (continued)

ATM VC Setting PVC: Under the **ATM VC Setting** heading, do not change the **PVC** (*Pvc0*) index for the initial connection.

ATM VC Setting VPI & VCI: Also under the **ATM VC Setting**, you see two numbers, the **VCI** and **VPI** values. Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.

ATM VC Setting Virtual Circuit: Set the **Virtual Circuit** setting to *Enabled* in the pull-down menu if it is not already enabled

WAN Setting: Click to select the **Bridge Mode** radio button in the **WAN Settings** options list. The menu will change to offer a different set of configuration options.

Bridge Mode Connection Type: Under **Bridge Mode**, choose the **Connection Type** from the pull-down menu. For bridge mode connections the available encapsulation methods are *1483 Bridged IP LLC* and *1483 Bridged IP VCMux*.

ATM: If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **VCI** in Kbps.

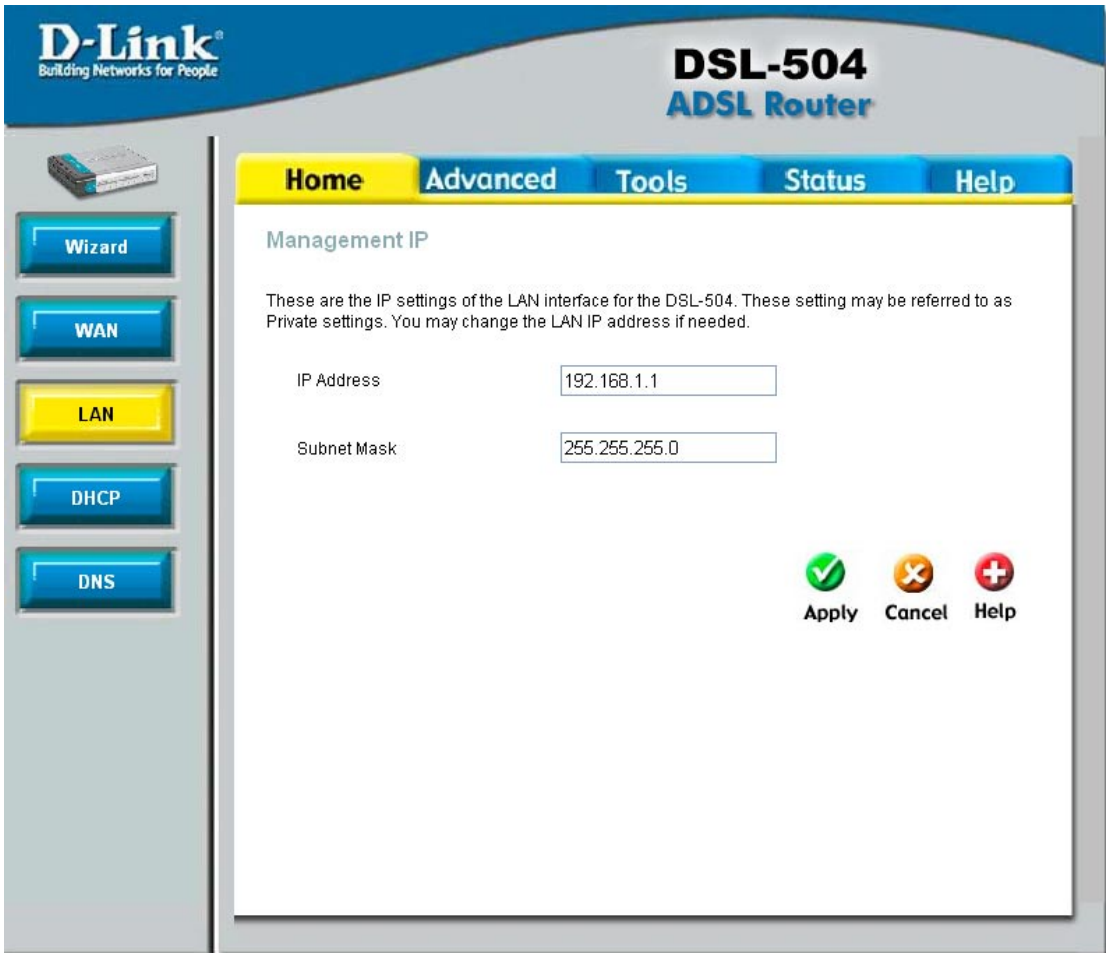
Apply: Click **Apply** when you have completed the configuration.

*The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** menu button. In the Misc Settings menu, click the **Reboot** button under **Force the DSL-504T to system restart**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection*

LAN IP Settings

You can configure the LAN IP address to suit your preference. Many users will find it convenient to use the default settings together with DHCP service to manage the IP settings for their private network. The IP address of the Router is the base address used for DHCP. In order to use the Router for DHCP on your LAN, the IP address pool used for DHCP must be compatible with the IP address of the Router. The IP addresses available in the DHCP IP address pool will change automatically if you change the IP address of the Router. See the next section for information on DHCP setup.

To access the **LAN Settings** menu, click the **LAN** button in the **Home** directory.



To change the **IP Address** or **Subnet Mask**, type in the desired values and click the **Apply** button. Your web browser should automatically be redirected to the new IP address

IP Address:	To change the **IP Address**, type in the desired values.
Subnet Mask:	To change the **Subnet Mask**, type in the desired values.
Apply:	Click **Apply** when you have completed the configuration.

DHCP Server Settings for the LAN

The DHCP server is enabled by default for the router's Ethernet LAN interface. DHCP service will supply IP settings to computers configured to automatically obtain IP settings that are connected to the router though the Ethernet port. When the router is used for DHCP it becomes the default gateway for DHCP client connected to it. Keep in mind that if you change the IP address of the router, you must change the range of IP addresses in the pool used for DHCP on the LAN.

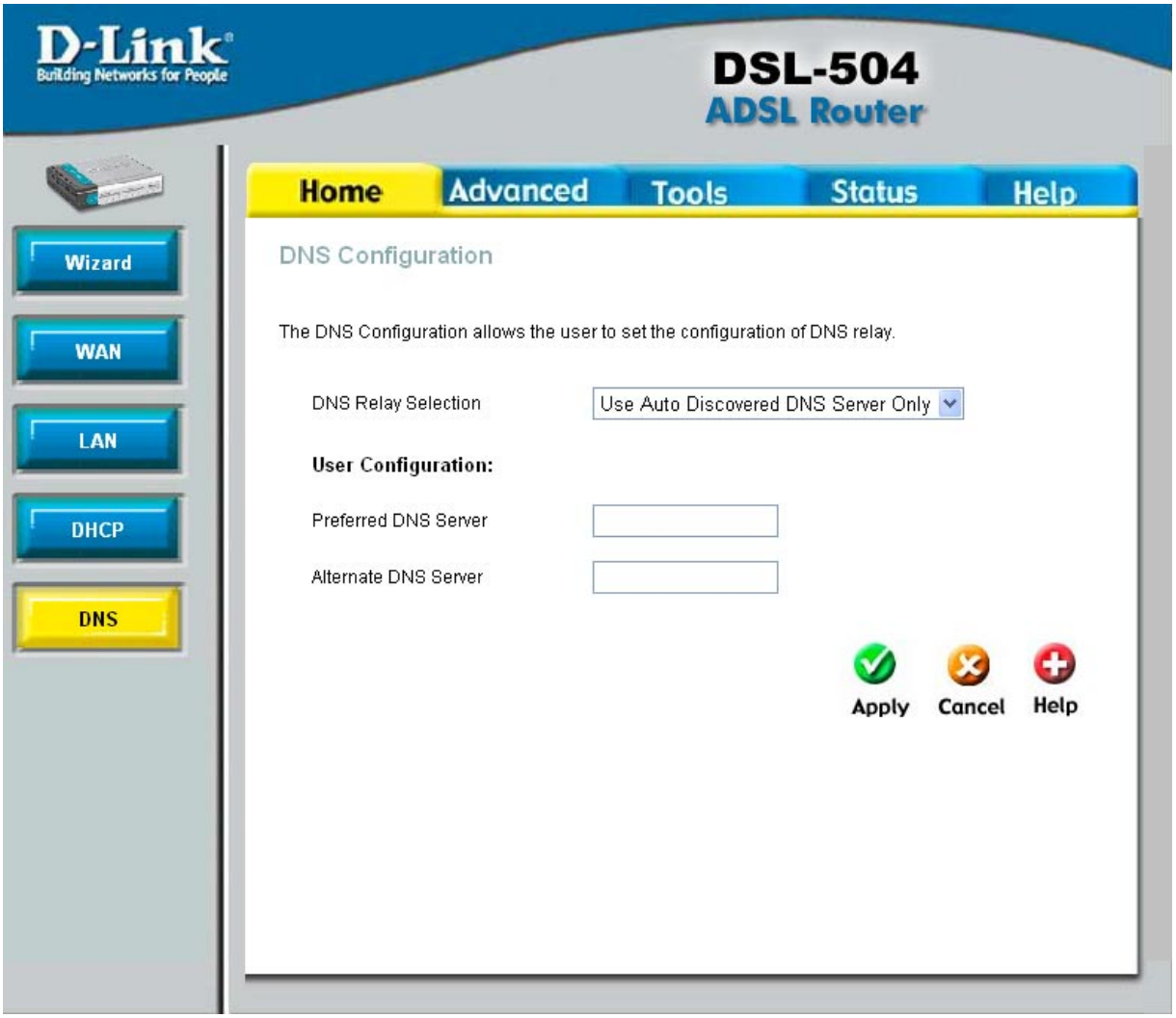
To display the **DHCP Server** menu, click the **DHCP** button in the **Home** directory. Active DHCP Clients appear listed in the **DHCP Client List** below the configuration menu. Information about DHCP clients include the IP address, MAC address, host name and lease time.
Please see the following page for an explanation of the fields in this window.

DHCP Server Settings for the LAN (continued)

No DHCP:	Disable DHCP service to manually configure IP settings for workstations. Click **Apply**.
DHCP Server:	Make this selection to use the router as a DHCP server for your LAN.
DHCP Relay:	Make this selection to use the DHCP service provided by your ISP. Type the DHCP Relay IP address in the space provided. Click
Starting IP Address:	The lowest available IP address. The default IP address is 192.168.1.2. If you change the address of the router, this address will automatically change to be the next consecutive address.
Ending IP Address:	The highest IP address number in the pool.
Lease Time:	This is the amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

*The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Misc** menu button. In the Misc Settings menu, click the **Reboot** button under **Force the DSL-504T to system restart**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection*

DNS Server Settings



The router can be configured to relay DNS from your ISP or another available service to workstations on your LAN. When using DNS relay, the router will accept DNS requests from hosts on the LAN and forward them to the ISP (or alternative) DNS servers. DNS relay can use auto discovery or the DNS IP address can be manually entered by the user. Alternatively, you may also disable the DNS relay and configure hosts on your LAN to use DNS servers directly. Most users who are using the Router for DHCP service on the LAN and are using DNS servers on the ISP's network leave DNS relay enabled (either auto discovery of user configured), unless specified by your ISP.

Please see the following page for an explanation of the fields in this window.

DNS Server Settings (continued)

DNS Relay Selection:	In the pulldown menu, select either **Use Auto Discovery**, **Use User Configured** or **Disable DNS relay**. If you have not been given specific DNS server IP addresses or if the router is not pre-configured with DNS server information, select the Auto Discover option for DNS relay. Auto discovery DNS instructs the router to automatically obtain the DNS IP address from the ISP through DHCP. If your WAN connection uses a static IP address, auto discovery for DNS cannot be used. If you choose to disable DNS relay, it will be necessary to configure DNS settings for hosts on the LAN since they will not be depending on the router to forward the DNS requests.
Preferred DNS Server:	If you have DNS IP addresses provided by your ISP, enter these IP addresses here.
Alternate DNS Server:	If you have DNS IP addresses provided by your ISP, enter these IP addresses here.
Apply:	When you have configured the DNS settings as desired, click the **Apply** button.

Advanced - Virtual Server

Use the Port Forwarding menu to create Virtual Server functions through the Router. A Virtual Server can allow remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DSL-504T will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the Private IP address you specify. Remember that the Private IP Address must be within the range specified for your LAN.

The Virtual Server feature employs UDP/TCP port redirection to direct traffic through the WAN port to specified servers on your private network. Port redirection can also be used to direct potentially hazardous packets to a proxy server outside your firewall. For example, you can configure the Router to direct HTTP packets to a designated HTTP server in the DMZ. You can define a set of instructions for a specific incoming port or for a range of incoming ports. Each instruction set or rule is indexed and can be modified or deleted later as needed.

Virtual server configuration sets can be used together with complimentary features such as Firewall Rules, DMZ devices and IP Filters to improve efficiency and security. Consider how these other functions will effect the virtual server sets you have configured and enabled.

To modify virtual server settings for any previously created virtual server set listed, click on the note pad icon in the right hand column of the **Virtual Servers List** for the set you want to configure. The set will appear highlighted in the list and the parameters that have been configured appear in the settings fields above the list. Adjust the settings as desired and click the **Apply** button to put them into effect.

Advanced - Virtual Server (continued)

To configure a virtual server set, define the following settings in the Virtual Server configuration menu located in the top half of the browser window.

Parameter	Description
Rule Name	Provide a name for the rule. This name will not appear in the list below, however it may be useful if you later need to edit the settings for the rule. Rule names are optional.
Private IP	This is the IP address of the server on your LAN that will provide the service to remote users. The Private IP address is used to direct the service to a specific computer on your private network such as an FTP, Email or public web server. Type in the IP address of the server used for the service being configured here.
Protocol	You can select the transport protocol (TCP or UDP) that the application on the virtual server will use for its connections. Select one of the following options from the pull-down menu to define a *TCP*, *UDP* or *Both*. The choice of this protocol is dependent on the application that is providing the service. If you do not know which protocol to choose, check your application's documentation.
Port Start/Port End	Configure a range of ports for forwarding. Type the lowest numbered port in the range in the Port Start space. Type the highest numbered port in the Port End space. For a single port, just enter the same number in both spaces.Virtual server port redirection must be used with a specified server or computer on

Click the **Apply** button to put the new virtual server configuration set or modification into effect. Any server sets configured in the menu will appear in the Virtual Server List with the new settings. The Router must save the new settings and reboot before the new virtual server configurations are applied.

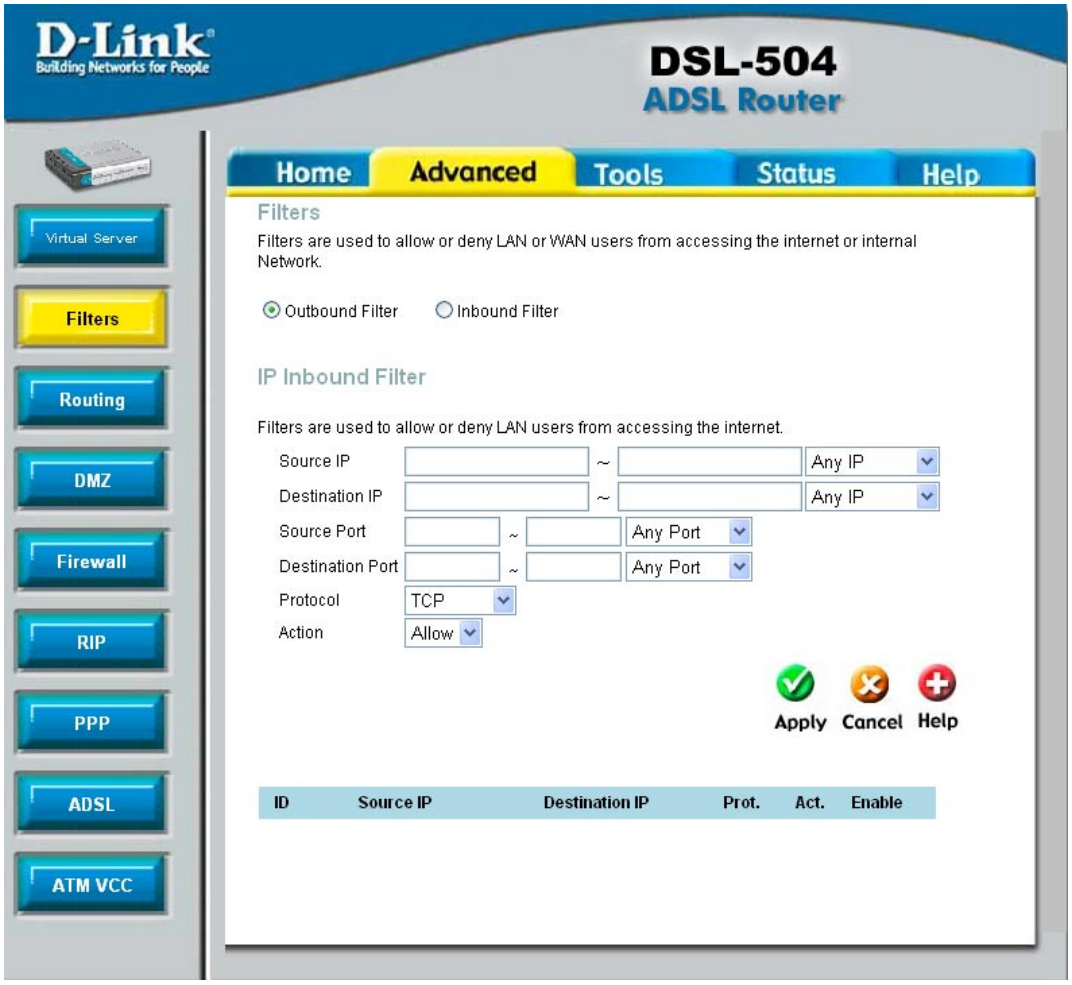
To remove any configuration set from the Virtual Server List, click on the trashcan icon for set you want to delete.

Some applications require multiple TCP or UDP ports to function properly. Applications such as Internet gaming, video conferencing, and Internet telephony are some examples of applications that often require multiple connections. These applications often conflict with NAT, and therefore require special handling. See the discussion of DMZ configuration below.

Advanced - Filters

Filter rules in the Router are put in place to allow or block specified traffic. The Filter Rules however can be used in a single direction to examine and then Allow or Deny traffic for Inbound (WAN to LAN) or Outbound (LAN to WAN) routed data. The rules based on IP address and TCP/UDP port.

Configure the filter rules as desired and click the **Apply** button to create the rule. The newly created rule appears listed in the Outbound Filter List at the bottom of the menu. The table below describes the various parameters that are configured for the filter



To modify any previously created filter rule, click on the note pad icon in the right hand column of the Filter List for the set you want to configure. Adjust the settings as desired and click the **Apply** button to put the new settings into effect.

First determine the direction of the traffic you want the rule to filter. To filter WAN to LAN traffic, select the **Inbound Filter** option. Any new Inbound Filter rules created will appear in the list. Likewise, should you wish to filter LAN to WAN traffic, create an **Outbound Filter** rule.

Advanced - Filters (continued)

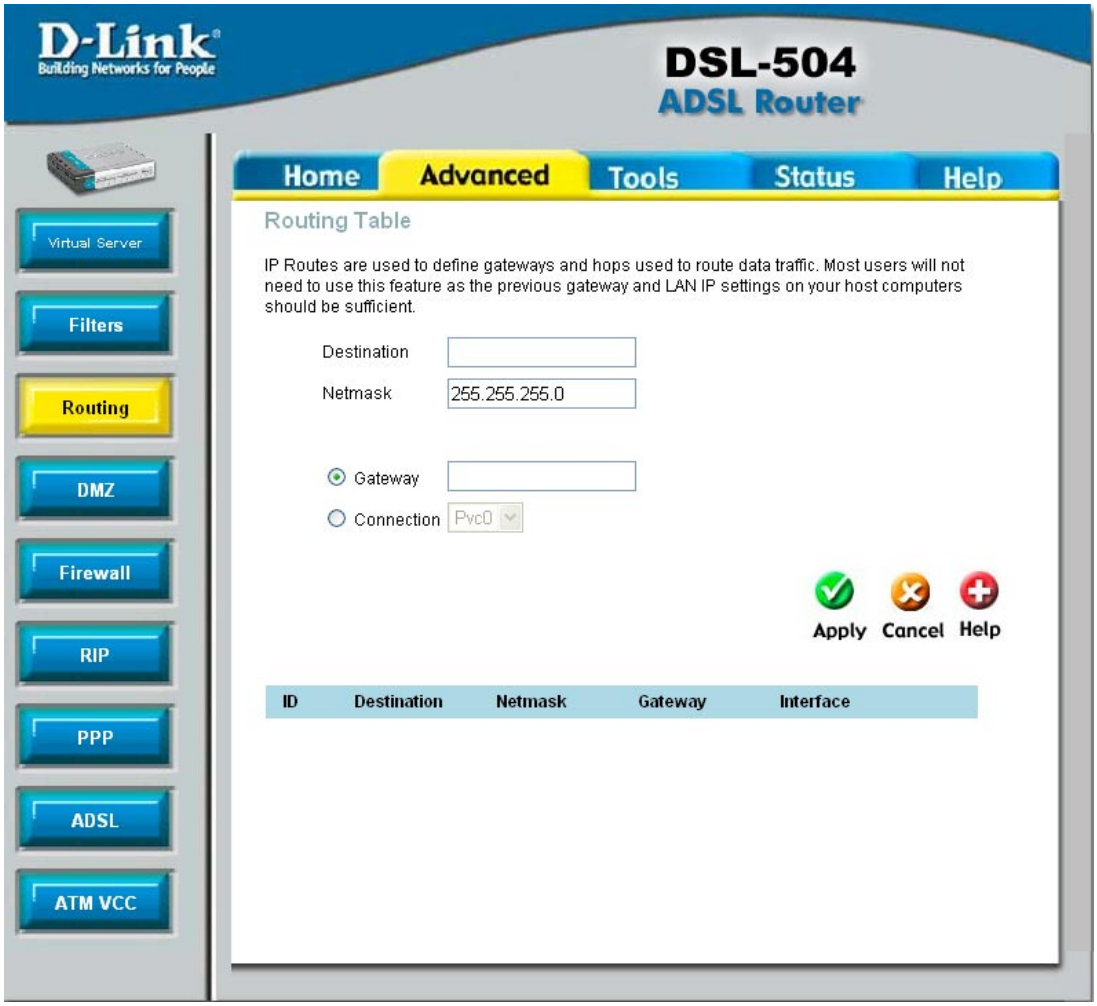
The parameters described below are used to set up filter rules

Parameter	Description
Source IP	For an Outbound Filter, this is the IP address or IP addresses on your LAN for which you are creating the filter rule. For an Inbound Filter, this is the IP address or IP addresses for which you are creating the filter rule. You can opt to indicate a *Mask Range*, a *Single IP*, an *IP Range* or *Any IP* from the pull-down menu. Choosing Any IP will apply the rule to all WAN or all LAN IP addresses depending on which type of rule (Inbound or Outbound) is being configured.
Destination IP	Where the Destination IP address resides also depends on if you are configuring an Inbound or Outbound filter rule. You can opt to indicate a *Mask Range*, a *Single IP*, an *IP Range* or *Any IP* from the pull-down menu.
Source Port	The Source Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define a *Any Port, Single Port*, *Port Range* or *Safe Range* (ports above 1024).
Destination Port	The Destination Port is the TCP/UDP port on either the LAN or WAN depending on if you are configuring an Outbound or Inbound Filter rule. Select one of the following options from the pull-down menu to define a *Any Port, Single Port*, *Port Range* or *Safe Range* (ports above 1024).
Protocol	Select the transport protocol (*TCP*, *UDP* or *All*) that will be used for the filter rule.
Action	Select to *Allow* or *Deny* transport of the data packets according to the criteria defined in the rule. Packets that are allowed are routed to their destination; packets that are denied are

Click the **Apply** button to put the new rule into effect. Any filter rule configured in the menu will appear in the Filters List with the new settings. The Router must save the new settings and reboot before the new rules are applied.

Advanced - Static Routing

Use Static Routing to specify a route used for data traffic within your Ethernet LAN or to route data on the WAN. This is used to specify that all packets destined for a particular network or subnet use a predetermined gateway.



To add a static route to a specific destination IP on the local network, enter a **Destination** IP address, **Netmask**, click the **Gateway** radio button and type in the Gateway's IP address. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation.

To add a static route to a specific destination IP on the WAN, click the Connection radio button and choose a connection from the pull-down menu, then enter a **Destination** IP address and **Netmask**. Click **Apply** to enter the new static route in the table below. The route becomes active immediately upon creation.

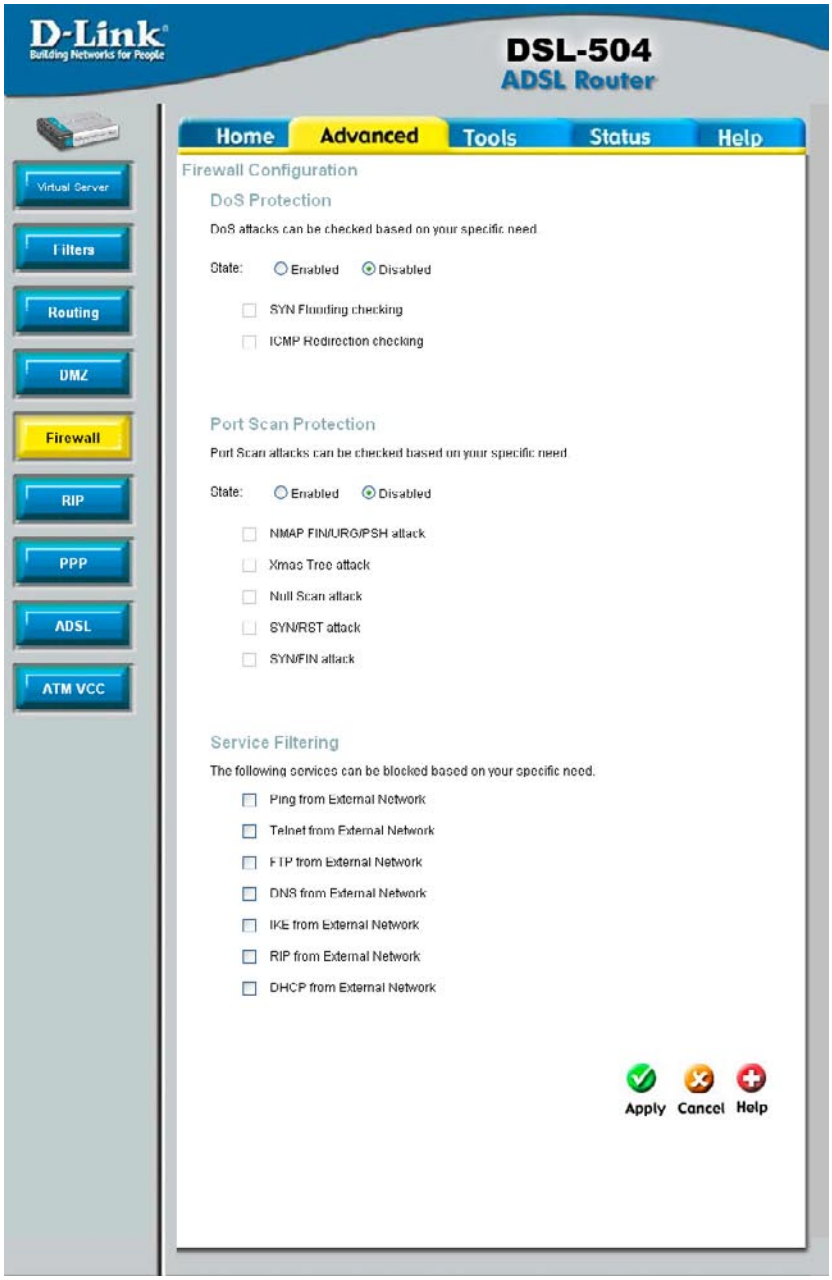
To remove a static route from the table in the bottom half of the window, choose to **Delete** it from the table and click the **Apply** button. Remember to save the configuration changes.

Advanced - DMZ

Since some applications are not compatible with NAT, the Router supports use of a DMZ IP address for a single host on the LAN. This IP address is not protected by NAT and will therefore be visible to agents on the Internet with the right type of software. Keep in mind that any client PC in the DMZ will be exposed to various types of security risks. If you use the DMZ, take measures (such as client-based virus protection) to protect the remaining client PCs on your LAN from possible contamination through the DMZ.

To designate a DMZ IP address, type in the **IP Address** of the server or device on your LAN, select the **Enabled** radio button and click the **Apply** button. To remove DMZ status from the designated IP address, select the Disabled radio button and click Apply. It will be necessary to save the settings and reboot the Router before the DMZ is activated.

Advanced - Firewall



The Firewall Configuration menu allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. There are two general types of protection (DoS and Port Scan) that can be enabled on the Router, as well as filtering for specific packet types sometimes used by hackers.

You can choose to **Enable** or **Disable** protection against a customized basket of attack and scan types. To enable **DoS Protection** or **Port Scan Protection**, select the **Enable** radio button for the protection type and click in the selection boxes for the various types of protection listed under each.

Advanced-Firewall (continued)

When DoS, Port Scan, or Service Filtering Protection is enabled, it will create a firewall policy to protect your network against the following:

Dos Protection
SYN Flood check
ICMP Redirection check

Port Scan Protection
Nmap/FIN attack
URG/PSH attack
Xmas Tree Scan
Null Scan attack
SYN/RST attack

Service Filtering
Ping from WAN
Telnet from WAN
FTP from WAN
DNS from WAN
IKE from WAN
RIP from WAN
DHCP from WAN

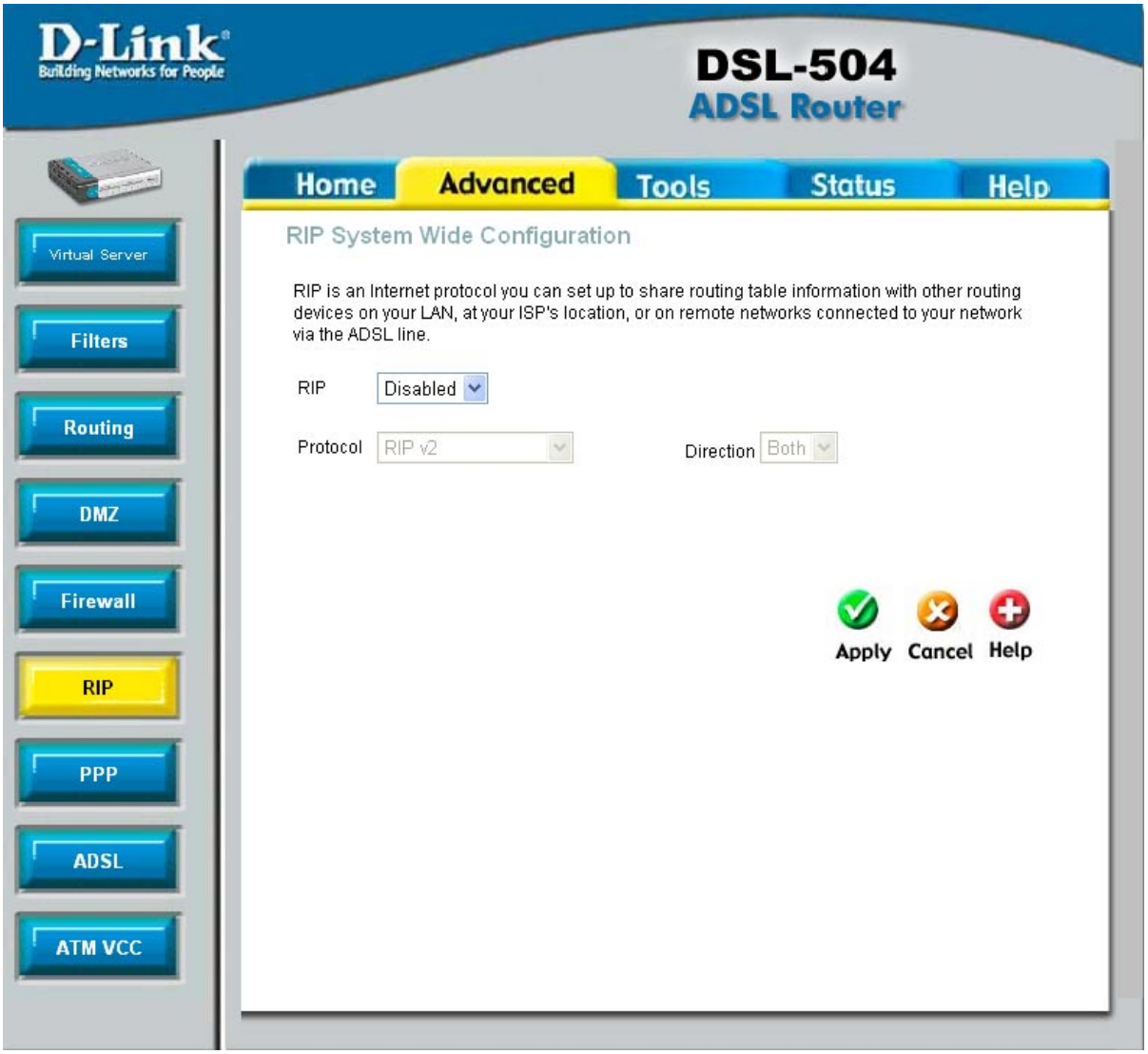
A DoS "denial-of-service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include: attempts to "flood" a network, thereby preventing legitimate network traffic, attempts to disrupt connections between two machines, thereby preventing access to a service, attempts to prevent a particular individual from accessing a service, or, attempts to disrupt service to a specific system or person.

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.
The Service Filtering options allow you to block FTP, Telnet response, Pings, etc, from the external network. Check the category you want to block to enable filtering of that type of packet.

When you have selected the desired Firewall policies, click the **Apply** button to enforce the policies. Remember to save any configuration changes.

Advanced - RIP

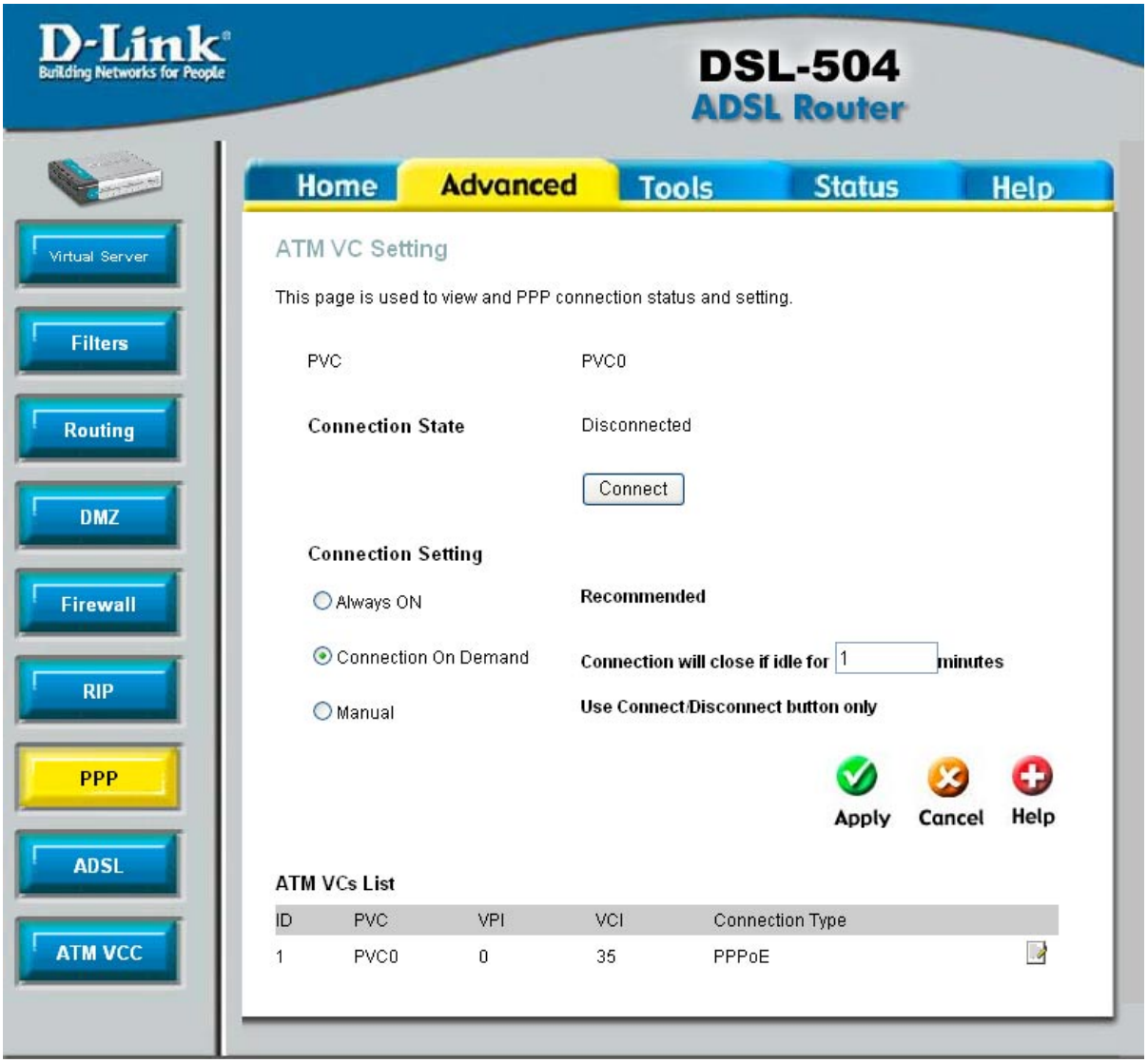
The Router supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices on your local network or remote LAN.



To enable RIP, select *Enabled* from the **RIP** pull-down menu, select the **Protocol** (*RIPv1*, *RIPv2* and *RIPv1 Compatible*) and **Direction** (*In*, *Out*, or *Both*), and click **Apply**. The RIPv1 Compatible option will respond to or send RIP requests compatible with both RIP v1 and RIP v2.

The direction configuration refers to the RIP request. Select In to allow RIP requests from other devices. Select Out to instruct the Router to make RIP requests for routing tables from other devices. Select Both to share routing tables in both directions.

Advanced - PPP



View the status of the PPP connection (Point to Point Protocol) in this window.

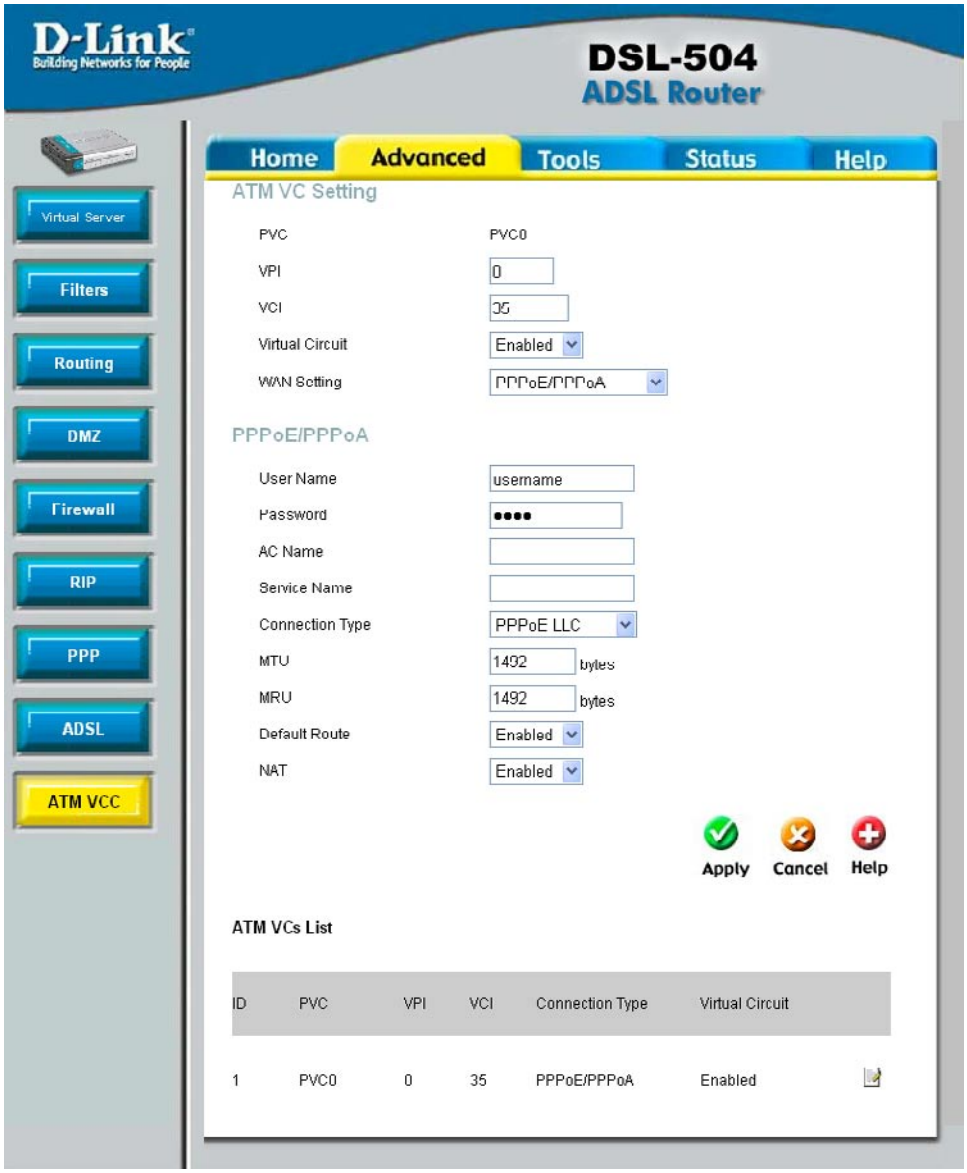
Advanced - ADSL

Select the ADSL modulation type in this window.

Advanced - ATM VC

The ATM Virtual Circuit connection menu is used to configure the WAN connection. If you are using multiple PVCs, you can change the configuration of any PVC in this menu. To create new or additional PVCs, read the section below on Multiple PVCs.

This menu can be used as an alternative menu to configure the same settings found on the WAN menu in the Home directory.



To configure an existing PVC configuration set, click the corresponding notepad icon in the right-hand column of the ATM VCs List. The PVCs current settings appear above in the entry fields of the ATM VC Settings menu. Configure the appropriate settings and click the **Apply** button to put the new settings into effect.

Tools - Admin

Click the **Tools** tab to reveal the menu buttons for various functions located in this directory. These menus are used to change the system password used to access the web manager, to save or load Router configuration settings, upgrade the device firmware, save current configuration settings, restore default settings, and to perform miscellaneous actions such performing Ping tests. These menus are described here.

To change the password used to access the Router web manager, click the **Admin** button in the **Tools** directory to display the Administrator Settings menu. Under the Administrator heading, type the **New Password** and **Confirm Password** to be certain you have typed it correctly. Click the **Apply** button to activate the new password. The System User Name (Login Name) remains "admin", this cannot be changed using the web manager interface. Be sure to save the new setting (see the instructions on the following page).

Tools - Admin (continued)

Enable Remote Web Management and Telnet Access

The Administrator Settings menu (see above) is also used to enable remote Telnet management and remote web management access to the Router. To enable remote management of the Router, select the **Enabled** radio button for either Remote Web or Remote Telnet Management and type the IP Address and Netmask of the remote network or system used for management. Click the **Apply** button to activate remote management from the chosen IP address. Be sure to save the new setting.

Tools - Time

The Router provides a number of options to maintain current date and time including SNTP.

To configure system time on the Router, select the method used to maintain time. The options available include SNTP, using your computer's system clock (default) or set the time and date manually. If you opt to use SNTP, you must enter the SNTP server URL or IP address. Click the **Apply** button to set the system time.

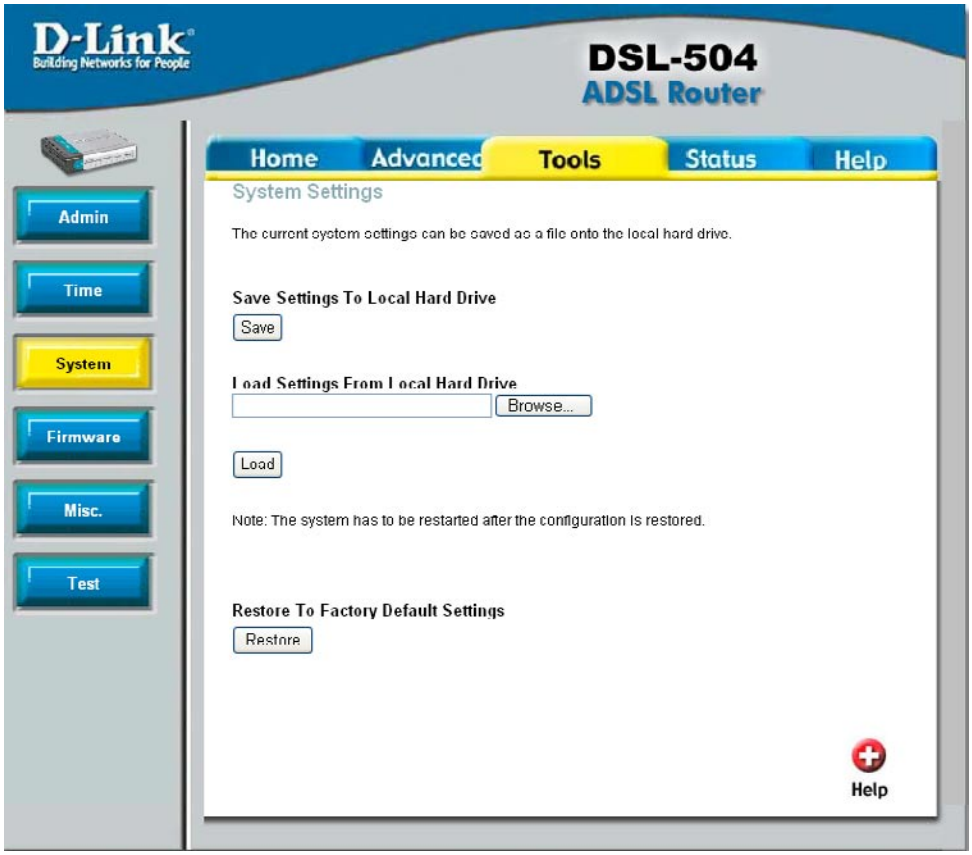
Tools - System

Save Configuration File to PC

Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. Use the System Setting menu to save the existing configuration file to the hard drive of the system you are using to access the web manager. To save the system configuration file to your computer, click the **Save** button. You will be prompted to select a location on your computer to put the file. The file type is .cfg and may be named anything you wish.

Load Saved Configuration Files

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Or type the full path and file name of the .cfg file in the space provided. Click the **Load** button to begin transferring and loading the .cfg file to the Router. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.



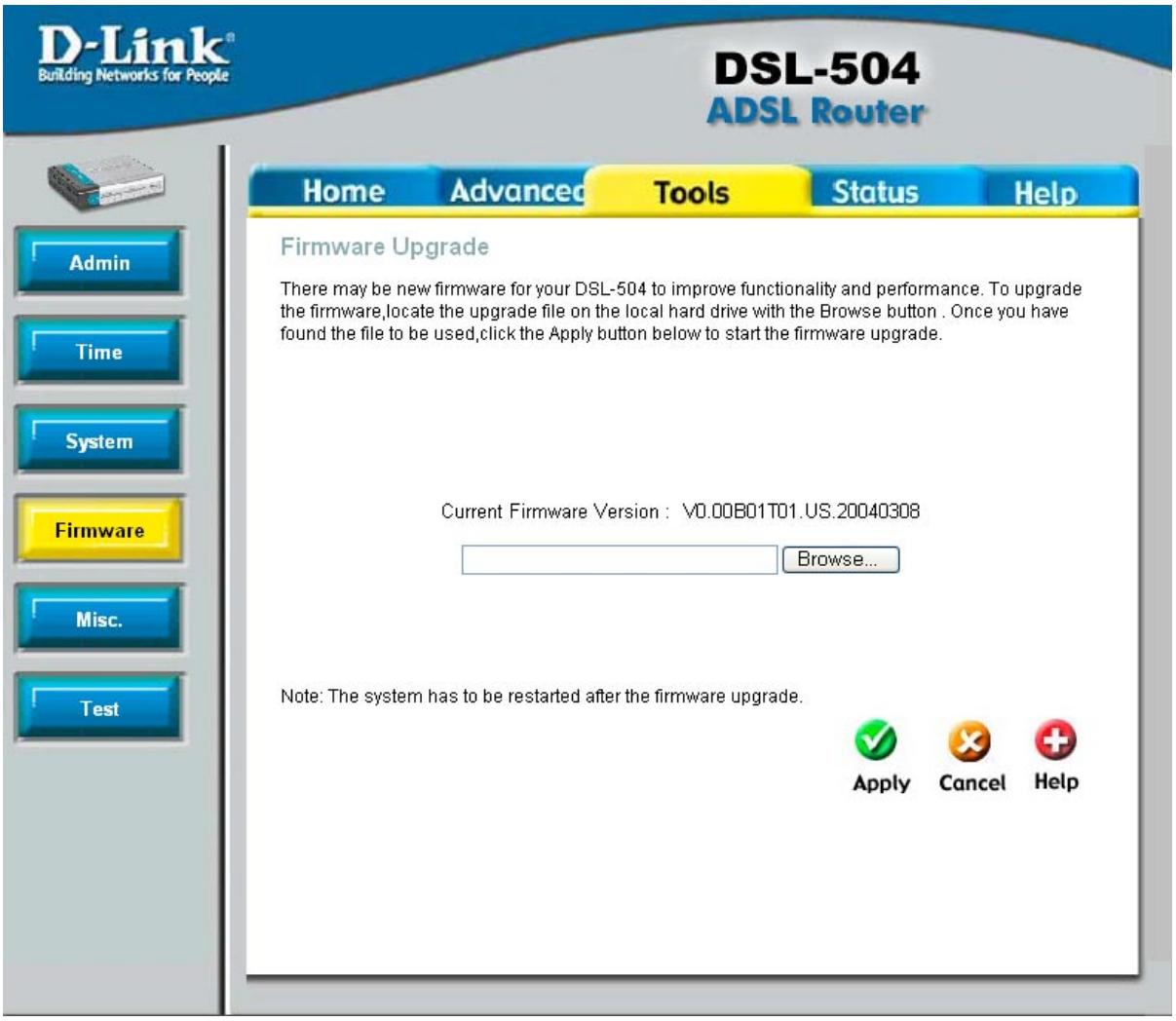
Restore Factory Default Settings

To reset the Router to its factory default settings, click the **Restore** button. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings. Depending on your IP settings, you may be logged out of the router.

Tools - Firmware

Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the Router's configuration settings before upgrading the firmware. Loading saved config files from earlier firmware is not recommended.

Use the Firmware Upgrade menu to load the latest firmware for the device. Note that the device configuration settings may return to the factory default settings, so make sure you save the configuration settings with the System Settings menu described above.



To upgrade firmware, type in the name and path of the file or click on the **Browse** button to search for the file. Click the **Apply** button to begin copying the file. The file will load and restart the Router automatically.

Tools - Misc

Other functions available in the Miscellaneous Configuration menu are a Ping test and IGMP enable/disable.

Ping Test

The Ping test functions on the WAN and LAN interfaces. Type the IP address you want to check in the space provided and click the **Ping** button. Read the Ping test result in the space immediately below.

IGMP

This is **Disabled** by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks, most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. If you are unsure, check with your ISP. To enable IGMP service to the LAN interface, select **Enabled** and click the **Apply** button.

UPnP

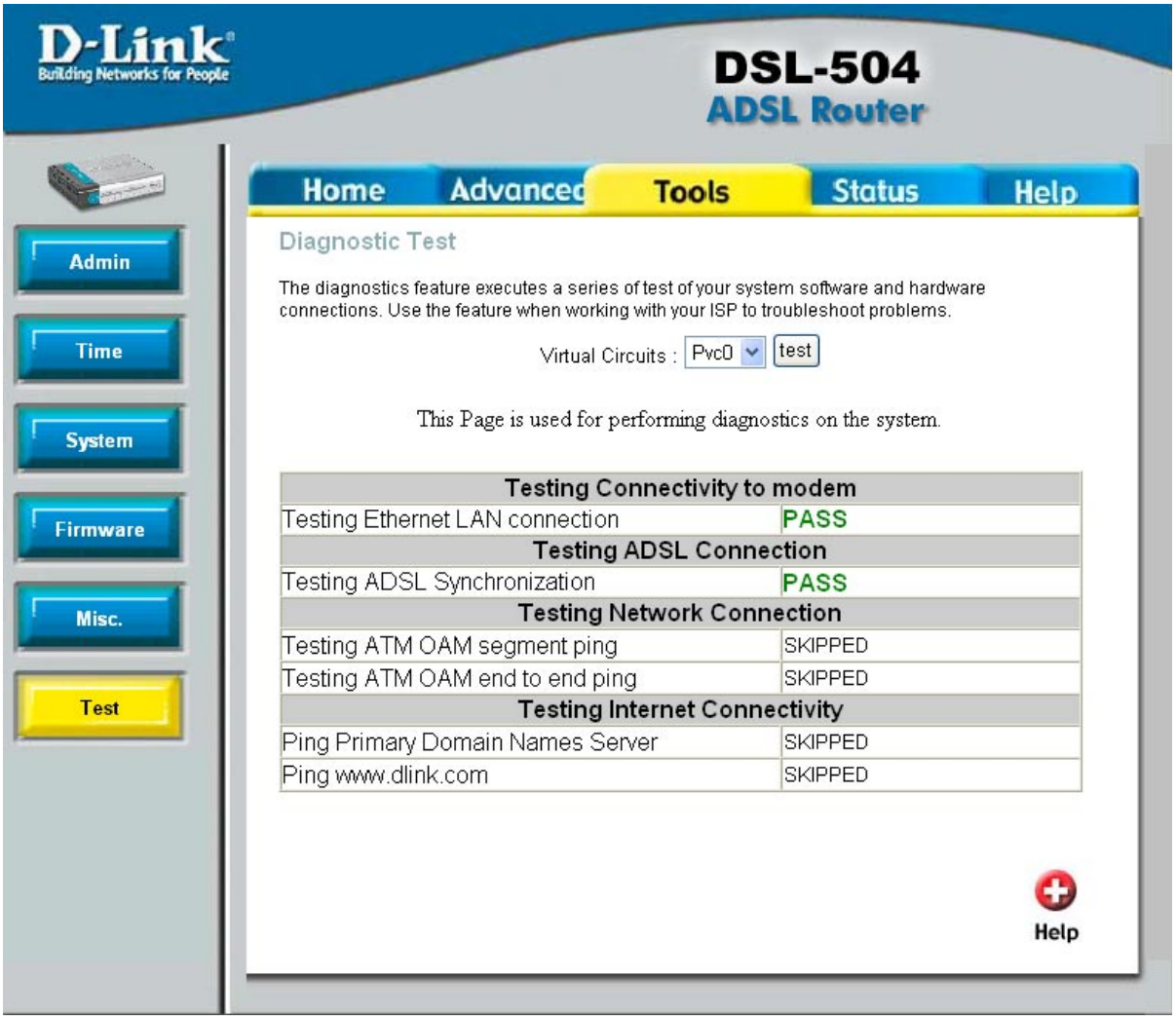
Enable or Disable UPnP (Universal Plug and Play).

Save Router Configuration Settings

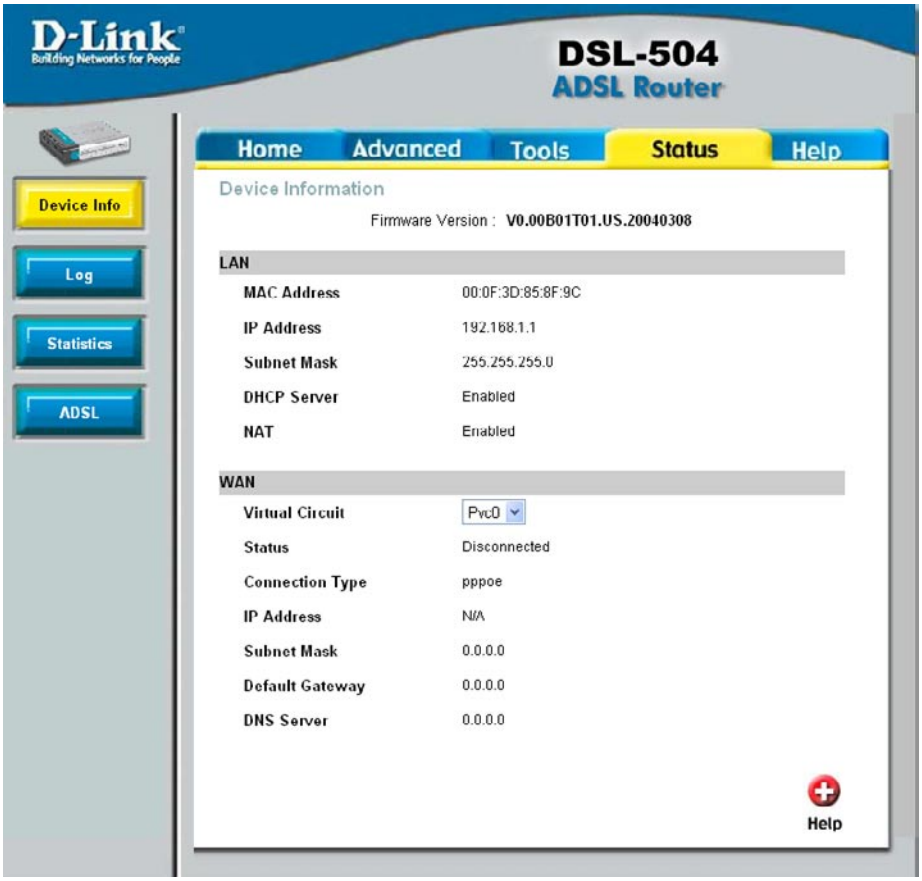
When you have completed configuration of the Router, make sure you save the current configuration settings to flash memory or risk losing the settings. To save the current configuration settings, click the **Misc.** menu button to view the **Miscellaneous Configuration** menu and click the **Reboot** button. The current settings will be saved to NV-RAM and the system will restart. Do not turn off the Router during this process. It should take about two minutes to complete. After restarting, it is a good idea to backup the Router configuration file to your computer. See the instructions below to save configuration files to your PC.

Tools - Test

This section provides connection information based on the Virtual Circuit that is selected. To view other Virtual Circuits, select from the drop down menu.



Status - Device Info



Router Status Information

Use the various read-only menus to view system information and monitor performance.

Device Information Display

Use the Device Information window to quickly view basic current information about the LAN and WAN interfaces. The basic information available in this window is summarized below.

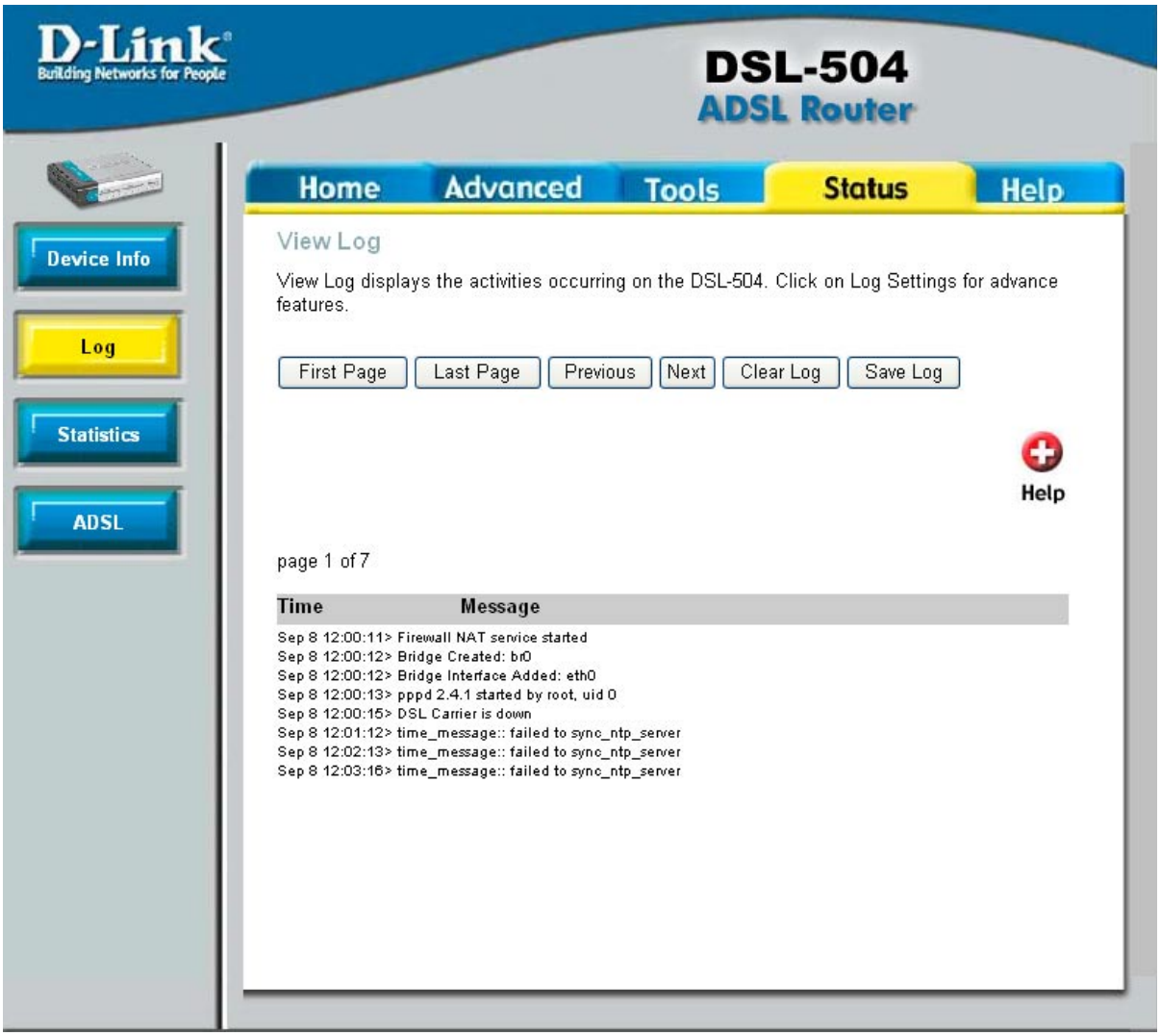
LAN

The MAC Address of the Ethernet LAN connection, IP Address, and Subnet Mask information will be displayed, as well as the setting (Enabled/Disabled) for the DHCP Server.

WAN (ADSL)

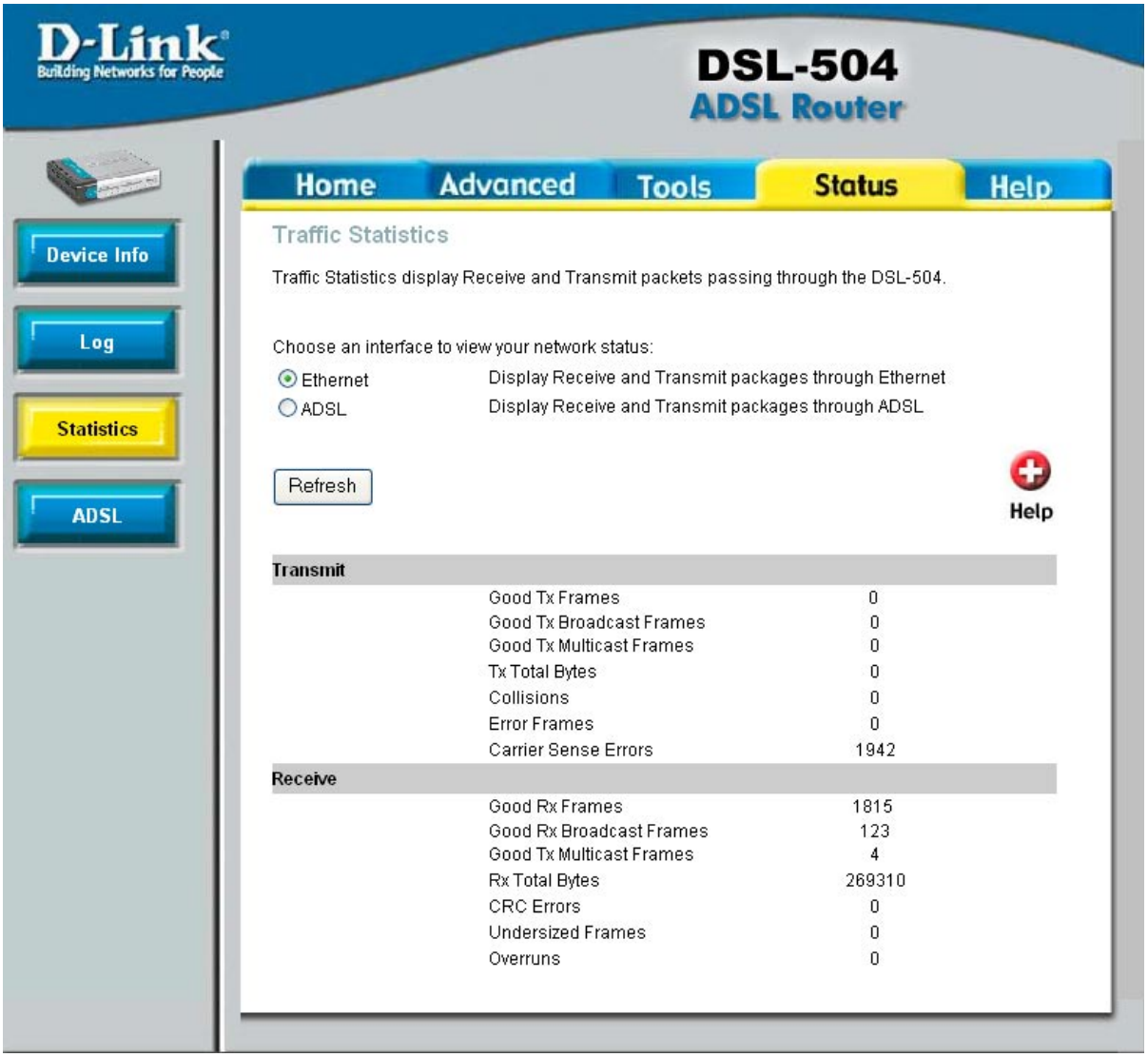
The MAC Address of the Ethernet WAN connection, IP Address, Subnet Mask, Default Gateway, and DNS (Domain Name Server) information will be listed. The connection type includes Dynamic, Static, PPPoE, PPPoE/PPPoA, and Bridged.

Status - Log



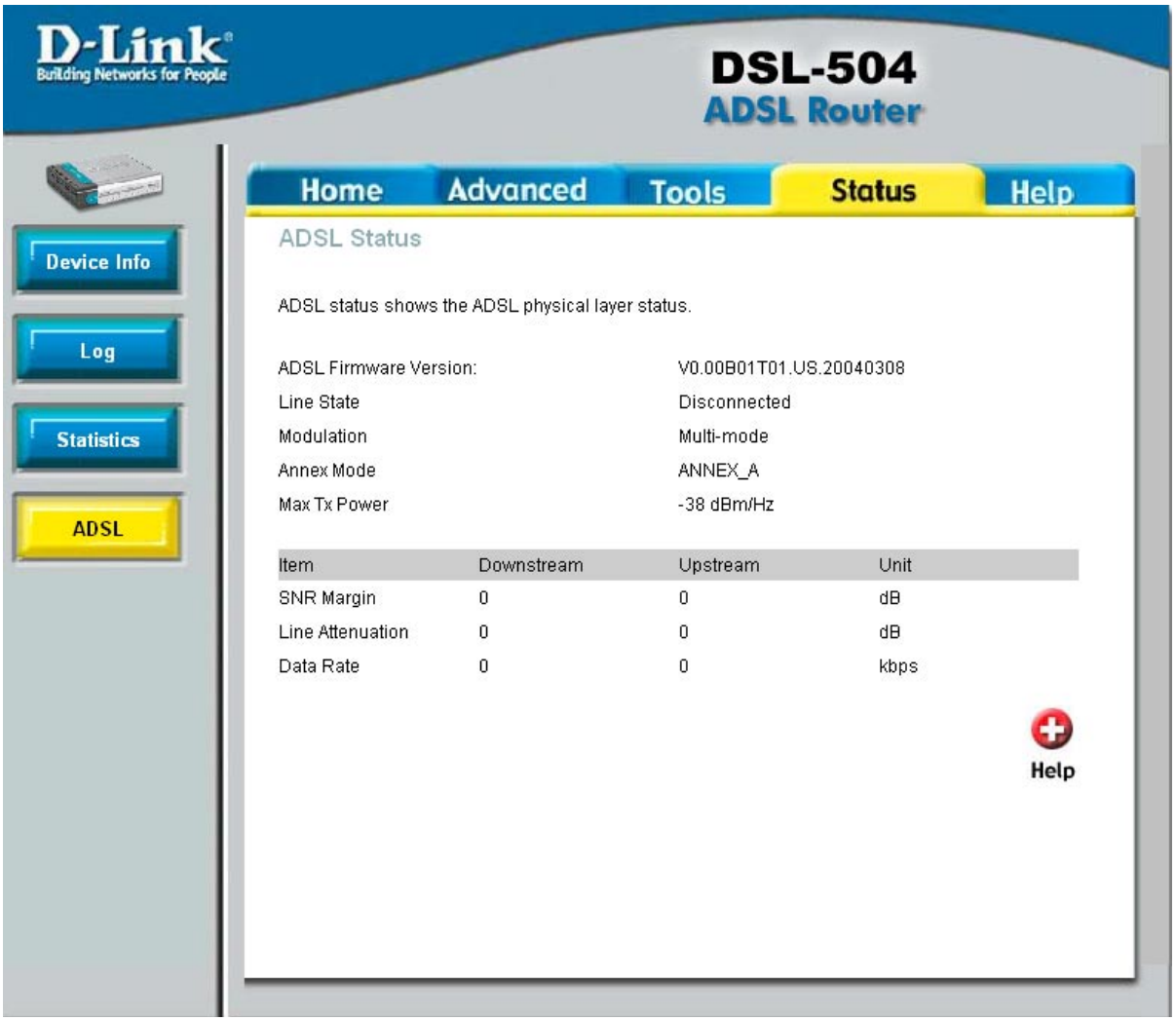
View, save and change log settings in this window.

Status - Statistics



View statistics for either the Ethernet or the ADSL network here.

Status - ADSL



View the ADSL statistics in this window.

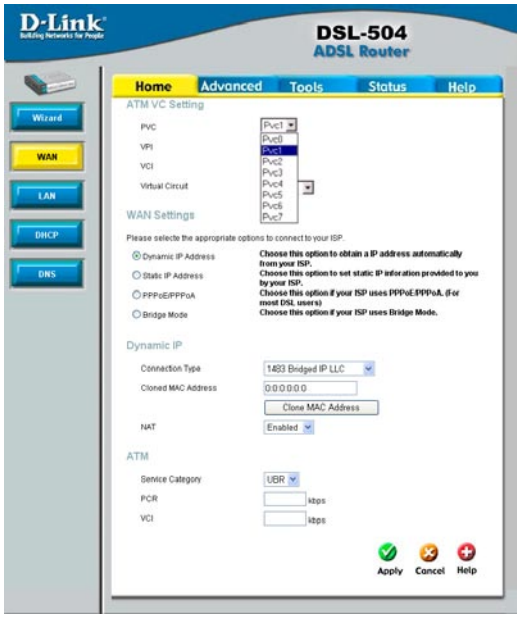
Multiple Virtual Connections

The Router supports multiple virtual connections. Up to eight PVCs to eight separate destinations can be created and operated simultaneously utilizing the same bandwidth. Additional PVC connections can be added for various purposes. For example, you may want to establish a private connection to remote office in order to create an extended LAN, or setup a server on a separate connection. Provisioning for additional PVC profiles must be done through your telecommunications services provider. Extended LAN operations employing multiple virtual connections require ADSL routers or modems at the remote site for a successful connection. Contact your ISP or telecommunications service provider if you are interested in setting up multiple virtual connections.

After the necessary arrangements have been made to use the Router with multiple virtual connections, follow the instructions below to setup the Router using the VPI/VCI settings given to you by your server provider.

Configure Multiple PVCs

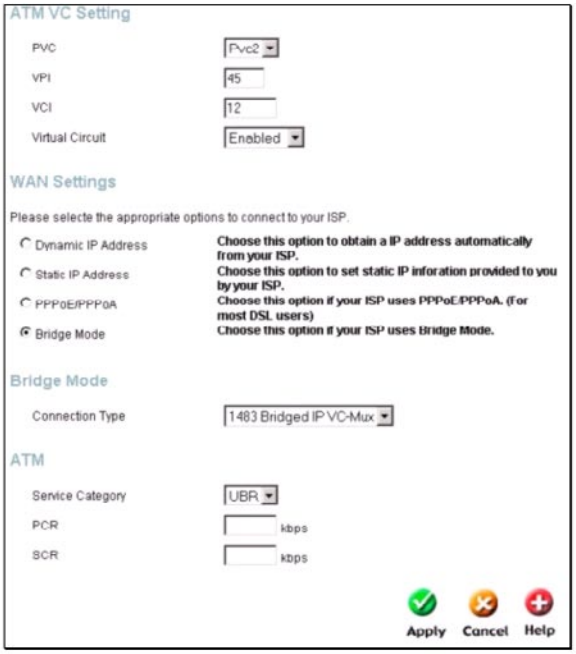
Additional PVCs can be configured by first accessing the WAN configuration menu in the Home directory.



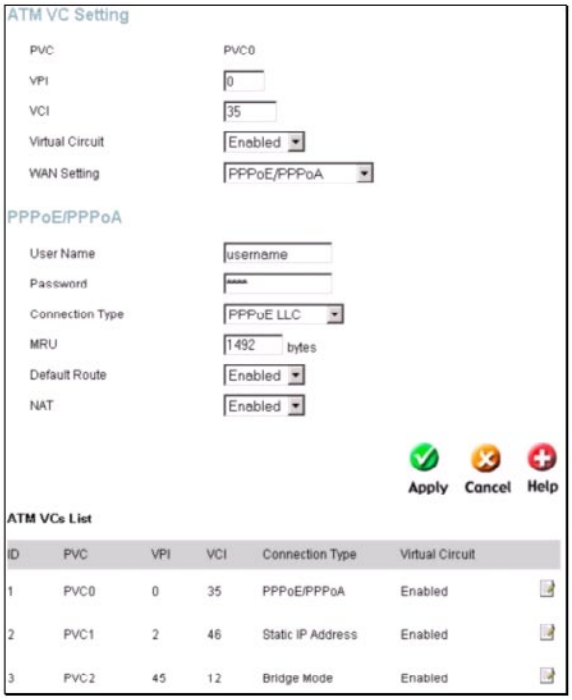
The PVC pull-down menu offers 8 virtual connections available for configuration. The default VC used by the Router is labeled Pvc0. Any additional connections that are configured must have a VPI/VCI combination that is unique to the Router. These numbers will have been already been established by your service provider on their network.
To add a new virtual connection:

1. Select the new **PVC** to configure from the pull-down menu.
2. Enter the values for the **VPI** and **VCI** given to you by your service provider.
3. To activate the VC, select *Enabled* from the **Virtual Circuit** pull-down menu.
4. Configure the WAN Settings and Connection Type as desired.

In the example below, a new VC (Pvc2) has been added using the WAN Settings menu. The connection is setup as a bridged connection.



The new VC appears listed in the ATM VC Setting menu located in the Advanced directory.



Any VC may be configured in the ATM VC menu by clicking the notepad icon for the PVC you want to configure. VCs configured with PPP connection types can be further configured in the PPP menu.

Technical Specifications

Standards

ITU G.992.1 (G.dmt) Annex A
ITU G.992.2 (G.lite) Annex A
ITU G.994.1 (G.Hs)
ITU-T Rec. I.361
ITU-T Rec. I.610
IEEE 802.3
IEEE 802.3u
IEEE 802.1d
RFC 791 (IP Routing)
RFC 792 (UDP)
RFC 826 (ARP)
RFC 1058 (RIP 1)
RFC 1389 (RIP 2)
RFC 1213 compliant
RFC 1483 (Bridged Ethernet)
RFC 1577 (IP over ATM)
RFC 1661 (PPP)
RFC 1994 (CHAP)
RFC 1334 (PAP)
RFC 2364 (PPP over ATM)
RFC 1631 (NAT)
RFC 1877 (Automatic IP assignment)
RFC 2516 (PPP over Ethernet)
Supports RFC 2131 and RFC 2132 (DHCP)
Compatible with all T1.413 issue 2 (full rate DMT over analog POTS), and CO DSLAM equipment
Supports ATM Forum UNI V3.1 PVC

Protocols

TCP/IP
UDP
RIP-1
RIP-2
IGMP
DHCP
BOOTP
ARP
AAL5

Data Transfer Rate

G.dmt full rate: Downstream up to 8 Mbps
Upstream up to 640 Kbps
G.lite: Downstream up to 1.5 Mbps
Upstream up to 512 Kbps

Media Interface

RJ-11 port ADSL telephone line connection
4 x RJ-45 ports for 10/100BASET Ethernet connection

Technical Specifications (continued)

Physical and Environmental	
DC Inputs **Power Adapter**	Input: 100V AC 50 ~ 60Hz Output: 12V AC, 1.2A
Power Consumption	12 Watts (max)
Operating Temperature	0° to 40° C (32° - 104° F)
Humidity	5 to 95% (non-condensing)
Dimensions	7.09 x 5.59 x 1.18 inches
Weight	0.8223 lbs.
EMI	CE Class B, FCC Class B (Part 15)
Safety	CSA International

Appendix A: IP Address Setup

IP Address Setup

The DSL-504T is designed to provide network administrators maximum flexibility for IP addressing on the Ethernet LAN. The easiest IP setup choice in most cases is to let the Router do it using DHCP, which is enabled by default. This appendix briefly describes various options including DHCP, used for IP setup on a LAN. If you are new to IP networking, the next appendix provides some background information on basic IP concepts.

Assigning Network IP Addresses

The IP address settings, which include the IP address, subnet mask and gateway IP address are the first and most important internal network settings that need to be configured. The Router is assigned a default LAN IP address and subnet mask. If you do not have a preexisting IP network and are setting one up now, using the factory default IP address settings can greatly ease the setup process. If you already have a preexisting IP network, you can adjust the IP settings for the Router to fit within your existing scheme.

Using the Default IP Address

The Router is shipped with a preset default IP address setting of 192.168.1.1 for the LAN port. There are two ways to use this default IP address, you can manually assign an IP address and subnet mask for each PC on the LAN or you can instruct the Router to automatically assign them using DHCP. The simplest method is to use DHCP. The DHCP function is active by default.

Manual IP Address Assignment

Manually configuring IP settings for the LAN means you must manually set an IP address, subnet mask and IP address of the default gateway (the Router's IP address) on each networked computer. The example listed below describes IP configuration for computers running Windows 95 or Windows 98. Regardless of what operating system is used on each workstation, the three network IP settings must be defined so the network interface used by each workstation can be identified by the Router, and vice versa. For detailed information about configuring your workstations IP settings, consult the user's guide included with the operating system or the network interface card (NIC).

1. In Windows 95/98, click on the **Start** button, go to **Settings** and choose **Control Panel**.
2. In the window that opens, double-click on the **Network** icon.
3. Under the Configuration tab, select the **TCP/IP** component and click *Properties*.
4. Choose the *Specify an IP address* option and edit the address settings

IP Address Setup (continued)

Using Default IP without DHCP

Host	IP Address	Subnet Mask	Gateway IP
Router	192.168.1.1	255.255.255.0	
Computer #1	192.168.1.2	255.255.255.0	192.168.1.1
Computer #2	192.168.1.3	255.255.255.0	192.168.1.1
Computer #3	192.168.1.4	255.255.255.0	192.168.1.1

IP Setup - Example #1

Please note that when using the default IP address as in the above example, the first, second and third number in the IP address must always be the same with only the fourth number changing. The first number defines the network IP address (all machines must belong to the same IP network), while the last number denotes the host IP address (each computer must have a unique address to distinguish it on the network). The IP address scheme used in Example #1 can be used for any LAN that requires up to 253 separate IP addresses (excluding the Router). Notice that the subnet mask is the same for all machines and the default gateway address is the LAN IP address of the Router.

It is a good idea to make a note of each device's IP address for reference during troubleshooting or when adding new stations or devices.

Using DHCP

The second way to use the default settings is to allow the Router to automatically assign IP settings for workstation using DHCP. To do this, simply make sure your computer's IP addresses are set to 0.0.0.0 (under Windows, choose the option Obtain an IP address automatically in the TCP/IP network component described above). When the computers are restarted, their IP settings will automatically be assigned by the Router. The Router is set by default to use DHCP. See the discussion in Chapter 3 for information on how to use configure the Router for DHCP.

Changing the IP Address of the Router

When planning your LAN IP address setup, you may use any scheme allowed by rules that govern IP assignment. It may be more convenient or easier to remember an IP scheme that use a different address for the Router. Or you may be installing the Router on a network that has already established the IP settings. Changing the IP address is a simple matter and can be done using the web manager (see *LAN IP Address* in Chapter 5). If you are incorporating the Router into a LAN with an existing IP structure, be sure to disable the DHCP function. Also, consider the effects of NAT (Network Address Translation). This is enabled by default but may be disabled in the NAT menu of the Advanced directory.

An IP addressing scheme commonly used for Ethernet LANs establishes 10.0.0.1 as the base address for the network. Using Example #2 below, the Router is assigned the base address 10.0.0.1 and the remaining addresses are assigned manually or using DHCP.

IP Address Setup (continued)

Alternative IP Assignment

Host	IP Address	Subnet Mask	Gateway IP
Router	10.0.0.1	255.0.0.0	
Computer #1	10.0.0.2	255.0.0.0	10.0.0.1
Computer #2	10.0.0.3	255.0.0.0	10.0.0.1
Computer #3	10.0.0.4	255.0.0.0	10.0.0.1

IP Setup - Example #2

These two examples are only examples you can use to help you get started. Other common private network IP addressing schemes use a base address of 192.168.1.1 or 192.168.0.1. If you are interested in more advanced information on how to use IP addressing on a LAN there are numerous resources freely available on the Internet. There are also many books and chapters of books on the subject of IP address assignment, IP networking and the TCP/IP protocol suite.

Appendix B: IP Concepts

This appendix describes some basic IP concepts, the TCP/IP addressing scheme and shows how to assign IP Addresses.

When setting up the Router, you must make sure it has a valid IP address. Even if you will not use the WAN port (ADSL port), you should, at the very least, make sure the Ethernet LAN port is assigned a valid IP address. This is required for telnet, in-band SNMP management, and related functions such as "trap" handling and TFTP firmware download.

IP Addresses

The Internet Protocol (IP) was designed for routing data between network sites all over the world, and was later adapted for routing data between networks within any site (often referred to as "subnetworks" or "subnets"). IP includes a system by which a unique number can be assigned to each of the millions of networks and each of the computers on those networks. Such a number is called an IP address.

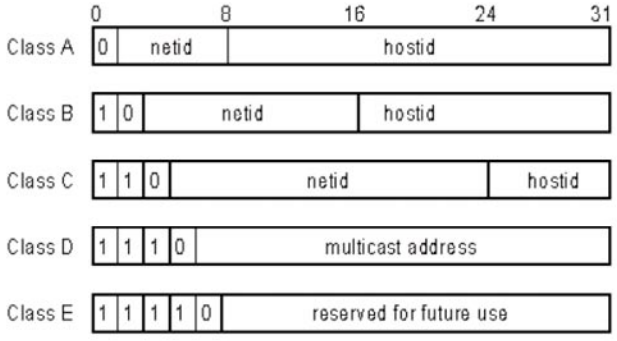
To make IP addresses easy to understand, the originators of IP adopted a system of representation called "dotted decimal" or "dotted quad" notation. Below are examples of IP addresses written in this format:

201.202.203.204 189.21.241.56 125.87.0.1

Each of the four values in an IP address is the ordinary decimal (base 10) representation of a value that a computer can handle using eight "bits" (binary digits — 1s and 0s). The dots are simply convenient visual separators.

Zeros are often used as placeholders in dotted decimal notation; 189.21.241.56 can therefore also appear as 189.021.241.056.

IP networks are divided into three classes on the basis of size. A full IP address contains a network portion and a "host" (device) portion. The network and host portions of the address are different lengths for different classes of networks, as shown in the table below.



Networks attached to the Internet are assigned class types that determine the maximum number of possible hosts per network. The previous figure illustrates how the net and host portions of the IP address differ among the three classes. Class A is assigned to networks that have more than 65,535 hosts; Class B is for networks that have 256 to 65534 hosts; Class C is for networks with less than 254 hosts.

IP Concepts (continued)

IP Network Classes			
Class	**Maximum Number of Networks in Class**	**Network Addresses (Host Portion in Parenthesis)**	**Maximum Number of Hosts per Network**
A	126	1(.0.0.0) to 126(.0.0.0)	16,777,214
B	16,382	128.1(.0.0) to 191.254(.0.0)	65,534
C	2,097,150	192.0.1(.0) to 223.255.254(.0)	254

Note: All network addresses outside of these ranges (Class D and E) are either reserved or set aside for experimental networks or multicasting.

When an IP address's host portion contains only zero(s), the address identifies a network and not a host. No physical device may be given such an address.

The network portion must start with a value from 1 to 126 or from 128 to 223. Any other value(s) in the network portion may be from 0 to 255, except that in class B the network addresses 128.0.0.0 and 191.255.0.0 are reserved, and in class C the network addresses 192.0.0.0 and 223.255.255.0 are reserved.

The value(s) in the host portion of a physical device's IP address can be in the range of 0 through 255 as long as this portion is not all0 or all255. Values outside the range of 0 to 255 can never appear in an IP address (0 to 255 is the full range of integer values that can be expressed with eight bits).

The network portion must be the same for all the IP devices on a discrete physical network (a single Ethernet LAN, for example, or a WAN link). The host portion must be different for each IP device — or, to be more precise, each IP-capable port or interface — connected directly to that network.

The network portion of an IP address will be referred to in this manual as a **network number**; the host portion will be referred to as a **host number**.

To connect to the Internet or to any private IP network that uses an Internet-assigned network number, you must obtain a registered IP network number from an Internet-authorized network information center. In many countries you must apply through a government agency, however they can usually be obtained from your Internet Service Provider (ISP).

If your organization's networks are, and will always remain, a closed system with no connection to the Internet or to any other IP network, you can choose your own network numbers as long as they conform to the above rules.

If your networks are isolated from the Internet, e.g. only between your two branch offices, you can assign any IP Addresses to hosts without problems. However, the Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of IP Addresses specifically for private (stub) networks:

IP Concepts (continued)

Class	Beginning Address	Ending Address
A	10.0.0.0	10.255.255.255
B	172.16.0.0	172.31.255.255
C	192.168.0.0	192.168.255.255

It is recommended that you choose private network IP Addresses from the above list. For more information on address assignment, refer to RFC 1597, *Address Allocation for Private Internets* and RFC 1466, *Guidelines for Management of IP Address Space*.

Subnet Mask

In the absence of subnetworks, standard TCP/IP addressing may be used by specifying subnet masks as shown below.

IP Class	Subnet Mask
Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

Subnet mask settings other than those listed above add significance to the interpretation of bits in the IP address. The bits of the subnet mask correspond directly to the bits of the IP address. Any bit an a subnet mask that is to correspond to a net ID bit in the IP address must be set to 1.

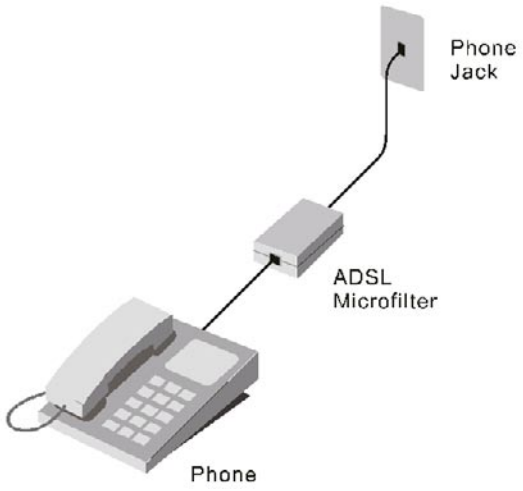
Appendix C: Microfilters & Splitters

Most ADSL clients will be required to install a simple device that prevents the ADSL line from interfering with regular telephone services. These devices are commonly referred to as microfilters or sometimes called (inaccurately) line splitters. They are easy to install and use standard telephone connectors and cable.

Some ADSL service providers will send a telecommunications technician to modify the telephone line, usually at the point where the telephone line enters the building. If a technician has divided or split your telephone line into two separate lines - one for regular telephone service and the other for ADSL – then you do not need to use any type of filter device. Follow the instructions given to you by your ADSL service provider about where and how you should connect the Router to the ADSL line.

Microfilters

Unless you are instructed to use a "line splitter" (see below), it is optional to install a microfilter (low pass filter) device for each telephone or telephone device (answering machines, Faxes etc.) that shares the line with the ADSL service. Microfilters are easy-to-install, in-line devices, which attach to the telephone cable between the telephone and wall jack. Microfilters that install behind the wall plate are also available. A typical in-line microfilter installation is shown in the diagram below.



Microfilter Installation

Important: Do not install the microfilter between the Router and the telephone jack. Microfilters are only intended for use with regular telephones, Fax machines and other regular telephone devices.

Microfilters and Splitters (continued)

Line Splitter

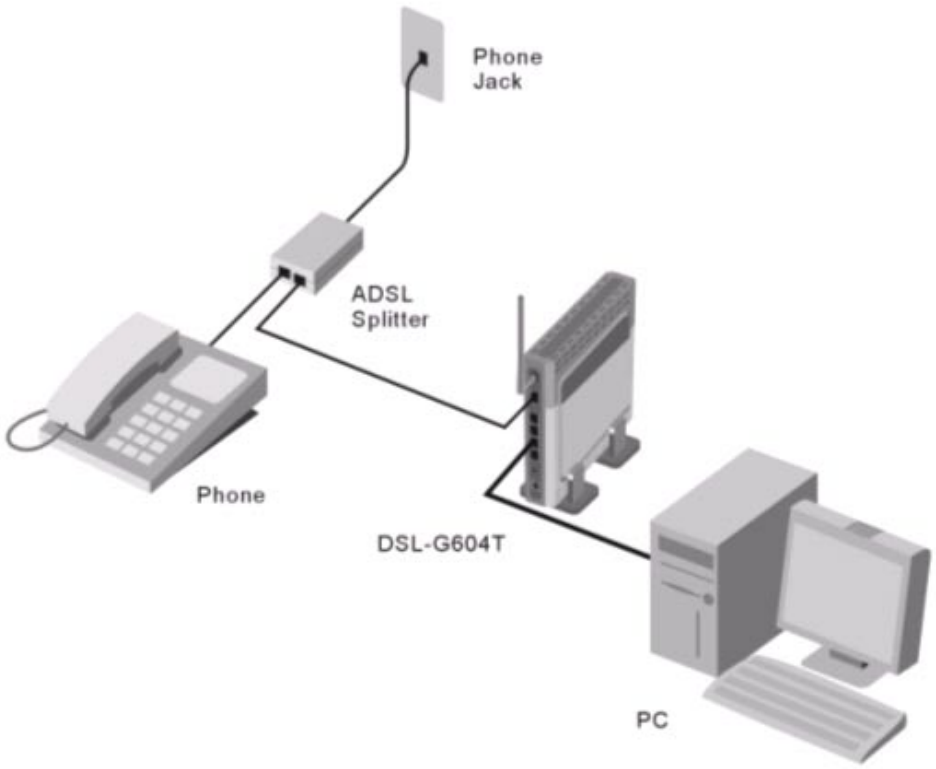
If you are instructed to use a "line splitter", you must install the device between the Router and the phone jack. Use standard telephone cable with standard RJ-11 connectors. The splitter has three RJ-11 ports used to connect to the wall jack, the Router and if desired, a telephone or telephone device. The connection ports are typically labeled as follows:

Line - This port connects to the wall jack.

ADSL – This port connects to the Router.

Phone – This port connects to a telephone or other telephone device.

The diagram below illustrates the proper use of the splitter.



Line Splitter Installation

Contacting Technical Support

You can find software updates and user documentation on the D-Link website.

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link technical support through our web site, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:
(877) 453-5465
Monday through Friday 6:00am to 6:00pm.
D-Link Technical Support over the Internet:
http://support.dlink.com
email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:
(800) 361-5265
Monday to Friday 8:30am to 9:00pm EST
D-Link Technical Support over the Internet:
http://support.dlink.ca
email:support@dlink.ca

When contacting technical support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited warranty for its product only to the person or entity that originally purchased the product from:

· D-Link or its authorized reseller or distributor and
· Products purchased and delivered within the fifty states of the United States, the District of Columbia, U.S. Possessions or Protectorates, U.S. Military Installations, addresses with an APO or FPO.

Limited Warranty: D-Link warrants that the hardware portion of the D-Link products described below will be free from material defects in workmanship and materials from the date of original retail purchase of the product, for the period set forth below applicable to the product type ("Warranty Period"), except as otherwise stated herein.

1-Year Limited Warranty for the Product(s) is defined as follows:

· Hardware (excluding power supplies and fans) One (1) Year
· Power Supplies and Fans One (1) Year
· Spare parts and spare kits Ninety (90) days

D-Link's sole obligation shall be to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund at D-Link's sole discretion. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or have an identical make, model or part. D-Link may in its sole discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. Repaired or replacement Hardware will be warranted for the remainder of the original Warranty Period from the date of original retail purchase. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

Limited Software Warranty: D-Link warrants that the software portion of the product ("Software") will substantially conform to D-Link's then current functional specifications for the Software, as set forth in the applicable documentation, from the date of original retail purchase of the Software for a period of ninety (90) days ("Warranty Period"), provided that the Software is properly installed on approved hardware and operated as contemplated in its documentation. D-Link further warrants that, during the Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. D-Link's sole obligation shall be to replace the non-conforming Software (or defective media) with software that substantially conforms to D-Link's functional specifications for the Software or to refund at D-Link's sole discretion. Except as otherwise agreed by D-Link in writing, the replacement Software is provided only to the original licensee, and is subject to the terms and conditions of the license granted by D-Link for the Software. Software will be warranted for the remainder of the original Warranty Period from the date or original retail purchase. If a material non-conformance is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to replace the non-conforming Software, the price paid by the original licensee for the non-conforming Software will be refunded by D-Link; provided that the non-conforming Software (and all copies thereof) is first returned to D-Link. The license granted respecting any Software for which a refund is given automatically terminates.

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product

purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

Submitting A Claim: The customer shall return the product to the original purchase point based on its return policy. In case the return policy period has expired and the product is within warranty, the customer shall submit a claim to D-Link as outlined below:

· The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.
· The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.
· After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.
· The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

· Return Merchandise Ship-To Address
USA: 17595 Mt. Herrmann, Fountain Valley, CA 92708
Canada: 2180 Winston Park Drive, Oakville, ON, L6H 5W1 (Visit http://www.dlink.ca for detailed warranty information within Canada)

D-Link may reject or return any product that is not packaged and shipped in strict compliance with the foregoing requirements, or for which an RMA number is not visible from the outside of the package. The product owner agrees to pay D-Link's reasonable handling and return shipping charges for any product that is not packaged and shipped in accordance with the foregoing requirements, or that is determined by D-Link not to be defective or non-conforming.

What Is Not Covered: This limited warranty provided by D-Link does not cover: Products, if in D-Link's judgment, have been subjected to abuse, accident, alteration, modification, tampering, negligence, misuse, faulty installation, lack of reasonable care, repair or service in any way that is not contemplated in the documentation for the product, or if the model or serial number has been altered, tampered with, defaced or removed; Initial installation, installation and removal of the product for repair, and shipping costs; Operational adjustments covered in the operating manual for the product, and normal maintenance; Damage that occurs in shipment, due to act of God, failures due to power surge, and cosmetic damage; Any hardware, software, firmware or other products or services provided by anyone other than D-Link; Products that have been purchased from inventory clearance or liquidation sales or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product. Repair by anyone other than D-Link or an Authorized D-Link Service Office will void this Warranty.

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED

WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

Limitation of Liability: TO THE MAXIMUM EXTENT PERMITTED BY LAW, D-LINK IS NOT LIABLE UNDER ANY CONTRACT, NEGLIGENCE, STRICT LIABILITY OR OTHER LEGAL OR EQUITABLE THEORY FOR ANY LOSS OF USE OF THE PRODUCT, INCONVENIENCE OR DAMAGES OF ANY CHARACTER, WHETHER DIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF GOODWILL, LOSS OF REVENUE OR PROFIT, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, FAILURE OF OTHER EQUIPMENT OR COMPUTER PROGRAMS TO WHICH D-LINK'S PRODUCT IS CONNECTED WITH, LOSS OF INFORMATION OR DATA CONTAINED IN, STORED ON, OR INTEGRATED WITH ANY PRODUCT RETURNED TO D-LINK FOR WARRANTY SERVICE) RESULTING FROM THE USE OF THE PRODUCT, RELATING TO WARRANTY SERVICE, OR ARISING OUT OF ANY BREACH OF THIS LIMITED WARRANTY, EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE SOLE REMEDY FOR A BREACH OF THE FOREGOING LIMITED WARRANTY IS REPAIR, REPLACEMENT OR REFUND OF THE DEFECTIVE OR NON-CONFORMING PRODUCT. THE MAXIMUM LIABILITY OF D-LINK UNDER THIS WARRANTY IS LIMITED TO THE PURCHASE PRICE OF THE PRODUCT COVERED BY THE WARRANTY. THE FOREGOING EXPRESS WRITTEN WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ANY OTHER WARRANTIES OR REMEDIES, EXPRESS, IMPLIED OR STATUTORY.

Governing Law: This Limited Warranty shall be governed by the laws of the State of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks: D-Link is a registered trademark of D-Link Systems, Inc. Other trademarks or registered trademarks are the property of their respective manufacturers or owners.

Copyright Statement: **No part of this publication or documentation accompanying this Product may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems, Inc., as stipulated by the United States Copyright Act of 1976. Contents are subject to change without prior notice. Copyright© 2002 by D-Link Corporation/D-Link Systems, Inc. All rights reserved.**

CE Mark Warning: This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Statement: **This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures**:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Registration

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

121604