

D-Link[®]

DSL-G664T
Wireless ADSL Router
User's Guide

(March 2004)

651G664T.015

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning

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

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstörungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo caso, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l'utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l'utente debba assumere provvedimenti adeguati.

TABLE OF CONTENTS

ABOUT THIS USER'S GUIDE	I
BEFORE YOU START	I
INSTALLATION REQUIREMENTS	I
PACKING LIST	IV
INTRODUCTION	1
Router Description and Operation.....	1
Standards Compatibility and Compliance.....	3
Packing List	4
Front Panel Display.....	4
Rear Panel Connections.....	5
Introduction to 802.11b Wireless	6
802.11g Wireless	6
Wireless LAN Basics.....	6
ADSL Technology.....	7
HARDWARE INSTALLATION	8
Location	8
Power on Router.....	9
Factory Reset Button.....	9
Network Connections.....	10
Power On Router.....	11
Factory Reset Button.....	11
BASIC ROUTER CONFIGURATION	12
Configuring IP Settings on Your Computer.....	12
Access the Configuration Manager	18
Login to Home Page.....	18
Configure the Router	19
Setup Menu.....	20
Wireless Settings.....	21
Wireless Security.....	22
Configure Connection 1 for PPPoA.....	26
Change the Connection Type	27
Configure Connection 1 for PPPoE.....	27
Configure Connection 1 for Bridge.....	29
Configure Connection 1 for Static IP for WAN.....	30
Configure Connection 1 for DHCP for WAN.....	32
Configure Connection 1 for CLIP.....	33
Create a New Connection	34
DHCP Configuration for LAN	36
Enable DHCP Relay.....	37
Management IP	38

Save Configuration Changes	39
---	-----------

ADVANCED ROUTER MANAGEMENT..... 41

UPnP.....	42
LAN Clients.....	43
Port Forwarding.....	44
Access Control.....	48
Advanced Security.....	50
Bridge Filters.....	51
Multicast Pass-through.....	52
Static Routing.....	53
Dynamic Routing.....	54

Wireless Management..... 55

Multiple Virtual Connections..... 55

Tools and Utility Menus..... 57

User Management.....	58
System Commands.....	59
Remote Log.....	60
Update Gateway.....	61
Ping Test.....	62
Modem Test.....	63

Status Menus..... 64

Network Statistics.....	65
Connection Status.....	66
DHCP Clients.....	67
Modem Status.....	68
Product Information.....	69
System Log.....	70
Help Menu.....	71

TECHNICAL SPECIFICATIONS..... 72

IP ADDRESS SETUP..... 74

IP CONCEPTS..... 76

MICROFILTERS AND SPLITTERS..... 79

About This User's Guide

This user's guide provides instructions on how to install the DSL-G664T ADSL Router and use it to connect a computer or Ethernet LAN to the Internet.

If you are using a computer with a functioning Ethernet port, the quickest and easiest way to set up the DSL-G664T is to insert the Installation CD into the CD-ROM drive of your computer and follow the instructions provided in the **Quick Installation Guide**.

Before You Start

Please read and make sure you understand all the prerequisites for proper installation of your new Router. Have all the necessary information and equipment on hand before beginning the installation.

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 set up 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-G664T 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.

802.11b Wireless LAN Configuration

All the 802.11b wireless LAN settings may be configured on a single page using the web-based manager. For basic wireless communication you need to decide what channel to use and what SSID to assign. These two settings must be the same for any wireless workstations or other wireless access point that communicate with the DSL-G664T through the wireless interface.

Security for wireless communication can be accomplished in a number of ways. The DSL-G664T supports WEP encryption, 802.1X authentication, and WPA (Wi-Fi Protected Access). Wireless access can also be controlled by selecting MAC addresses that are allowed to associate with the device. Please read the section on Wireless Configuration.

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 PPPoE, PPPoA or CLIP (IPoA) 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.

About CLIP Connections (RFC 1577)

Classical IP over ATM (CLIP) connections may require global IP settings for the device. Your service provider will give you IP settings information if needed. Some CLIP connections function like peer-to-peer connections and therefore do not require IP settings on the WAN interface.

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 – <u>user@isp.com</u> . Your ADSL service provider uses this to identify your account.	Record info here
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: PPPoE, PPPoA, PPPoA with DHCP, Bridge, and CLIP (IPoA).	
Modulation Type	ADSL uses various standardized modulation techniques to transmit data over the allotted signal frequencies. Some users may need to change the type of modulation used for their service. The default DSL modulation (MMODE) used for the Router automatically detects all types of ADSL modulation. However, if you are instructed to specify the modulation type used for the Router, you have three alternatives: G.LITE, G.DMT and T1.413	
Security 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 provider's network and your computer.	
IP Address (RADIUS server)	For 802.1X and WPA security.	
Port	For 802.1X and WPA security.	
Secret	For 802.1X and WPA security.	

Information you will need about your DSL-G664T 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 may be changed by the user.	Record info here
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-G664T	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 DSL-G664T	This is the subnet mask used by the DSL-G664T, and will be used throughout your LAN. The default subnet mask is 255.0.0.0 . 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-G664T to this Ethernet port using an Ethernet cable. You can also use the Ethernet port on the DSL-G664T to connect to other Ethernet devices, such as a Wireless Access Point.	Record info here
DHCP Client status	Your DSL-G664T 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-G664T 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 DHCP clients.)	

It is recommended that you 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-G664T 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 (see 錯誤! 找不到參照來源。 below).

Packing List

Open the shipping carton and carefully remove all items. Make sure that you have the items listed here.

1. One DSL-G664T 802.11g Wireless ADSL Ethernet Router
2. One CD-ROM containing the User's Guide
3. One twisted-pair telephone cable used for ADSL connection
4. One straight-through Ethernet cable
5. One AC power adapter suitable for your electric service
6. One Quick Installation Guide



Introduction

This section provides a brief description of the Router, its associated technologies and a list of Router features.

Router Description and Operation

The DSL-G664T ADSL Router is designed to provide a simple, cost-effective and secure ADSL Internet connection for wired (Ethernet) and wireless (802.11g) stations on your network. The DSL-G664T combines high-speed ADSL connection technology, TCP/IP routing and 802.11g wireless connectivity in one compact unit.

The Router is easy to install and use. The DSL-G664T connects to an Ethernet LAN via wireless and a standard Ethernet 10/100 BASE-T interface using RJ-45 connectors. The ADSL connection is made using ordinary twisted-pair telephone line with standard RJ-11 connectors. This arrangement allows wired and wireless workstations to share network resources and connect to the Internet using a single WAN interface and IP address.

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

All the 802.11g wireless settings for the Router are entered on a single page in the web manager. Security for the wireless interface comes in two forms, WEP Encryption and MAC Address Control.

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 800 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.

Router Features

The DSL-G664T ADSL Router utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. DSL-G664T advantages include:

- **PPP (Point-to-Point Protocol) Security** – The DSL-G664T 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-G664T 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-G664T 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-G664T supports both RIP-1 and RIP-2 exchanges with other routers. Using both versions lets 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-G664T 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 8 Mbps downstream bit rate using the G.dmt.
- **Full Network Management** – The DSL-G664T incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or Telnet connection.
- **Telnet Connection** – The Telnet enables a network manager to access the Router’s management software remotely.
- **Easy Installation** – The DSL-G664T uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.

Standards Compatibility and Compliance

The DSL-G664T complies with or is compatible with the following standards as recognized by their respective agencies.

- ITU G.992.1 (G.DMT) compliant
- 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 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 NAT for up to 4096 connections
- Supports DHCP for up to 253 host connections
- Supports IGMP
- Supports DVMRP
- 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

Packing List

Open the shipping carton and carefully remove all items. Make sure that you have the items listed here.

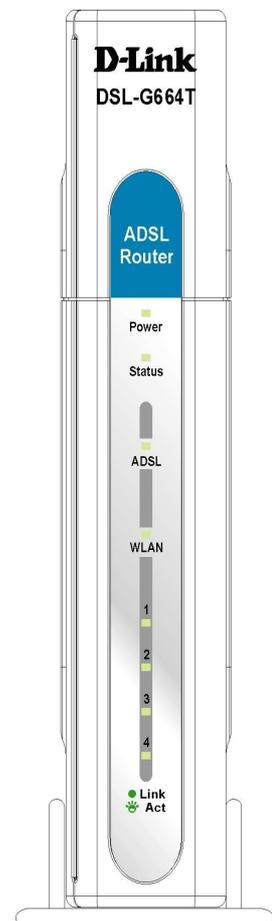
1. One DSL-G664T 802.11g Wireless ADSL Ethernet Router
2. One screw-on antenna
3. One CD-ROM containing the User's Guide
4. One twisted-pair telephone cable used for ADSL connection
5. One straight-through Ethernet cable
6. One AC power adapter suitable for your electric service
7. One Quick Installation Guide

Front Panel Display

Place the Router in a location that permits an easy view of the LED indicators on the front panel.

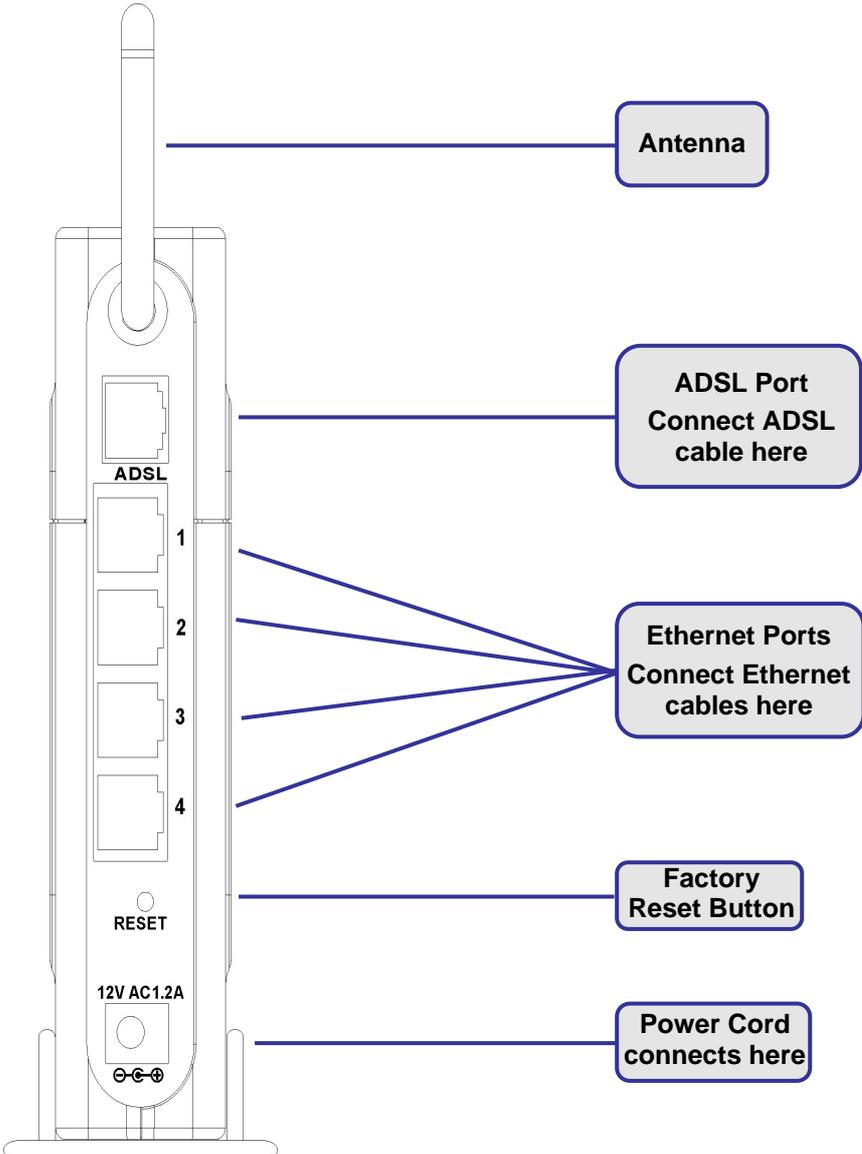
The LED indicators on the front panel include the **Power**, **Status**, **ADSL Link/Act** and **WLAN (1-4) Link/Act** indicators. The ADSL and Ethernet indicators monitor link status and activity (Link/Act).

Power	Steady green light indicates the unit is powered on. When the device is powered off this remains dark.
Status	Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator lights steady green after the POST, the system has failed and the device should be rebooted.
ADSL: Link/Act	Steady green light indicates a valid ADSL connection. This will light after the ADSL negotiation process has been settled. A blinking green light indicates activity on the WAN (ADSL) interface.
LAN 1 - 4: Link/Act	A solid green light indicates a valid link on startup. These lights blink when there is activity currently passing through the Ethernet 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 in the next chapter for instructions on using the reset button).



Note *The Router may be rebooted by disconnecting and then reconnecting the power.*

Introduction to 802.11b Wireless

The IEEE 802.11b standard is the most widely used standard for wireless LANs today. A wireless LAN (WLAN) is a cellular computer network that transmits data using radio signals instead of cables. WLAN technology is commonly used in home, small office and large corporate networks. WLAN devices have a high degree of mobility and flexibility that allow networks to be quickly set up or dismantled and allow them to roam freely throughout the network.

Wireless LAN users can use the same network applications used on an Ethernet LAN. 802.11b adapter cards used on laptop and desktop computers support the same protocols as Ethernet adapter cards. For most users, there is no functional difference between a computer attached to a wired Ethernet LAN or a mobile 802.11b workstation except that hardware is not physically attached to the network. For most networks however, it may be desirable for mobile network devices to be able to link to the wired Ethernet LAN to use shared resources such as servers, printers or an Internet connection. The DSL-G664T unites Ethernet and 802.11b wireless private networks with an Internet connection.

D-Link Wireless LAN devices have earned a reputation for reliability, flexibility and value. D-Link offers a full range of IEEE 802.11b and IEEE 802.1a WLAN products including:

- 802.11b and 802.11a Wireless Adapter cards for notebook computers
- 802.11b and 802.11a Wireless PCI cards for desktop computers
- 802.11b and 802.11a Wireless Access Points
- Dual-band (802.11b plus 802.11a) Wireless Access Points
- 802.11b and 802.11a Wireless Home Gateways
- 802.11b and 802.11a Wireless ADSL Routers

802.11g Wireless

Today's 11-megabits-per-second 802.11b wireless networks are fine for broadband Internet access (which typically tops out at about 1 mbps) but rather slow for large internal file transfers or streaming video. However, 54-mbps, corporate-oriented 802.11a is expensive--and because its radio uses the 5-GHz band and 802.11b uses the 2.4-GHz band, upgrading to an 802.11a network means either scrapping 802.11b gear or buying even-pricier hardware that can support both standards.

But 802.11g promises the same speed as 802.11a and the ability to coexist with 802.11b equipment on one network, since it too uses the 2.4-GHz band.

802.11g is an extension to 802.11b, the basis of many wireless LANs in existence today. 802.11g will broaden 802.11b's data rates to 54 Mbps within the 2.4 GHz band using OFDM (orthogonal frequency division multiplexing) technology. Because of backward compatibility, an 802.11b radio card will interface directly with an 802.11g access point (and vice versa) at 11 Mbps or lower depending on range. You should be able to upgrade the newer 802.11b access points to be 802.11g compliant via relatively easy firmware upgrades.

Similar to 802.11b, 802.11g operates in the 2.4GHz band, and the transmitted signal uses approximately 30MHz, which is one third of the band. This limits the number of non-overlapping 802.11g access points to three, which is the same as 802.11b.

Wireless LAN Basics

Some basic understanding of 802.11b wireless technology and terminology is useful when you are setting up the Router or any wireless access point. If you are not familiar with wireless networks please take a few minutes to learn the basics.

Radio Transmission

WLAN devices use electromagnetic waves within a broad, unlicensed range of the radio spectrum to transmit and receive radio signals. When a wireless access point is present, it becomes a base station for the WLAN nodes

in its broadcast range. WLAN nodes transmit digital data using FM (frequency modulation) radio signals. WLAN devices generate a carrier wave and modulate this signal using various techniques. In this way, digital data can then be superimposed onto the carrier signal. This radio signal carries data to WLAN devices within range of the transmitting device. The antennae of WLAN devices listen for and receive the signal. The signal is demodulated and the transmitted data extracted. The transmission method used by the access point is called Direct Sequence Spread Spectrum (DSSS) and operates in a range of the radio spectrum between 2.4GHz and 2.5GHz for transmission. DSSS is the preferred method used on many 802.11b and 802.11g devices.

Range

Range should not be a problem in most homes or small offices. If you experience low or no signal strength in some areas, consider positioning the Router in a location between the WLAN devices that maintains a roughly equal straight-line distance to all devices that need to access the Router through the wireless interface. Adding more 802.11b access points to rooms where the signal is weak can improve signal strength. Read the section about placement of the Router titled Location in the next chapter, Hardware Installation, for more information.

SSID

Wireless networks use an SSID (Service Set Identifier) to allow wireless devices to roam within the range of the network. Wireless devices that wish to communicate with each other must use the same SSID. Several access points can be set up using the same SSID so that wireless stations can move from one location to another without losing connection to the wireless network.

The DSL-G664T operates in *Infrastructure* mode. It controls network access on the wireless interface in its broadcast area. It will allow access to the wireless network to devices using the correct SSID after a negotiation process takes place. The DSL-G664T broadcasts its SSID so that any wireless station in range can learn the SSID and ask permission to associate with it. Many wireless adapters are able to survey or scan the wireless environment for access points. An access point in Infrastructure mode allows wireless devices to survey that network and select an access point with which to associate.

It is important to understand the difference between the SSID and a BSSID (Basic Service Set Identifier) or Preferred BSSID. The Preferred BSSID is defined by wireless stations to designate an access point used for access to the wireless network. The Preferred BSSID is the MAC address of the access point. Therefore any wireless stations (wireless clients) that use the DSL-G664T through the wireless interface must use its MAC address for the Preferred BSSID. A wireless station that scans the network for available access points may present the user with a choice of access points identified by their BSSID.

ADSL Technology

Asymmetric Digital Subscriber Line (ADSL) is a broadband technology that utilizes ordinary copper telephone lines to enable 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 for faster downloads and more reliable connectivity without interfering with regular telephone services. 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.

Hardware Installation

The DSL-G664T functions on three separate networks: a wired Ethernet LAN, a wireless LAN and a wired ADSL WAN. Placement of the Router must take into account the fact that it is connected to these three networks with three types of media. Ethernet cables connect the Router to computers and network devices and the ADSL line connects it to a wall socket. In addition, the device must be near an AC wall outlet for power. How to accommodate these wired connections is often not a complicated matter. However, the added dimension of wireless communication does complicate the decision of Router placement.

Location

Many environmental factors can affect the effective wireless function of the DSL-G664T. If this is your first time setting up a wireless network device, read and consider the points listed below.

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.

Designed to go up to 100 meters indoors and up to 300 meters outdoors, Wireless LAN lets you access your network from anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit the signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. To determine the range and signal strength, use these basic guidelines:

1. **Keep the number of walls and ceilings to a minimum:**
The signal emitted from Wireless LAN devices can penetrate through ceilings and walls. However, each wall or ceiling can reduce the range of Wireless LAN devices from 1 to 30M. Position your wireless devices so that the number of walls or ceilings obstructing the signal path is minimized.
2. **Consider the direct line between access points and workstations:** A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90° angle) a wall or ceiling for better reception.
3. **Building Materials make a difference:** Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.
4. **Position the antennas for best reception.** Play around with the antenna position to see if signal strength improves. Some adapters or access points allow the user to judge the strength of the signal.
5. **Keep your product away (at least 1-2 meters) from electrical devices:**
Position wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

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 a few 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 factory default IP address of the Router is 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 above 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

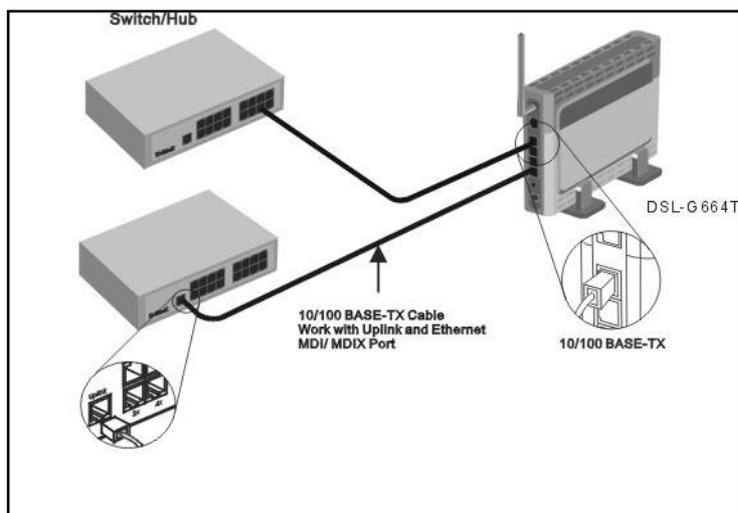
The Router may be connected to a single computer or Ethernet device through the 10/100 BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that 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.

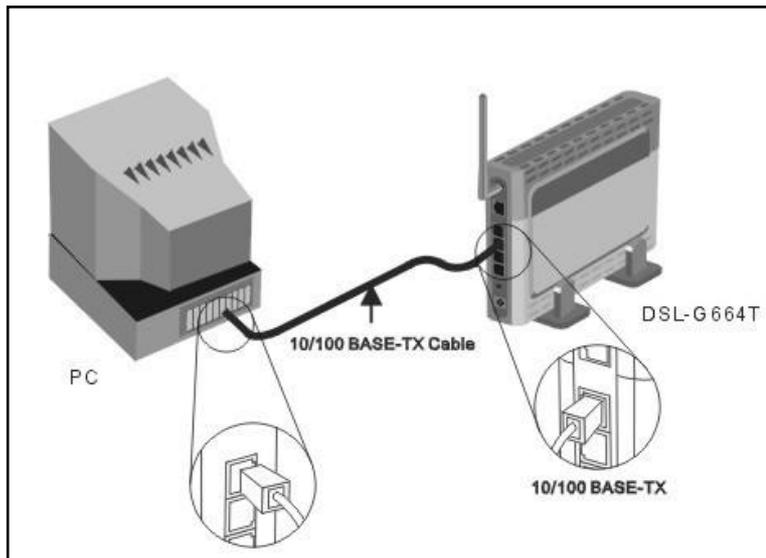
Hub or Switch to Router Connection

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.

Power On Router

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 you have the Router connected to your network you can look at the Ethernet Link/Act LED and WLAN indicators to make sure they have valid connections. The Router will attempt to establish the ADSL connection, if the ADSL line is connected and the connection is properly configured this should light up after several seconds.

Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to push down the reset button. Remember that this will wipe out any settings stored in flash memory including IP settings. The factory default IP address of the Router is 192.168.1.1 and the subnet mask is 255.255.255.0.

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 software 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. Below 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, configure the system to be a DHCP client.



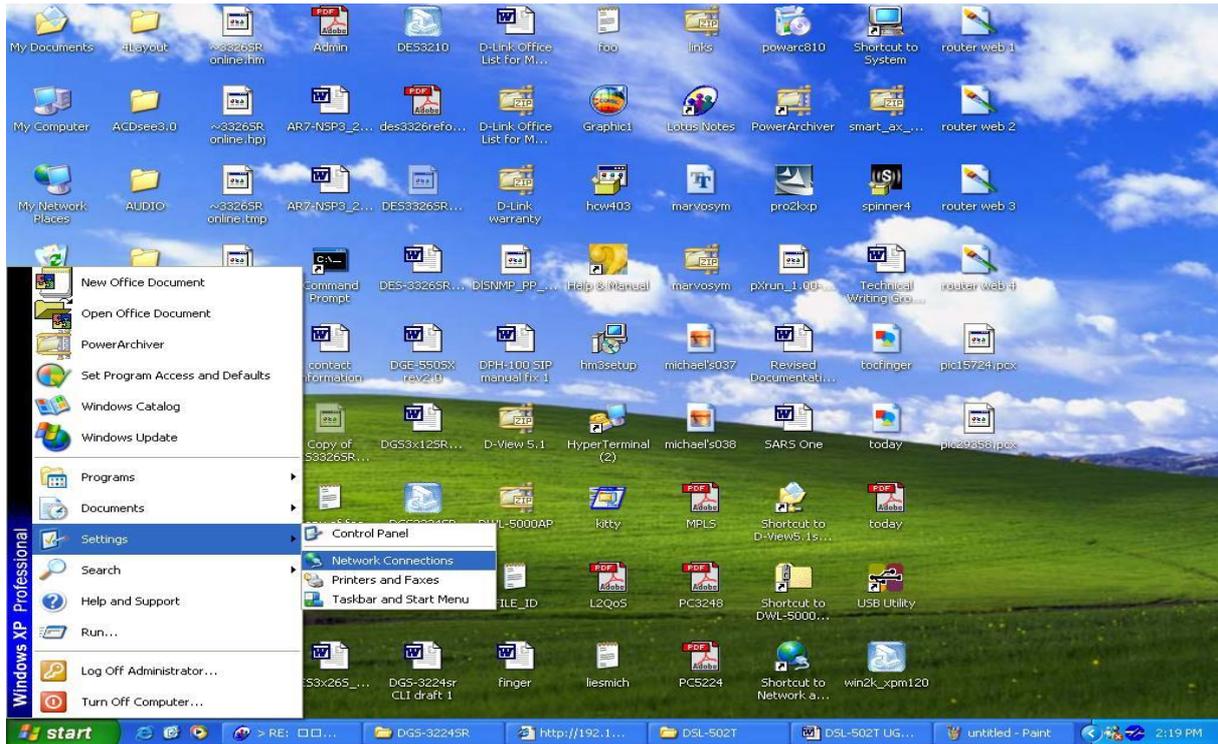
Note

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.

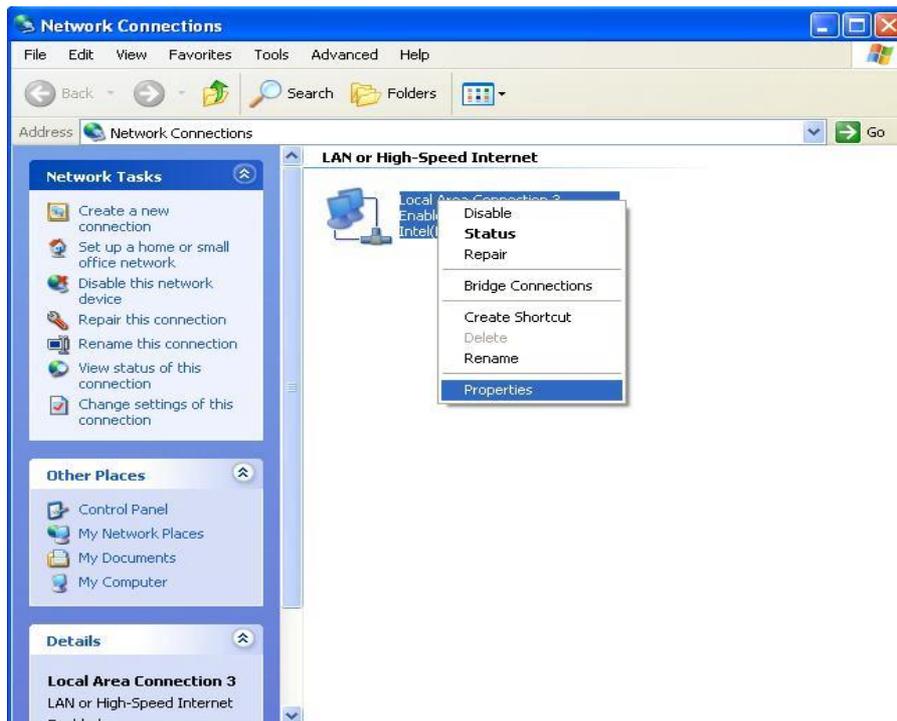
Configure Windows XP for DHCP

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

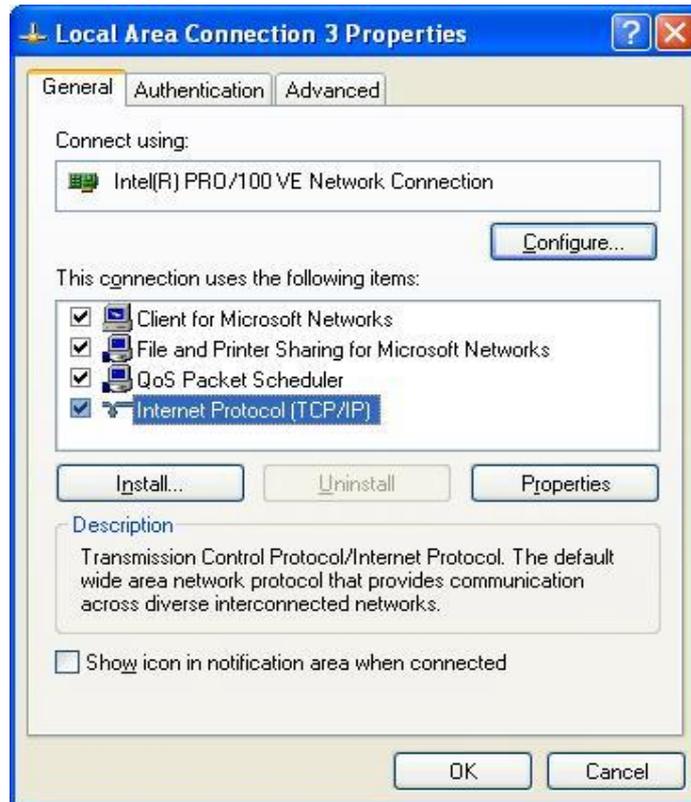
1. From the **Start** menu on your desktop, go to **Settings**, then click on **Network Connections**.



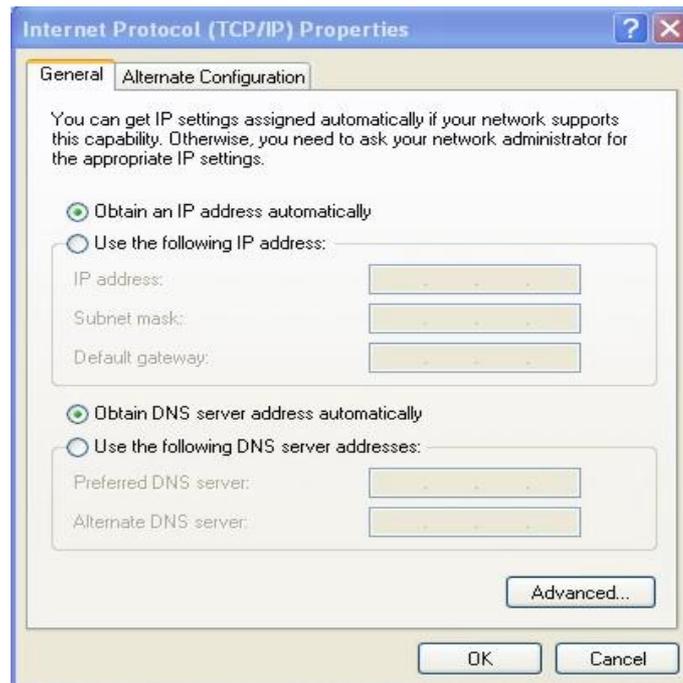
2. In the **Network Connections** window, right-click on **LAN (Local Area Connection)**, then click **Properties**.



3. 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.



4. 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.

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

Windows ME

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 **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 95 and 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 95 and 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.



Note

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** pull-down menu in Internet Explorer.*

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**.

Login to Home Page

A new window will appear and you will be prompted for a user name and password to access the web-based manager.

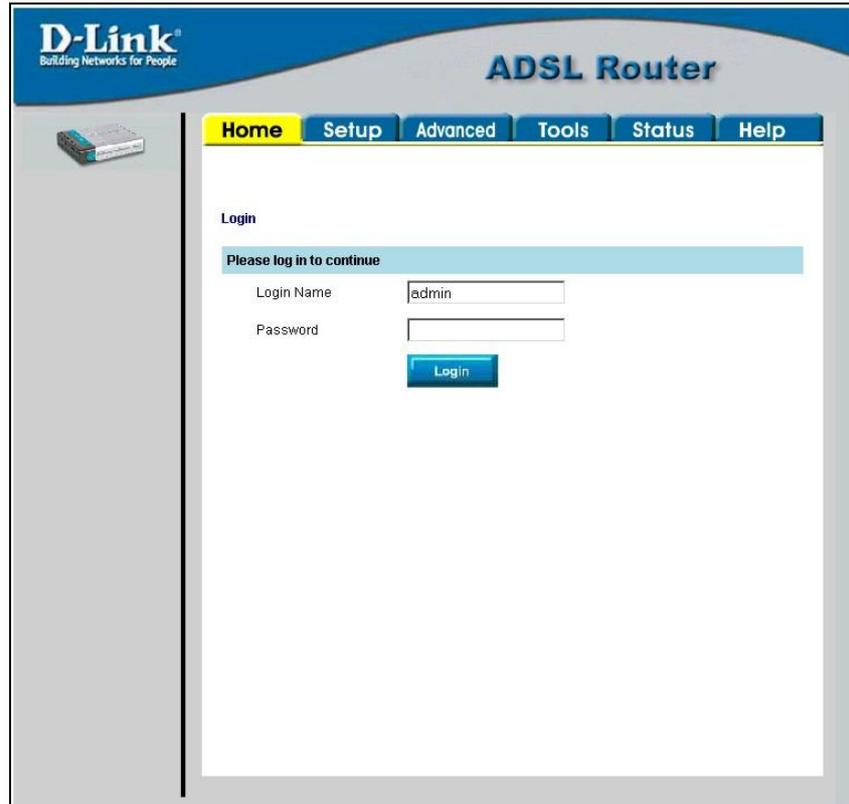
The screenshot shows the web-based management interface for a D-Link ADSL Router. At the top left is the D-Link logo with the tagline "Building Networks for People". To the right of the logo is the text "ADSL Router". Below the logo is a small image of the router. A navigation bar contains tabs for "Home", "Setup", "Advanced", "Tools", "Status", and "Help". The "Home" tab is selected. The main content area is titled "Login" and contains a light blue banner that says "Please log in to continue". Below the banner are two input fields: "Login Name" with the text "admin" entered, and "Password" which is empty. A blue "Login" button is positioned below the password field.

Figure 3-1. Home - Login window

Use the default user name **admin** and password **admin** for first time setup. 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 PC within the same subnet as the Modem to access the web-based manger.



Note

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 service provider's network.

Configure the Router

The first page that appears after you successfully login displays information about the Router and its connection status. Tabs across the top of the screen show other available menus: **Setup**, **Advanced**, **Tools**, **Status**, and **Help**.

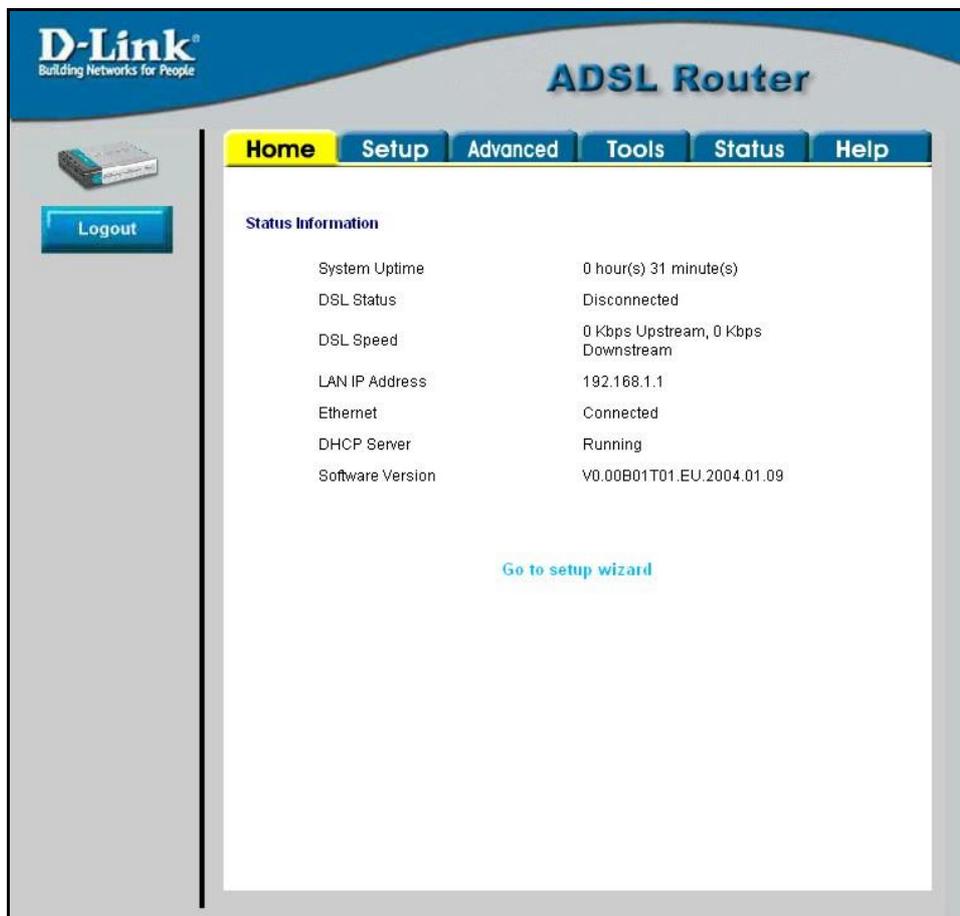


Figure 3-2. Home – Status Information window

When the Router is used to provide Internet access it actually must first access your service provider's network, that is, it must communicate with computers and other routers owned by your service provider. These computers and routers then provide access to the Internet. The Router must be configured to communicate with the systems that give it access to the larger network. Click either the **Setup** tab (or the **Go to setup wizard** hyperlink); the Setup window will appear.

Setup Menu

The **Setup** window offers links to menus to configure settings for the LAN (Local Area Network) and for the WAN (Wide Area Network) setup. The first menu you see when clicking the **Setup** tab or the **Go to setup wizard** hyperlink is the Setup menu.

Now you are ready to configure the settings needed for the WAN connection. All the information you need to make the changes needed for a functioning WAN connection should have been provided to you by your ISP or network service provider.

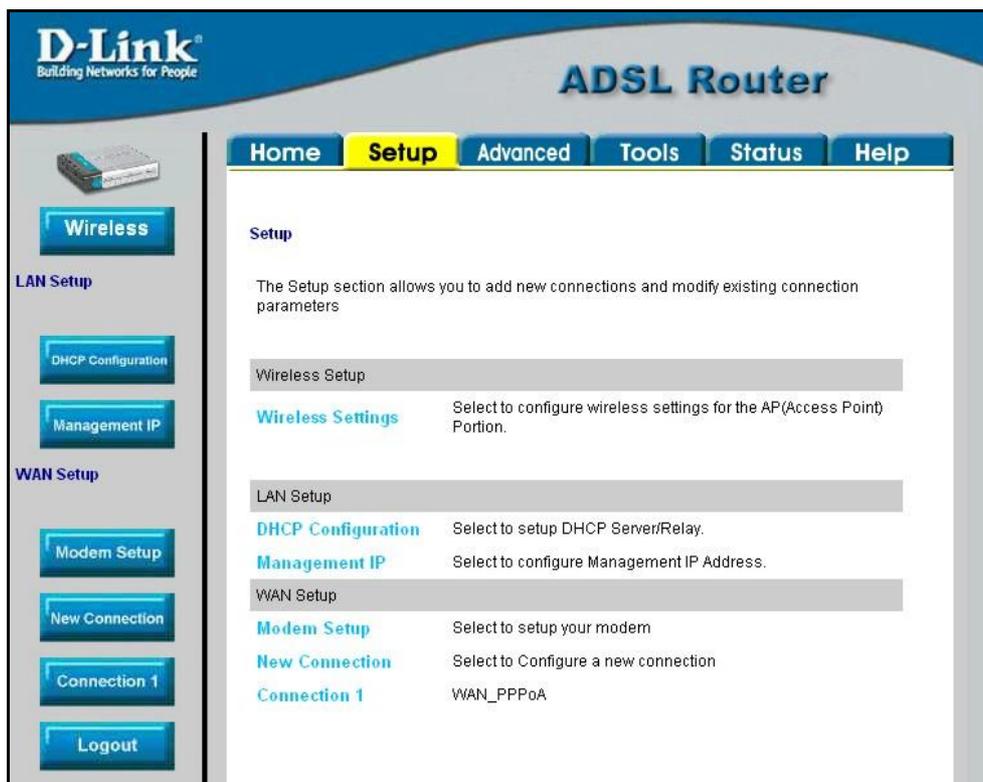


Figure 3-3. Opening Setup window

If you are not instructed to change the modulation type, click the **Wireless** button or hyperlink to configure the wireless settings. Skip ahead to Configure Connection below to configure a PPPoA connection type. Detailed instructions follow on how to configure other connection types.

If you are instructed to change the method of modulation used for ADSL, click the **Modem Setup** button or Modem Setup hyperlink and select the Modulation Type used for the connection. Skip ahead to the next page for an example of the Modem Setup menu. Then proceed to Configure Connection to configure a PPPoA connection or Change the Connection Type for other connection types.

Wireless Settings

Click the **Enable AP** box to allow the router to operate in the wireless environment.

SSID: The SSID identifies members of Service Set.

Accept the default name or change it to something else. *If the default SSID is changed, all other devices on the wireless network must use the same SSID.*

Channel: What channels are available for use by the access point depends on the local regulatory environment. Remember that all devices communicating with the device must use the same channel (and use the same SSID). Use the drop down menu to select the channel used for your 802.11g wireless LAN.

The wireless channel number is available from your Internet Service Provider (ISP).

If network Security is not used, click **None**, then click **Apply**.

Important Note: For initial configuration of the Router, make sure that **None** is selected. It is more important first to make sure that your wireless network is functioning properly.*

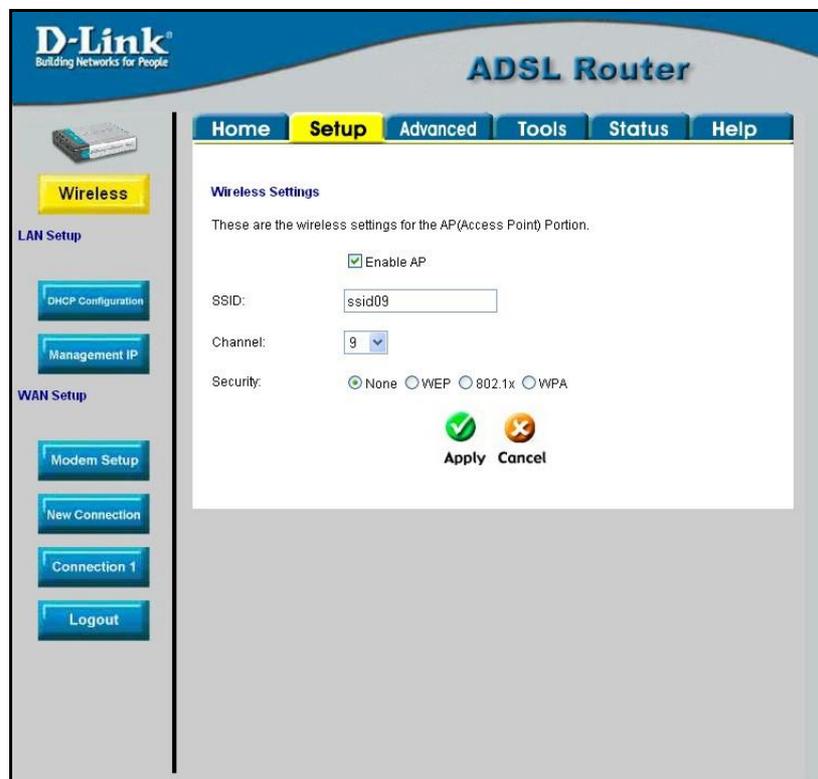


Figure 3-4. Wireless configuration window

* For information on applying various types of security to your network, see the next few pages.

Wireless Security

The DSL-G664T offers three types of network security: **WEP**, **802.1X**, and **WPA**.

WEP

WEP (Wireless Encryption Protocol) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys.

The router offers 64-, 128, or 256-bit encryption with four keys available.

To bring up the WEP configuration window, click the **WEP** radio button.

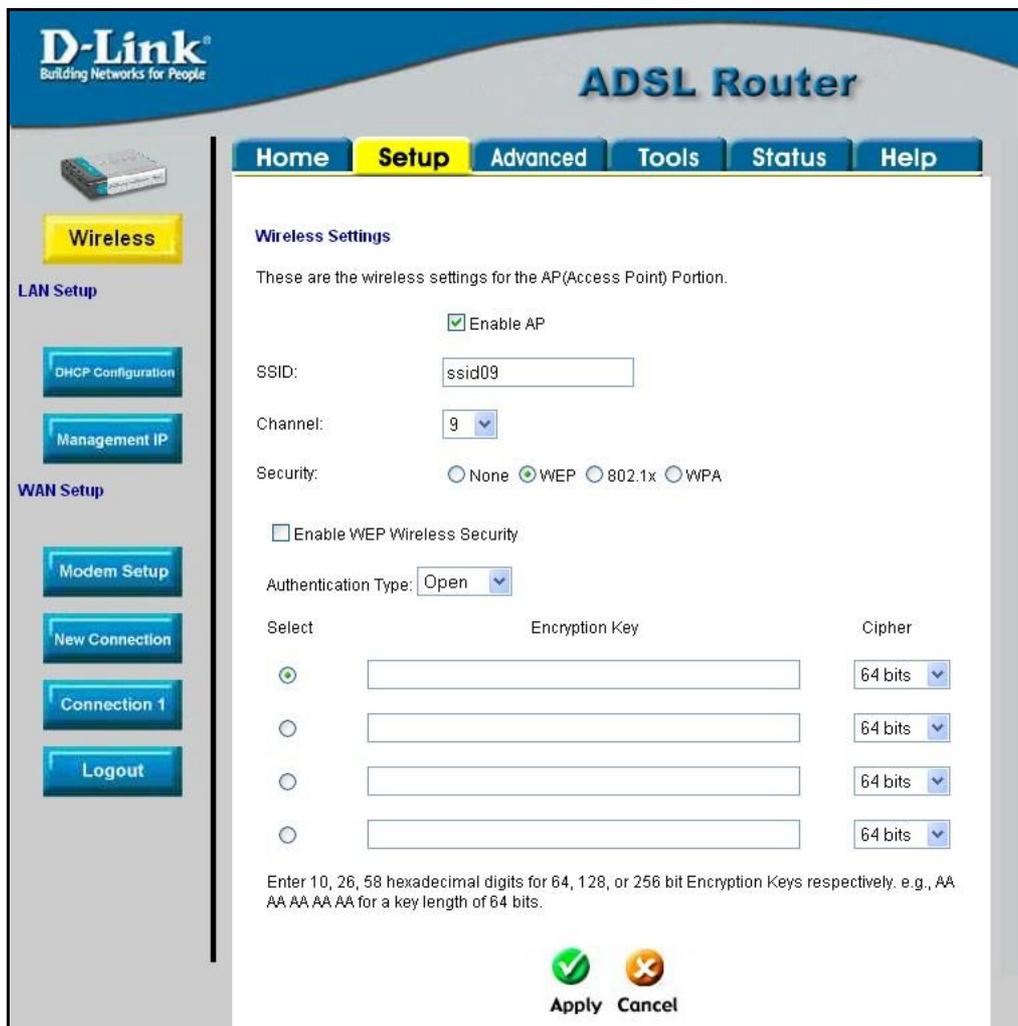


Figure 3-5. WEP configuration window

From the drop-down menu, select an Authentication Type: **Open**, **Shared**, or **Both**.

Select a key by clicking a radio button on the left, select an encryption level from the drop-down menu on the right, then enter the proper-length key. (Key length is outlined at the bottom of the window.)

Click **Apply**.

Important Note: If encryption of any kind, at any level is applied to the Router, all devices on the network must comply with all security measures.

802.1X

Some network-security experts now recommend that wireless networks use 802.1X security measures to overcome some weaknesses in standard WEP applications. A RADIUS server is used to authenticate all potential users.

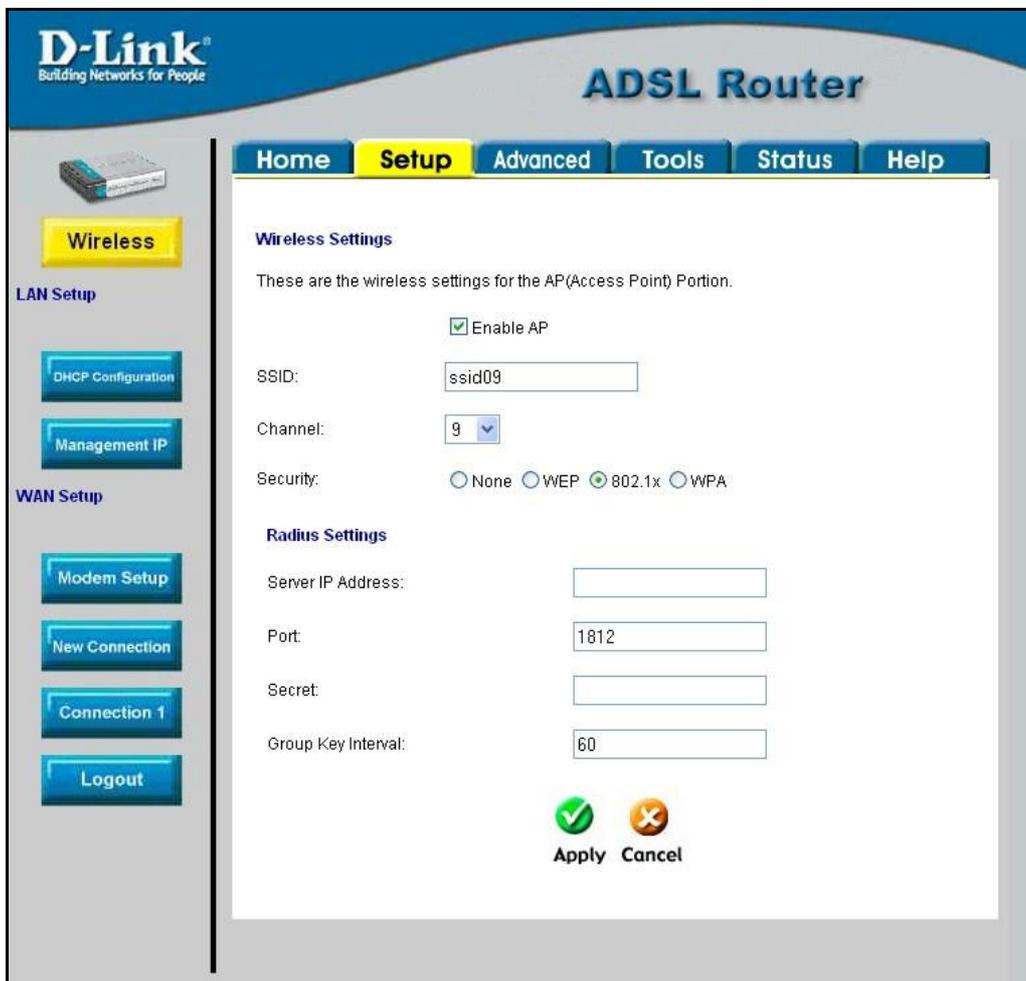
Server IP Address: enter the IP address of the Radius server

Port: enter a port number, or accept the default

Secret: enter a password (1-63 character)

Group Key Interval: time (in seconds) after which the Group Key is changed automatically (1-99999).

Important Note: The values needed for the above entries can be obtained from your Internet Service Provider (ISP).



The screenshot shows the D-Link ADSL Router configuration interface. The top navigation bar includes 'Home', 'Setup' (highlighted), 'Advanced', 'Tools', 'Status', and 'Help'. The left sidebar contains navigation options: 'Wireless', 'LAN Setup' (with 'DHCP Configuration' and 'Management IP'), and 'WAN Setup' (with 'Modem Setup', 'New Connection', 'Connection 1', and 'Logout'). The main content area is titled 'Wireless Settings' and includes a sub-section for 'Radius Settings'. The 'Wireless Settings' section has a checked 'Enable AP' box, an SSID field with 'ssid09', a Channel dropdown set to '9', and Security options with '802.1x' selected. The 'Radius Settings' section includes fields for 'Server IP Address', 'Port' (1812), 'Secret', and 'Group Key Interval' (60). At the bottom of the settings area are 'Apply' and 'Cancel' buttons.

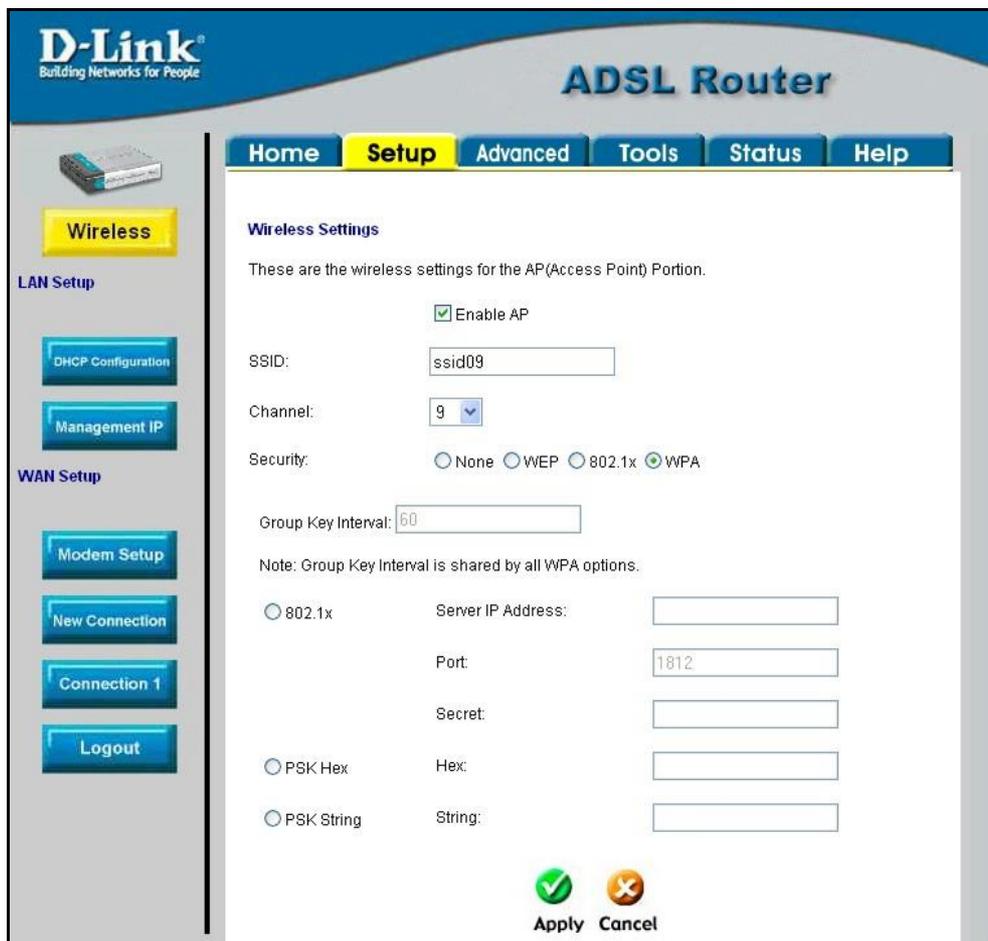
Figure 3-6. 802.1X configuration window

Important Note: If encryption of any kind, at any level is applied to the Router, all devices on the network must comply with all security measures.

WPA (Wi-Fi Protected Access)

Wi-Fi Protected Access was designed to provide improved data encryption, perceived as weak in WEP, and to provide user authentication, largely nonexistent in WEP.

For most small networks, such as in a small business or home-based enterprise, WPA is the easiest way to obtain effective network security. Of the three options in WPA, **PSK String** is the easiest to implement.



The screenshot shows the D-Link ADSL Router configuration interface. The top navigation bar includes 'Home', 'Setup' (highlighted), 'Advanced', 'Tools', 'Status', and 'Help'. The left sidebar contains 'Wireless' (highlighted), 'LAN Setup' (with 'DHCP Configuration' and 'Management IP' buttons), and 'WAN Setup' (with 'Modem Setup', 'New Connection', 'Connection 1', and 'Logout' buttons). The main content area is titled 'Wireless Settings' and contains the following fields and options:

- Enable AP
- SSID:
- Channel:
- Security: None WEP 802.1x WPA
- Group Key Interval:
- Note: Group Key Interval is shared by all WPA options.
- 802.1x
 - Server IP Address:
 - Port:
 - Secret:
- PSK Hex
 - Hex:
- PSK String
 - String:

At the bottom of the window are 'Apply' and 'Cancel' buttons with green and orange icons respectively.

Figure 3-7. WPA configuration window

Group Key Interval: time (in seconds) after which the Group Key is changed automatically (1-99999).

802.1X

IP address of the RADIUS server, **Port** number, and **Secret** (password) can be obtained from your Internet Service Provider (ISP).

PSK HEX

PSK (Pre-Shared Key) Hex is a hexadecimal value 1-32 characters in length.

PSK String

PSK (Pre-Shared Key) is an alphanumeric value 1-63 characters in length.

Enter the appropriate values, then click **Apply**.

Important Note: If encryption of any kind, at any level is applied to the Router, all devices on the network must comply with all security measures.

Modem Setup

The Modem Setup menu is used to change the Modulation Type used for the ADSL connection. This setting should only be changed if your service provider has given explicit instructions to change it.



Do not change the (ADSL) Modulation type used unless you have been instructed to do so. If this setting is not configured properly, the Router will not work.

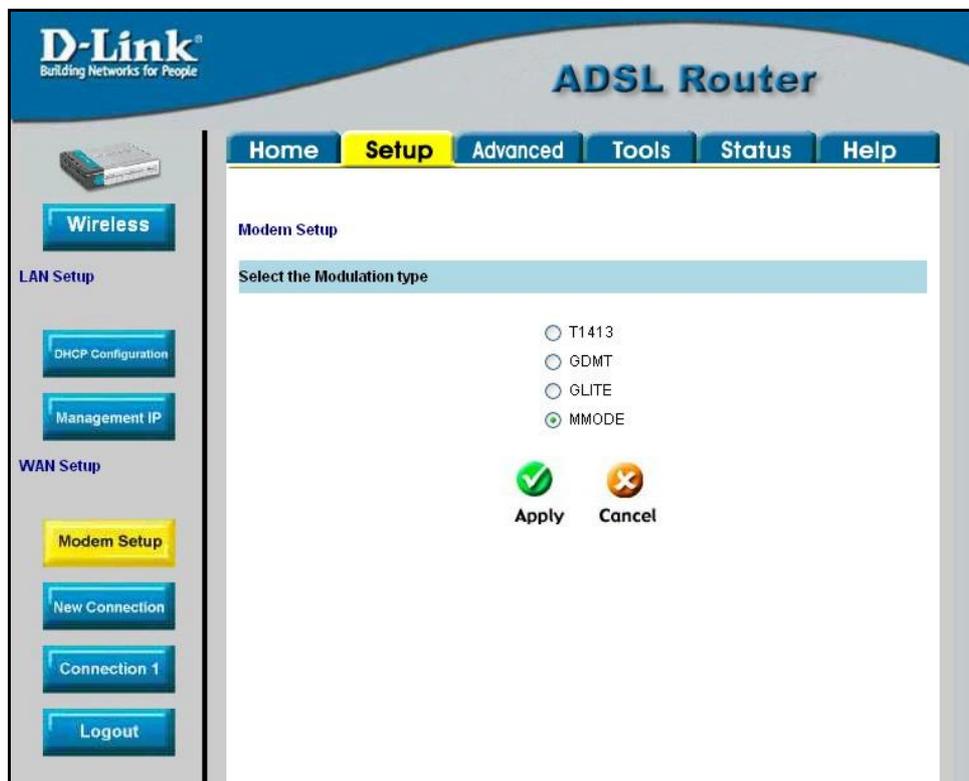


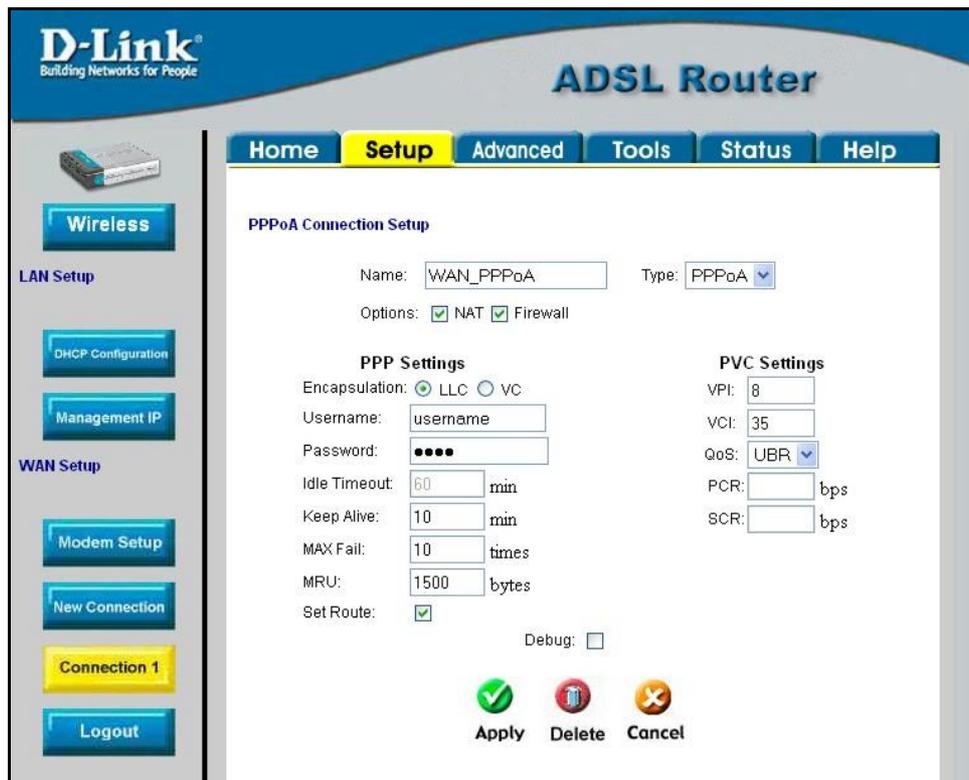
Figure 3-8. Modem Setup menu (change modulation type)

If you are instructed by your ISP to change the Modulation type is used for your service, select the desired modulation type and then click **Apply**. The modulation types available are **T1413**, **G.DMT**, **GLITE** and **MMODE**. By default, the Router will automatically detect the modulation used; this setting is listed as MMODE (Multi-mode).

Configure Connection 1 for PPPoA

PPP or Point-to-Point protocol is a standard method of establishing a network connection/session between networked devices. Different forms of PPP include PPPoA and PPPoE (discussed below) involve an authentication process that requires a username and password to gain access to the network. PPPoA (PPP over ATM) as described in RFC 2364, is a method of using PPP on an ATM network. ATM is used for many types of telecommunications services including ADSL.

To configure the WAN connection for PPPoA, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.



The screenshot displays the D-Link ADSL Router web interface. The top navigation bar includes 'Home', 'Setup' (highlighted), 'Advanced', 'Tools', 'Status', and 'Help'. The left sidebar contains 'Wireless', 'LAN Setup' (with 'DHCP Configuration' and 'Management IP' buttons), and 'WAN Setup' (with 'Modem Setup', 'New Connection', 'Connection 1' (highlighted), and 'Logout' buttons). The main content area is titled 'PPPoA Connection Setup'. It features a 'Name' field with 'WAN_PPPoA' and a 'Type' dropdown set to 'PPPoA'. Below are 'Options' for 'NAT' and 'Firewall', both checked. The 'PPP Settings' section includes 'Encapsulation' (LLC selected), 'Username' (username), 'Password' (masked), 'Idle Timeout' (60 min), 'Keep Alive' (10 min), 'MAX Fail' (10 times), 'MRU' (1500 bytes), and 'Set Route' (checked). The 'PVC Settings' section includes 'VPI' (8), 'VCI' (35), 'QoS' (UBR), 'PCR' (empty), and 'SCR' (empty). At the bottom are 'Apply', 'Delete', and 'Cancel' buttons, along with a 'Debug' checkbox.

Figure 3- 9. PPPoA Connection 1 Setup menu

To configure the default connection type (PPPoA) for Connection 1, follow the steps listed below. To change the connection type of Connection 1 to an alternative type follow the instructions according to the desired type as described below in Change the Connection Type.

1. Click the **Connection 1** button under **WAN Setup** to view the **PPPoA Connection Setup** menu pictured in the example above.
2. Type in a **Name** for the connection or use the default name *WAN_PPPoA* in the space provided.
3. Under **Options**, enable **NAT** and/or **Firewall** by selecting the corresponding selection box.
4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
7. Type the **Username** and **Password** used to verify the identity of your account. Typically, the Username is an account number assigned by your ISP and appears in the form *account#@serviceprovider.com*, while the Password may have been chosen by the account holder. For most users, the remaining settings will not need to be changed. See your ISP for further information.

8. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the Router.
9. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
10. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

Change the Connection Type

The default connection protocol used for the Router is Point-to-Point Protocol over ATM (PPPoA). The menu used to configure a PPPoA connection is the first menu to appear when you click on the **Connection 1** button in the Setup menu. The alternative connection types supported by the Router are the **PPPoE** (PPP over Ethernet), **CLIP** (Classical IP over ATM or IPoA), **DHCP** (for WAN), **Static** (IP for WAN), and **Bridge** connection types. There are two ways you may configure the WAN connection to use these alternative types. You can create a **New Connection** using the alternative connection type or you may configure the Connection 1 settings to use the connection type of choice. This section describes how to change the Connection 1 settings to use a different connection type. To change the Connection 1 settings to use a different connection type, follow the instructions below according to the type of connection you want to use. To create and configure a New Connection, skip ahead to Create a New Connection.

Configure Connection 1 for PPPoE

PPP or Point-to-Point protocol is a standard method of establishing a network connection/session between networked devices. PPPoE configuration requires the same basic information as the previously discussed PPPoA and both menus are nearly identical. It may be worthwhile for the user to change the default name of Connection 1 to something that states what connection type is being used, for example, *WAN_PPPoA*, the name used in the example below. Notice the VPI and VCI values are included in the name. It is not functionally necessary to change the name of the connection; this is done merely to provide descriptive reference.

The screenshot shows the D-Link ADSL Router web interface. The main navigation tabs are Home, Setup, Advanced, Tools, Status, and Help. The 'Setup' tab is active, and the 'PPPoE Connection Setup' page is displayed. The page contains the following fields and options:

- Name:** WAN_PPPoA
- Type:** PPPoE
- Options:** NAT Firewall
- PPP Settings:**
 - Username:** username
 - Password:** [masked]
 - Idle Timeout:** 60 min
 - Keep Alive:** 10 min
 - MAX Fail:** 10 times
 - MRU:** 1492 bytes
 - Set Route:**
 - Enforce MRU:** **Debug:**
- PVC Settings:**
 - VPI:** 8
 - VCI:** 35
 - QoS:** UBR
 - PCR:** [empty] bps
 - SCR:** [empty] bps

At the bottom of the page, there are three buttons: **Apply** (with a green checkmark icon), **Delete** (with a red trash can icon), and **Cancel** (with an orange X icon).

Figure 3-10. Setup – Configure Connection 1 for PPPoE

To configure Connection 1 for PPPoE, follow the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *PPPoE* from the **Type:** pull-down menu. The menu will blink momentarily
3. Type in a **Name:** for the connection or use the default name in the space provided (*WAN_PPPoA* used in the above example).
4. Under **Options**, enable **NAT** and/or **Firewall** by selecting the corresponding selection box.
5. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
6. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
7. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
8. Type the **Username** and **Password** used to verify the identity of your account. Typically, the Username is an account number assigned by your ISP and appears in the form *account#@serviceprovider.com*, while the Password may have been chosen by the account holder. For most users, the remaining settings will not need to be changed. See your ISP for further information.
9. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the Router.
10. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
11. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

Configure Connection 1 for Bridge

“Bridge” means a pure bridged connection with no IP address assigned to the Router. This connection method makes the Router act as a bridge, and just passes packets across the DSL port. When the device is used in this manner, it is necessary to install additional connection software on any computer or server used to access the Internet.

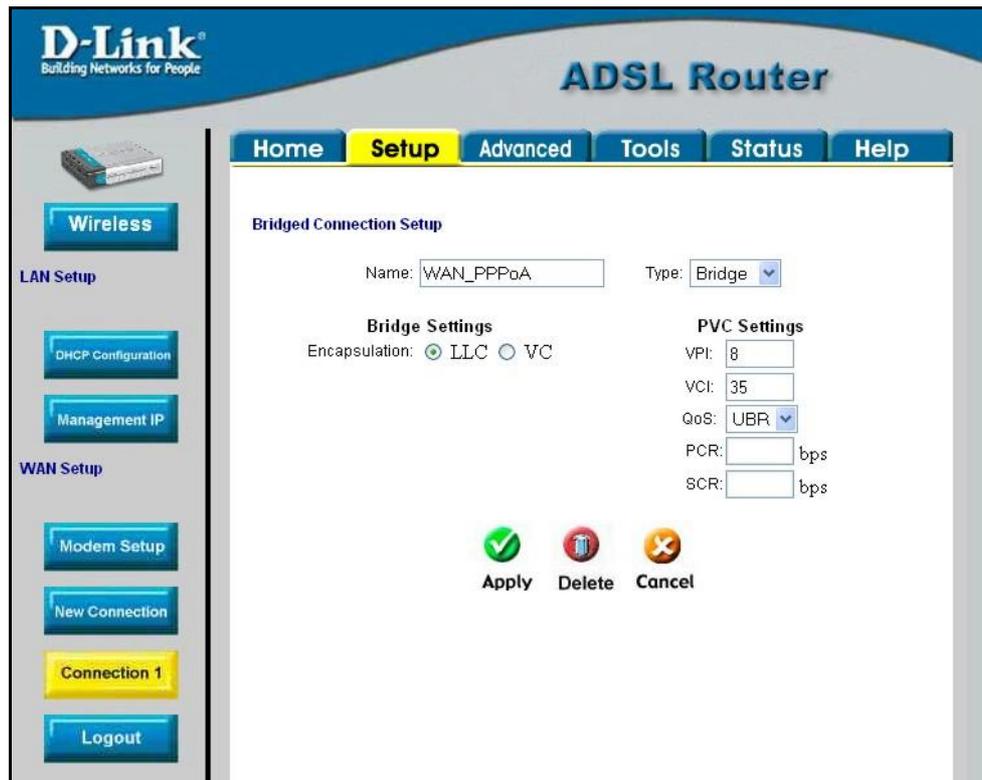


Figure 3-11. Setup – Configure Connection 1 for Bridge

To configure the WAN connection for Bridge, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *Bridge* from the **Type:** pull-down menu. This action will change the menu so it offers fewer settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPOA* is used in the above example).
4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
7. The **Encapsulation** values LLC (SNAP) and VC (MUX) are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.
8. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the Router.

9. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
10. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read “N/A”. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

Configure Connection 1 for Static IP for WAN

Static is used whenever a known static IP is assigned. The accompanying information such as the Subnet mask and the gateway should also be specified in order to be able to connect. Up to three Domain Name Server (DNS) addresses can also be specified. These are the servers would enable you to have access to other web servers. Valid IP addresses range from 1.0.0.1 to 223.255.255.254.

The screenshot shows the D-Link ADSL Router web interface. The main navigation tabs are Home, Setup, Advanced, Tools, Status, and Help. The 'Setup' tab is active. On the left sidebar, there are sections for Wireless, LAN Setup (with buttons for DHCP Configuration and Management IP), and WAN Setup (with buttons for Modem Setup, New Connection, Connection 1, and Logout). The 'Connection 1' button is highlighted in yellow. The main content area is titled 'Static Connection Setup' and contains the following fields and options:

- Name:** WAN_PPPOA
- Type:** Static (dropdown menu)
- Options:** NAT Firewall
- Static Settings:**
 - Encapsulation:** LLC VC
 - IP Address:** 0.0.0.0
 - Mask:** (empty field)
 - Default Gateway:** (empty field)
 - DNS 1:** (empty field)
 - DNS 2:** (empty field)
 - DNS 3:** (empty field)
 - Mode:** Bridged Routed
- PVC Settings:**
 - VPI:** 8
 - VCI:** 35
 - QoS:** UBR (dropdown menu)
 - PCR:** (empty field) bps
 - SCR:** (empty field) bps

At the bottom of the form, there are three buttons: Apply (with a green checkmark icon), Delete (with a red trash can icon), and Cancel (with a red X icon).

Figure 3-12. Setup – Configure Connection 1 for Static IP for the WAN

To configure the WAN connection for Static, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select *Static* from the **Type:** pull-down menu. This action will change the menu so it offers different settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPOA* is used in the above example).
4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.

7. The **Encapsulation** values LLC (SNAP) and VC (MUX) are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.
8. Based on the information provided by your ISP, enter the **IP Address**, **Subnet Mask**, **Default Gateway** (if provided), and **Domain Name Services (DNS)** values (if provided).
9. Select the desired **Mode**, **Bridged** or **Routed**.
10. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the Router.
11. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
12. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read "N/A". If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

Configure Connection 1 for DHCP for WAN

Dynamic Host Configuration Protocol (DHCP) allows the gateway to automatically obtain the IP address from a DHCP server on the service provider's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the Router requests an IP address.

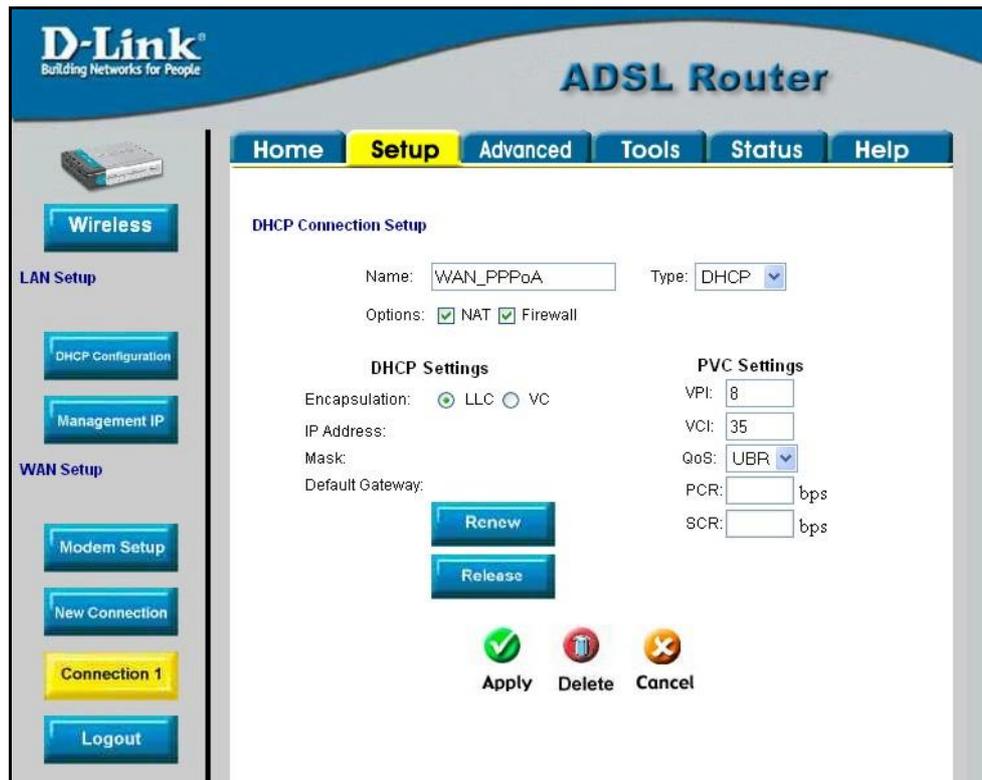


Figure 3-13. Setup – Configure Connection 1 for DHCP service for the WAN

To configure the WAN connection for DHCP, perform the steps listed below. Some of the settings do not need to be changed the first time the device is set up, but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select **DHCP** from the **Type:** pull-down menu. This action will change the menu so it offers different settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPoA* is used in the above example).
4. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
5. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
6. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.
7. The **Encapsulation** values LLC (SNAP) and VC (MUX) are two different methods of encapsulating the PPP packet. Contact your ISP to make sure which encapsulation is being supported.
8. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the Router.
9. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.

10. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read *Connected*. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

Configure Connection 1 for CLIP

CLIP or IPoA connections function in a similar way to DHCP or Static IP connections. Certain CLIP connections function like P2P networks. The router must obtain IP settings from a server owned by an ISP, or use a static IP address assigned by the ISP.

The screenshot shows the D-Link ADSL Router web interface. The top navigation bar includes 'Home', 'Setup', 'Advanced', 'Tools', 'Status', and 'Help'. The 'Setup' tab is active. On the left sidebar, there are sections for 'Wireless', 'LAN Setup', and 'WAN Setup'. Under 'WAN Setup', the 'Connection 1' button is highlighted. The main content area is titled 'CLIP Connection Setup'. It contains the following fields and options:

- Name:** WAN_PPPoA
- Type:** CLIP (dropdown menu)
- Options:** NAT, Firewall
- CLIP Settings:**
 - IP Address:** 0.0.0.0
 - Mask:** (empty field)
 - ARP Server:** 0.0.0.0
 - Default Gateway:** (empty field)
- PVC Settings:**
 - VPI:** 8
 - VCI:** 35
 - QoS:** UBR (dropdown menu)
 - PCR:** (empty field) bps
 - SCR:** (empty field) bps

At the bottom of the form are three buttons: 'Apply' (green checkmark), 'Delete' (red trash can), and 'Cancel' (orange X).

Figure 3-14. Setup – Configure Connection 1 for CLIP (IPoA)

To configure the WAN connection for CLIP, perform the steps listed below. Some of the settings do not need to be changed when you first set up the device but can be changed later if you choose.

1. Click the **Connection 1** button under **WAN Setup** to view the default **PPPoA Connection Setup** configuration menu.
2. Select **CLIP** from the **Type:** pull-down menu. This action will change the menu so it offers different settings for configuration.
3. Type in a **Name:** in the space provided (*WAN_PPPoA* is used in the above example).
4. Under **Options**, enable **NAT** and/or **Firewall** by selecting the appropriate checkbox. This option is not available for a Bridge connection.
5. Based upon the information your ISP provided, enter the **IP Address** (e.g. 168.128.1.1), the Subnet **Mask** (e.g. 255.255.255.0), **ARP Server** (e.g. 168.128.1.2) and the **Default Gateway** (e.g. 168.128.1.1).
6. If you are told to change the **VPI** or **VCI** values, type in the values given to you by your service provider. Many users will be able to use the default settings.
7. Leave the default **QoS** values if you are unsure or the ISP did not provide this information.
8. Do not change the **PCR** or **SCR** values unless you are required to do so. If you are told to change these, type in the values given to you by your service provider.

9. Click the **Apply** button when you have entered all the information. The web browser will briefly go blank. You are now finished changing setting for the primary WAN connection known as Connection 1. It is now necessary to save the changes you just made and restart the Router.
10. To save the changes made to Connection 1, click the **Tools** tab and then click on the **System Commands** button. Click on the **Save All** button to store the configuration settings. Click on **Back** button to return to the System Commands menu.
11. Check the WAN connection status. Click the **Status** tab and then the **Connection Status** button. Look under **WAN** to view the **State** of Connection 1, it should read “N/A”. If the WAN connection state does not appear to *Connected* after a few minutes, go back to the Connection 1 Setup menu, check the settings and make sure they are correct.

Create a New Connection

An alternative method of changing the connection type used by the Router is to create a new connection. Creating a new connection will not change the Connection 1 settings, it will make a new set of connection configuration settings. The new set created will be labeled **Connection 2**, additional connections created will be likewise labeled Connection 3, Connection 4 and so on. Use the method described here to create up to 8 different connection configuration sets. At any time you may reconfigure the settings for any previously created connection by clicking on the menu button for the connection displayed under the **WAN Setup** heading.

New Connection Example 1 - Create a New PPPoE Connection

The example below describes how to set up a new connection that uses a PPPoE type WAN connection. To create a new connection:

1. Click on the **New Connection** button.
2. Configure the Router for the **Type** of connection used and all the remaining settings as discussed in the preceding section. In this example, the type of connection used for **Connection 2** is *PPPoE*. Notice also that the VPI and VCI values have been changed.
3. Click the **Apply** button to create the new connection. Notice that a new menu button is created (Connection 2), this links to the configuration menu for Connection 2 (see example below). If at any time you want to change, delete, disconnect or connect this WAN connection, click on the Connection 2 button.
4. Save the new connection.

The screenshot shows the D-Link ADSL Router web interface. The main navigation tabs are Home, Setup (highlighted), Advanced, Tools, Status, and Help. On the left sidebar, there are buttons for Wireless, LAN Setup (DHCP Configuration, Management IP), and WAN Setup (Modem Setup, New Connection, Connection 1, Logout). The main content area is titled "PPPoE Connection Setup". It contains the following fields and options:

- Name:** [text input field]
- Type:** [dropdown menu showing PPPoE]
- Options:** NAT Firewall
- PPP Settings:**
 - Username:** [text input field with value "username"]
 - Password:** [password input field with masked characters "••••"]
 - Idle Timeout:** [text input field with value "60"] min
 - Keep Alive:** [text input field with value "10"] min
 - MAX Fail:** [text input field with value "10"] times
 - MRU:** [text input field with value "1492"] bytes
 - Set Route:**
 - Enforce MRU:** **Debug:**
- PVC Settings:**
 - VPI:** [text input field with value "0"]
 - VCI:** [text input field with value "0"]
 - QoS:** [dropdown menu showing UBR]
 - PCR:** [text input field] bps
 - SCR:** [text input field] bps

At the bottom of the form, there are three buttons: **Apply** (with a green checkmark icon), **Delete** (with a red trash can icon), and **Cancel** (with an orange X icon).

Figure 3- 15. Set up a New Connection – Connection 2

New Connection Example 2 - Create a New Bridge Connection

You may create new connections to suit different purposes. For example, let's create a new Bridge connection used to connect directly to a server acting as a firewall and proxy.

1. Click the **New Connection** button.
2. Select *Bridge* from the **Type:** menu.
3. Configure the remaining settings (including **VPI:** and **VCI:**) as necessary.
4. Click the **Apply** button. Notice that a new menu button, Connection 3, appears under WAN Setup.
5. Remember to save any newly created connections using the **Save All** procedure in the **Tools/System Commands** menu.

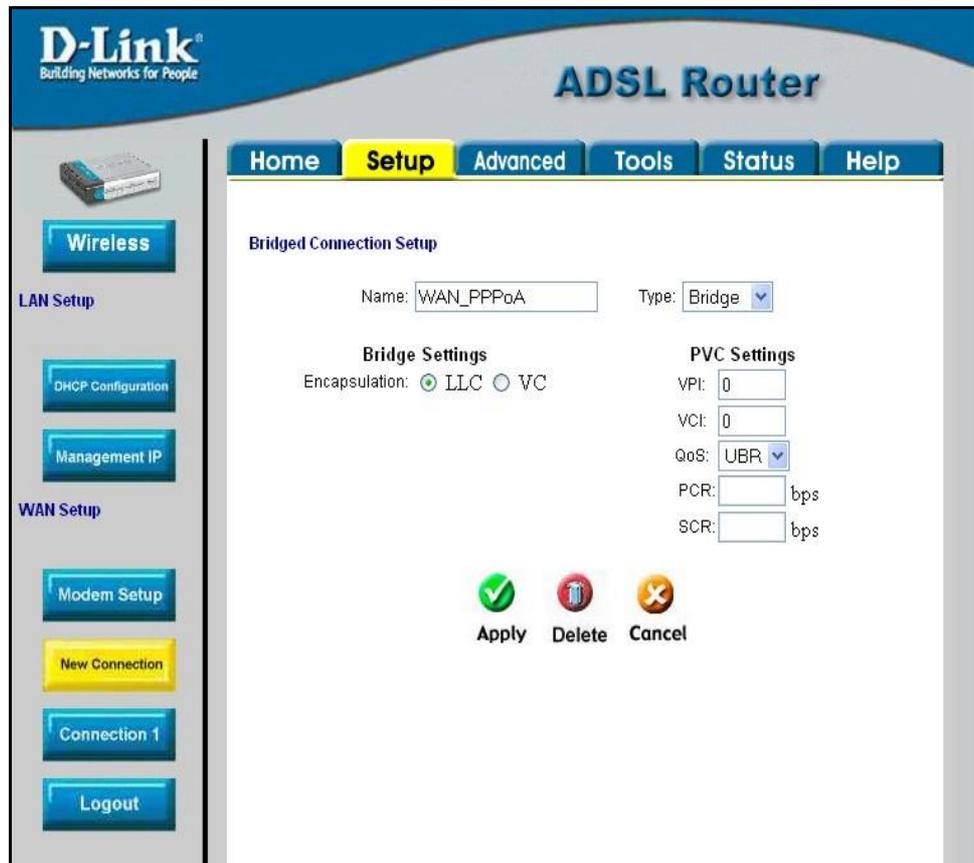


Figure 3- 16. Set up a New Connection – Connection 3

To delete the Bridge connection, click the **Delete** button.

DHCP Configuration for LAN

The Router supports three DHCP modes for the LAN. By default, DHCP service is provided using an IP pool of 192.168.1.2 – 192.168.1.254 for a total of 253 IP addresses available. The Router can also relay DHCP service from another server through the WAN port. You may prefer to disable DHCP service and DHCP relay and use a different preferred method for IP addressing on your LAN.

To disable the embedded DHCP server, select the **Server and Relay Off** option and click the **Apply** button.

The screenshot shows the DHCP Configuration page of a D-Link ADSL Router. The page title is "ADSL Router" and the navigation tabs are "Home", "Setup", "Advanced", "Tools", "Status", and "Help". The "Setup" tab is selected. The page content is titled "DHCP Configuration" and includes the text: "The device can be setup as a DHCP Server to distribute IP addresses to the LAN network." There are three radio button options: "Server On" (selected), "Relay On", and "Server and Relay Off". The "Server On" option has input fields for "Start IP" (192.168.1.2), "End IP" (192.168.1.254), and "Lease Time" (3600 Seconds). The "Relay On" option has a "Relay IP" field (0.0.0.0). At the bottom, there are "Apply" and "Cancel" buttons.

Figure 3- 17. Configure DHCP service for the LAN

For DHCP service on the LAN, select the **Server On** option to enable DHCP service from the Router (enabled by default) and configure DHCP server parameters as follows:

DHCP Parameter	Description
Start IP	Type in the base address for the IP pool of unassigned IP addresses. This IP address must be consistent with the Management IP address of the Router. Normally the Start IP address is one greater than the Management IP address.
End IP	Type in the last address of the contiguous IP address range to be used by the Router for DHCP function. Up to 253 consecutive IP addresses may be used for the pool.
Lease Time	This specifies the amount of time (in seconds) a client can lease an IP address, from the dynamically allocated IP pool.

Click the **Apply** button to make the changes to the DHCP settings. Remember to **Save All** in the **Tools/System Commands** menu.

Enable DHCP Relay

Some service providers provide DHCP service for private networks from their own servers. To enable DHCP service from outside your LAN select the **DHCP Relay** option and type in the server IP address in the **Relay IP** field.

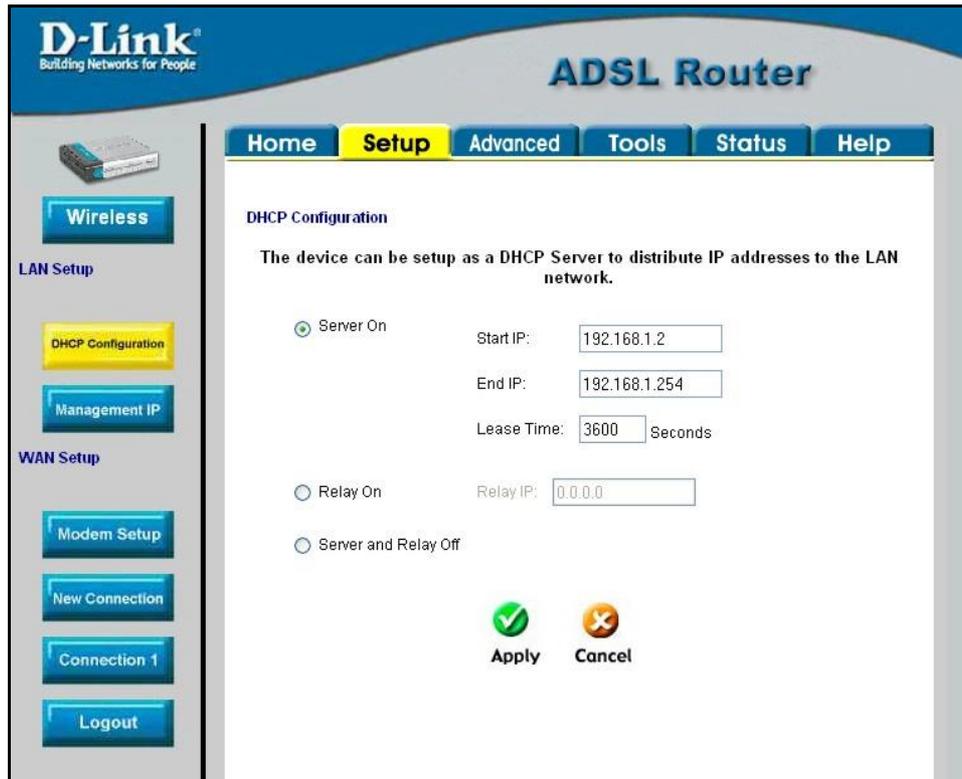
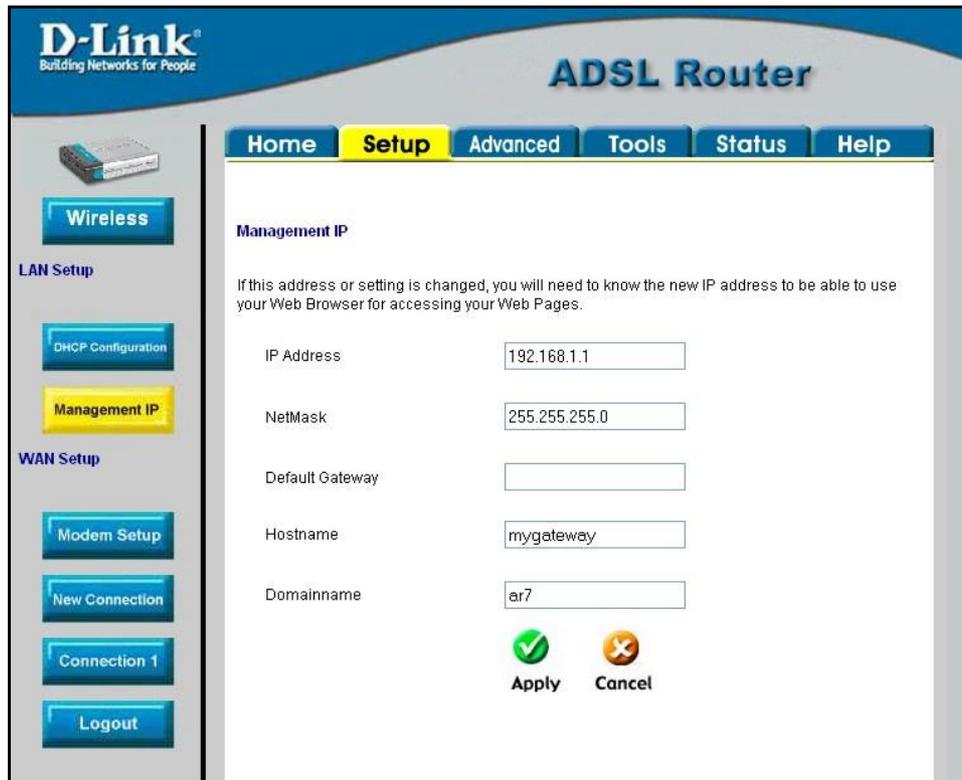


Figure 3- 18. Configure DHCP Relay Service

Click the **Apply** button to change the DHCP Relay settings. Remember to **Save All** in the **Tools/System Commands** menu.

Management IP

The IP address of the Router can be changed to suit the requirements of your LAN. Remember, if you are using DHCP from the Router, the IP address must be consistent with the DHCP IP settings.



The screenshot shows the D-Link ADSL Router web interface. The top navigation bar includes 'Home', 'Setup' (highlighted), 'Advanced', 'Tools', 'Status', and 'Help'. The left sidebar contains 'Wireless', 'LAN Setup' (with 'DHCP Configuration' and 'Management IP' buttons), and 'WAN Setup' (with 'Modem Setup', 'New Connection', 'Connection 1', and 'Logout' buttons). The main content area is titled 'Management IP' and includes a warning: 'If this address or setting is changed, you will need to know the new IP address to be able to use your Web Browser for accessing your Web Pages.' Below this are input fields for 'IP Address' (192.168.1.1), 'NetMask' (255.255.255.0), 'Default Gateway', 'Hostname' (mygateway), and 'Domainname' (ar7). At the bottom are 'Apply' and 'Cancel' buttons.

Figure 3- 19. Configure Management IP

Change IP settings as desired and click the **Apply** button to change the DHCP Relay settings. You may also provide a Host name and Domain name if necessary for your LAN. Remember to **Save All** in the **Tools/System Commands** menu.

Save Configuration Changes

Any changes made to the Router's configuration must be saved to non-volatile memory or they will be lost if the Router is restarted or powered off. When you are finished making changes to the Router settings, follow the instructions here to save the new settings.

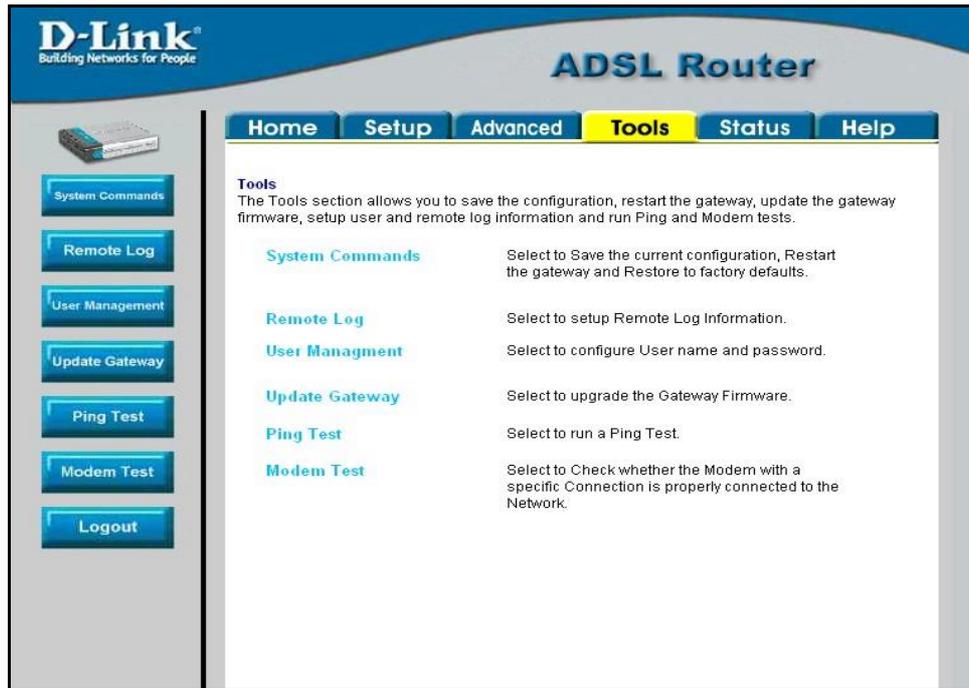


Figure 3- 20. Router Tools Menus

Click on the **Tools** tab to access the **System Commands** menu link - then click the System Commands link to see the menu pictured below.

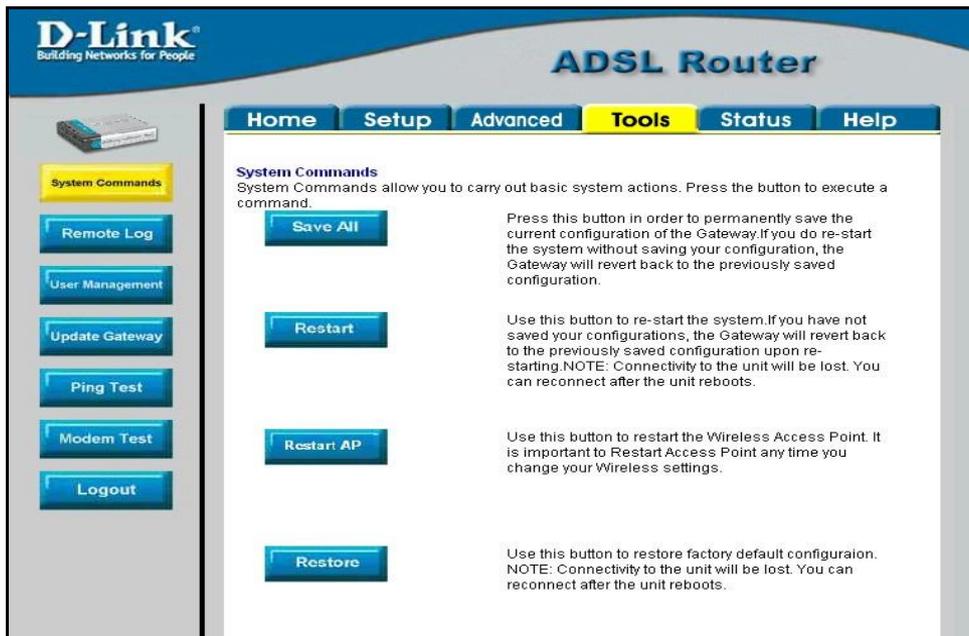


Figure 3- 21. Available System Commands

To save the new settings, click on the **Save All** button. It will take a second or two to perform the save. After the save is completed, a message appears in a new menu (see below).

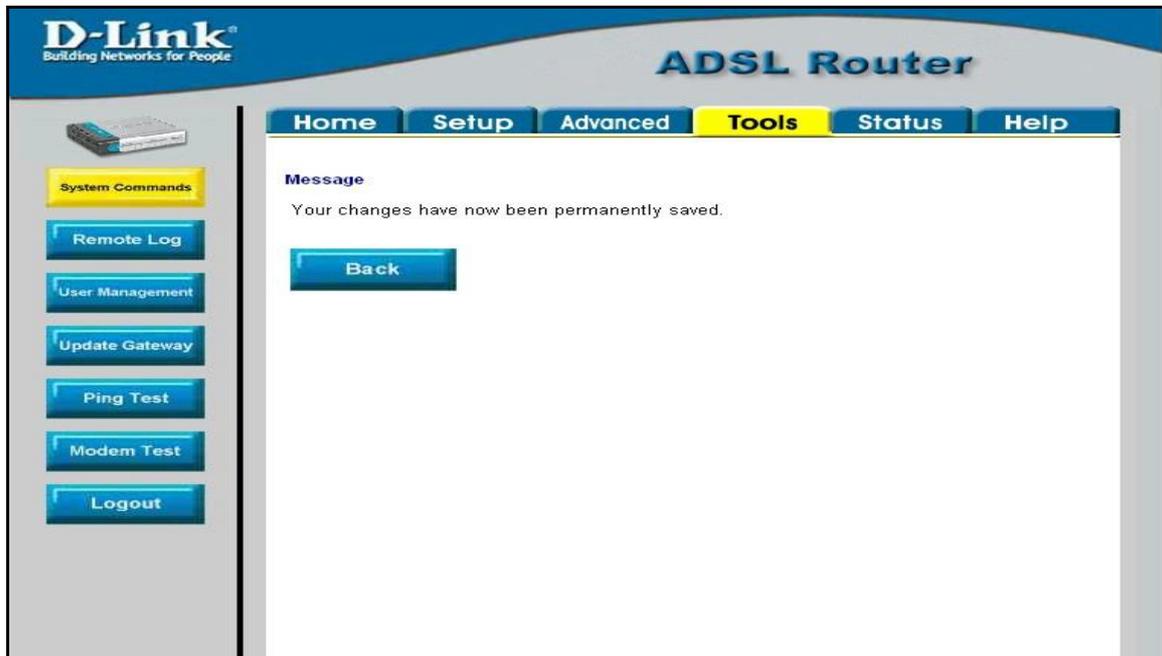


Figure 3-22. Changes permanently saved message

To return to the System Commands menu you can click the **Back** button in the new menu or use the back function of the web browser.

Advanced Router Management

Click the **Advanced** tab to access menus used to configure **UPnP**, **Port Forwarding**, **Access Control**, **Advanced Security** (including NAT, Firewall and DMZ setup), **LAN Clients**, **Bridge Filters**, **Multicast** pass-through, **Static Routing** and **Dynamic Routing** (RIP setup) and **Wireless Management** and **Wireless Performance**.

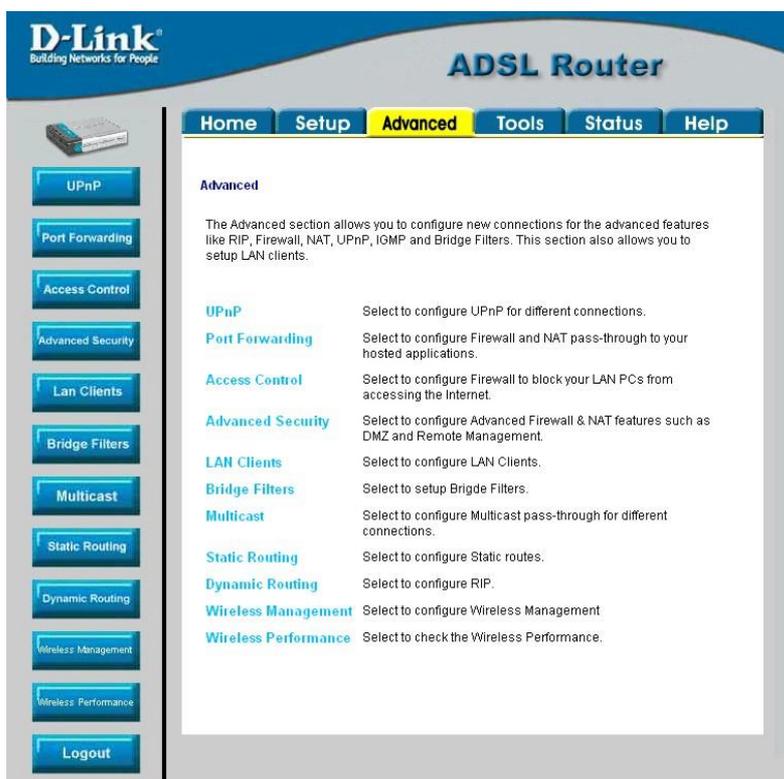


Figure 4-1. Advanced setup main menu

UPnP

UPnP supports zero-configuration networking and automatic discovery for many types of networked devices. When enabled, it allows other devices that support UPnP to dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices. DHCP and DNS service can also be used if available on the network. UPnP also allows supported devices to leave a network automatically without adverse effects to the device or other devices on the network.

UPnP can be supported by diverse networking media including Ethernet, 802.11g wireless, Firewire, phoneline and powerline networking.

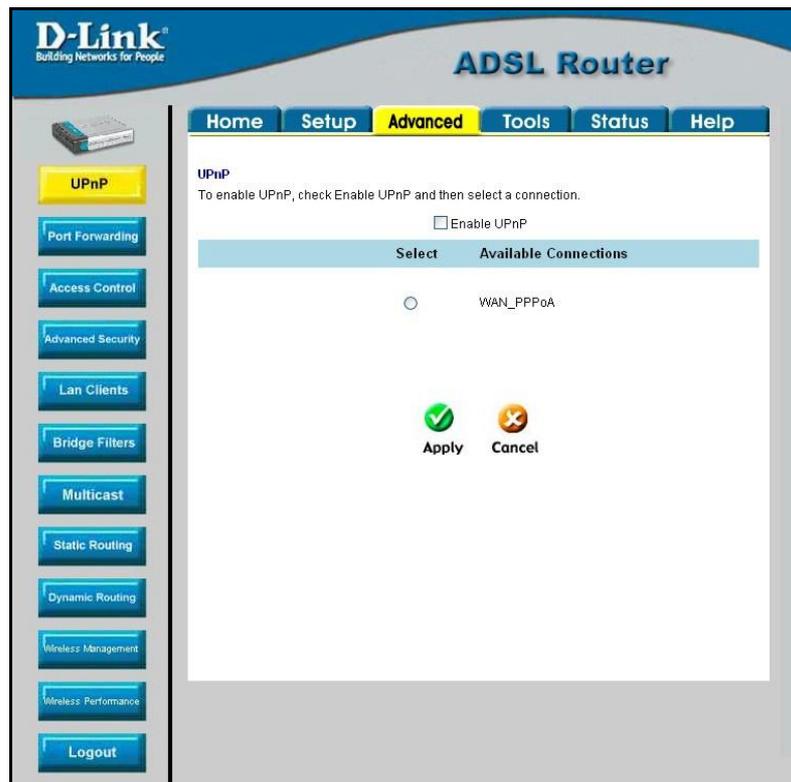


Figure 4-2. Advanced – UPnP window

To enable UPnP for any available connection, click to check the **Enable UPnP** selection box, select the connection or connections on which you will enable UPnP listed under **Available Connections** and click the **Apply** button.

LAN Clients

The LAN Clients menu is used when establishing Port Forwarding, Access Control and Advanced Security rules for IP addresses on the LAN. This menu can be accessed directly by clicking on the **LAN Clients** button or hyperlink in the **Advanced** setup menu. You can also click on the New IP button located in the Port Forwarding, Access Control and Advanced Security menus to access this menu. In order to use these advanced features it is necessary to have IP addresses available for configuration. If there are no IP addresses listed in the LAN Clients menu, it will not be possible to configure Port Forwarding, Access Control and Advanced Security.

Use the LAN Clients menus to add or delete static IP addresses for the advanced functions mentioned above, or to Reserve a Dynamically assigned IP address for an advanced function. Dynamically assigned IP addresses will only be listed if DHCP is enabled on the Router.

The screenshot displays the 'LAN Clients' configuration page on a D-Link ADSL Router. The interface includes a sidebar with various setup options, with 'Lan Clients' highlighted. The main area shows the 'Advanced' tab selected. It features input fields for 'IP Address' and 'Host Name', followed by an 'Add' button. A message indicates the 'Valid IP Range : 1.0.0.1 - 223.255.255.254'. Below this, there are two tables: 'Static Addresses' and 'Dynamic Addresses'. The 'Dynamic Addresses' table contains one entry with IP 192.168.1.11, Host Name LUKE, and Type Dynamic. At the bottom, there are 'Apply' and 'Cancel' buttons.

Figure 4-3. LAN Clients Setup

To add a static IP address to the list of available IP addresses, type an IP address that falls within the range a available IP addresses and click on the **Add** button. In the example above, available addresses range from 1.0.0.1 to 223.255.255.254. Any addresses added will appear in the list of **Static Addresses** available for advanced configuration. These addresses can then be used in the other Port Forwarding, Access Control and Advanced Security menus.

To delete an IP address from the list of Static Addresses, click the **Delete** box for the address or addresses you want to eliminate and click on the **Apply** button.

Dynamically assigned IP addresses may be reserved so that the lease does not expire for the LAN IP address. Click the Reserve box for the address or addresses you want to reserve and click the Apply button. These addresses will become Static IP addresses and will no longer be available for DHCP assignment.

Port Forwarding

Port Forwarding allows specific functions to bypass NAT protection that would otherwise not allow them to function. To use Port Forwarding, you must have specific client IP addresses available for configuration. Use the LAN Clients menu to establish client IP addresses available for port forwarding.



In order to use Port Forwarding, Firewall support must be enabled. See Enable/Disable NAT and Firewall in the Advanced Security menu.

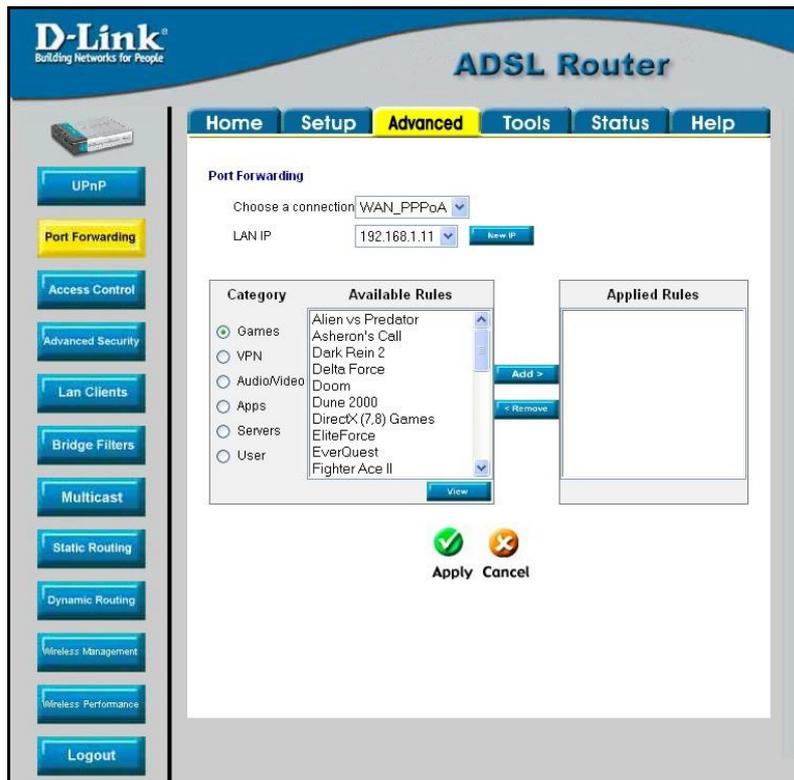


Figure 4-4. Advanced – Port Forwarding window

There are many different pre-configured rules available for specific functions such as Internet gaming, VPN, streaming and interactive multi-media, standard TCP/IP protocols, reserved ports, p2p, network management applications, and so on.

You may also create customized rules to manage TCP/UDP ports. The pre-configured rules include those listed in the table here:

Category	Available Rules
Games:	Alien vs. Predator, Asheron's Call, Dark Rein, Delta Force, Doom, Dune, DirectX Games, EliteForce, EverQuest, Fighter Ace II, Half Life, Heretic II, Hexen II, Kali, Motorhead, MSN Gaming Zone, Myth: The Fallen Lords, Need for Speed Porsche, Need for Speed 3, Outlaws, Rainbow 6, Starcraft, Tiberian Sun, Ultima, Unreal Tournament.
VPN	IPSec, PPPTP
Audio/Video	Net2Phone, Netmeeting, QuickTime
Applications	VNC, Win2k Terminal, PC Anywhere, Netbios, RemoteAnything, Radmin, LapLink, CorbonCopy, Gnutella.
Servers	Quake 2, Quake 3, Unreal, Web, FTP, Telnet, DNS, LDAP, NNTP, SMTP, POP 2, POP3, IMAP, IRC, Lotus, Remote.
User	Use this to set up custom TCP/UDP port rules.

To configure a new port-forwarding rule for any of the pre-configured rules, follow these steps:

1. Select the WAN connection you want to use for the new rule from the **Choose a connection** pull-down menu.
2. Select a **LAN IP** from the available client IP addresses listed in the pull-down menu; or, create a **New IP** by clicking the button. This brings up the LAN Client menu (see above).
3. Select the **Category** of the rule you are creating. The **Available Rules** for the category appear listed.
4. Highlight to select the Available Rule you want to apply.
5. Click on the **Add>** button to place the rule in the **Applied Rules** list of port forwarding that are actively applied to the client

The Available Rules can be applied to a single client IP address. That is, it is not possible to use an applied rule for multiple IP addresses on the LAN.

The **User** category for port forwarding is used to set up customized port forwarding rules.

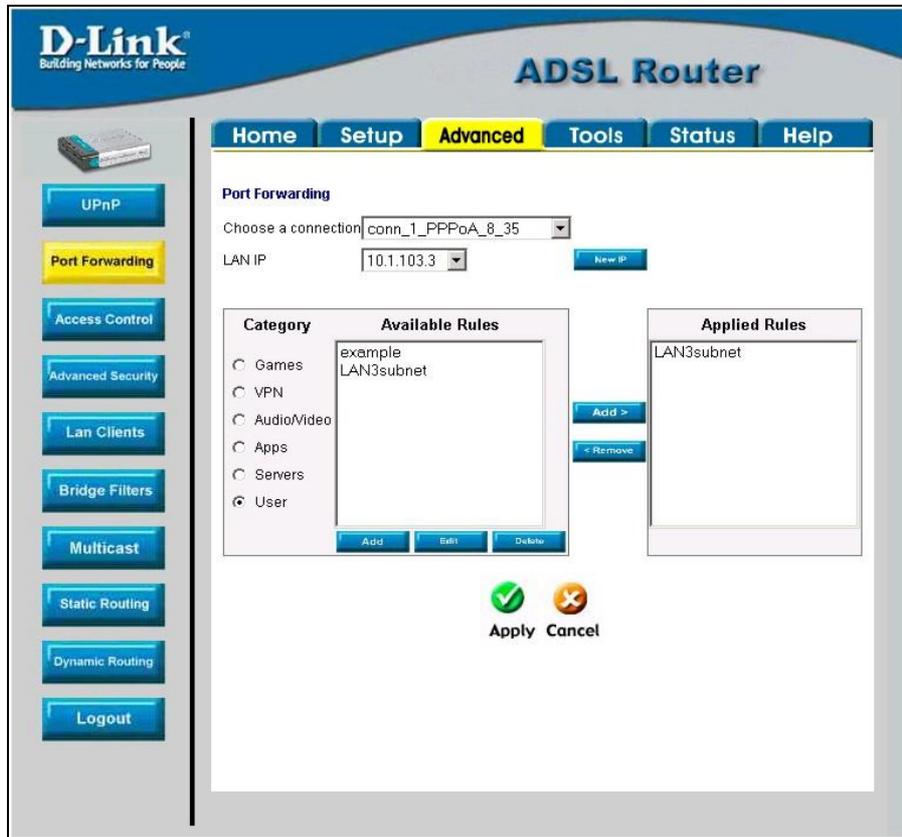


Figure 4- 5. Set up Custom Port Forwarding Rules

To set up custom TCP or UDP port forwarding rules, follow these steps:

1. Select the **User** category and click the **Add** button located below the Available Rules list. This will change the menu to look like the example below.

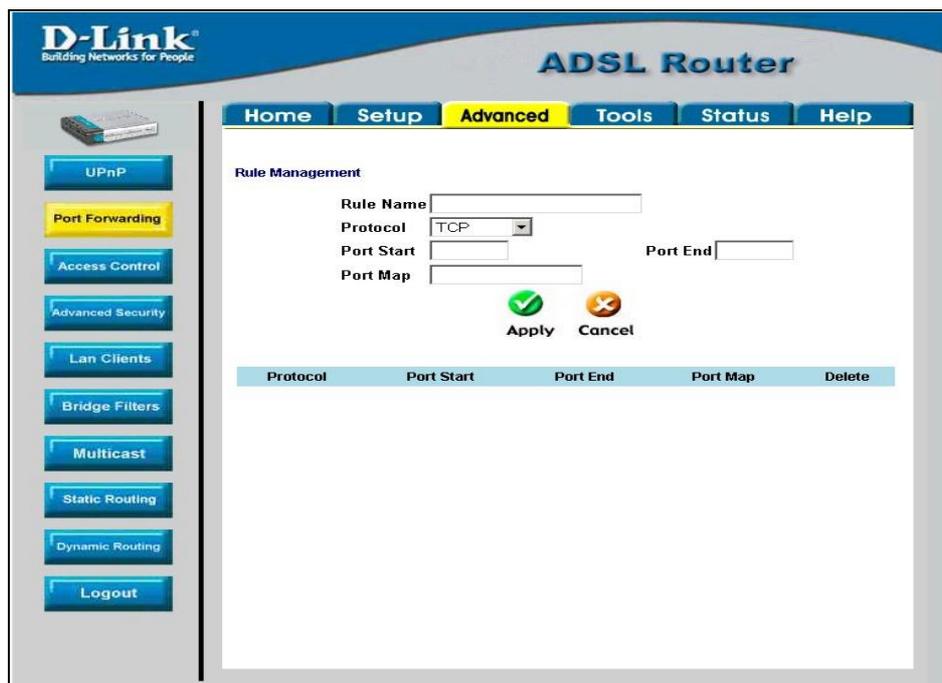


Figure 4- 6. Port Forwarding User Rules Management

2. Type a **Rule Name** in the space provided.
3. Select the port **Protocol** from the pull-down menu - you may select *TCP*, *UDP* or both (*TCP/UDP*).
4. 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.
5. Type a number for the Port Map in the space provided.
6. Click the **Apply** button to create the new rule. The new rule will appear listed in the table of custom port forwarding rules.

Access Control

Access Control settings are used to block various services and protocols for specific client IP addresses. The configuration process is similar to setting up port forwarding, except access control will deny specific functions to client IP addresses. There are pre-configured rules for specific functions that may be blocked or you can block specific UDP or TCP ports. Access control operates for specific IP addresses across all WAN connections. If you are using more than one WAN connection, a single set of access rules is maintained for each controlled IP address that operates on all WAN connections.



Note

In order to use Port Access Control, Firewall support must be enabled. See Enable/Disable NAT and Firewall in the Advanced Security menu.

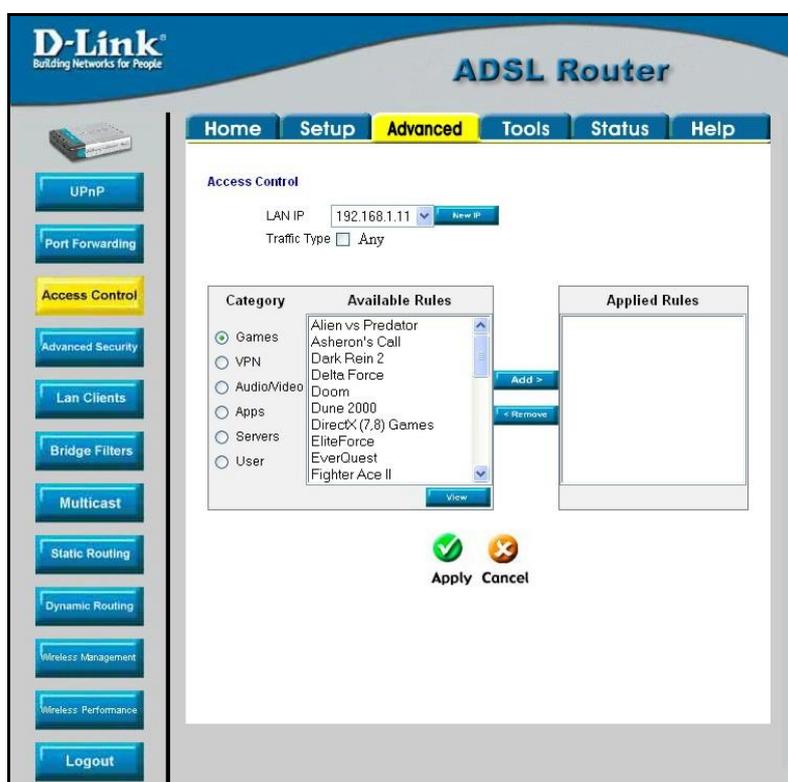


Figure 4-7. Access Control menu

Remember, if the client IP address you want does not appear listed in the LAN IP pull-down menu, click on the New IP button to go to the LAN Clients menu.

To block all traffic from the WAN port to a specific IP address, select the **LAN IP** address to block and click to check the **Traffic Type** **Any** selection box, then click the **Apply** button. This will block all traffic from the WAN port to the specified client.

Remember to save the configuration changes.

Access Control pre-configured rules are the same as for port forwarding:

Category	Available Rules
Games:	Alien vs. Predator, Asheron's Call, Dark Rein, Delta Force, Doom, Dune, DirectX Games, EliteForce, EverQuest, Fighter Ace II, Half Life, Heretic II, Hexen II, Kali, Motorhead, MSN Gaming Zone, Myth: The Fallen Lords, Need for Speed Porsche, Need for Speed 3, Outlaws, Rainbow 6, Starcraft, Tiberian Sun, Ultima, Unreal Tournament.
VPN	IPSec, PPPTP
Audio/Video	Net2Phone, Netmeeting, QuickTime
Applications	VNC, Win2k Terminal, PC Anywhere, Netbios, RemoteAnything, Radmin, LapLink, CorbonCopy, Gnutella.
Servers	Quake 2, Quake 3, Unreal, Web, FTP, Telnet, DNS, LDAP, NNTP, SMTP, POP 2, POP3, IMAP, IRC, Lotus, Remote.
User	Use this to set up custom TCP/UDP port rules.

To configure a new Access Control rule for any of the pre-configured rules, follow these steps:

1. Select a **LAN IP** from the available client IP addresses listed in the pull-down menu; or, create a **New IP** by clicking the button. This brings up the LAN Client menu (see above).
2. Select the **Category** of the rule you are creating. The **Available Rules** for the category appear listed.
3. Highlight to select the Available Rule you want to apply.
4. Click on the **Add>** button to place the rule in the **Applied Rules** list of port forwarding that are actively applied to the client

The Available Rules can be applied to a single client IP address. That is, it is not possible to use an applied rule for multiple IP addresses on the LAN.

To set up custom TCP or UDP access control rules, follow these steps:

1. Select the User category and click the **Add** button located below the Available Rules list.
2. In the new menu that appears, type a **Rule Name** in the space provided.
3. Select the port **Protocol** from the pull-down menu - you may select *TCP*, *UDP* or both (*TCP/UDP*).
4. 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.
5. Type a number for the Port Map in the space provided.
6. Click the **Apply** button to create the new rule. The new rule will appear listed in the table of custom port control rules.

Advanced Security

Use the Advanced Security features of the Router to globally enable or disable NAT and Firewall protection for any WAN connection, enable or disable DMZ IP addresses, enable or disable remote Telnet or web management from specified IP addresses, and enable/disable ICMP ping packets from the WAN.



Figure 4-8. Advanced Security menu

Follow the instructions below to set up the Advanced Security features. To enable ICMP Ping packets from the WAN, click to check the **Allow Incoming ICMP Ping** selection box and click the **Apply** button. The ICMP (Internet Control Message Protocol) Ping packet is used to test connectivity of IP devices. Keep in mind that when this is enabled, the Router may be vulnerable to denial of service type attacks.

Enable/Disable NAT and Firewall

NAT and basic Firewall protection can be enabled or disabled for any WAN connection. These may also be enabled or disabled when configuring the WAN connection for any connection type except Bridge connections. By default, they are enabled for WAN connections (except Bridge connections) when they are first set up. Firewall protection includes the previously discussed Port Forwarding and Access Control. Therefore, this must be enabled to use these features.

To enable NAT and Firewall protection for any WAN connection including Bridge type connections, check the **Enable NAT and Firewall Services** selection box and click the **Apply** button. Be sure to save the changes in the System Commands menu or the settings will be lost.

To disable NAT and Firewall Services, deselect it and click the **Apply** button. Be aware that this remove basic security and expose your LAN to potentially malicious agents form the WAN.

Remember to save the configuration changes.

DMZ IP Address

A DMZ address is used for a device that is not given basic protection of NAT and Firewall services. You may select an IP address from the pull-down menu or create a **New IP** by pressing the button. This brings up the LAN Clients menu in which you may create a static client IP or reserve a dynamically assigned IP address for DMZ designation.

Setup Remote Management

Telnet and web management through the WAN port can be enabled for specified IP addresses. To enable remote management, click to check the selection box for **Remote Telnet** or **Remote Web** and type in an IP address and net mask of a trusted host.

Bridge Filters

Bridge filters are used to block or allow various types of packets through the WAN interface. This may be done for security or to improve network efficiency. The rules are configured for individual devices based on MAC address. Filter rules can be set up for source, destination or both. You can set up filter rules and disable the entire set of rules without losing the rules that have been configured.



Figure 4-9. Bridge Filters menu

To add a bridge filter rule, check **Enable Bridge Filters**, type in a Source MAC, a Destination MAC or both in the entry fields, and click the **Add** button. To edit an existing rule, select the rule by clicking the **Edit** radio button. The rule will appear in the entry fields above as it is currently configured. Make the desired changes and click the **Add** button. To remove a bridge filter from the table in the bottom half of the window, click to select the corresponding **Delete** box, and then click **Apply**. Remember to save the configuration changes.

The protocols that may be specifically allowed or denied to pass through the WAN interface are the following: *IPv4, IPv6, RARP, PPPoE Discovery and PPPoE Session.*

Multicast Pass-through

Multicast pass-through can be enabled or disabled for any WAN connection. When enabled it allows IGMP packets to pass through the WAN interface. IGMP packets are used to control multicasts and discontinue multicasts to individual IP addresses when they are no longer needed.

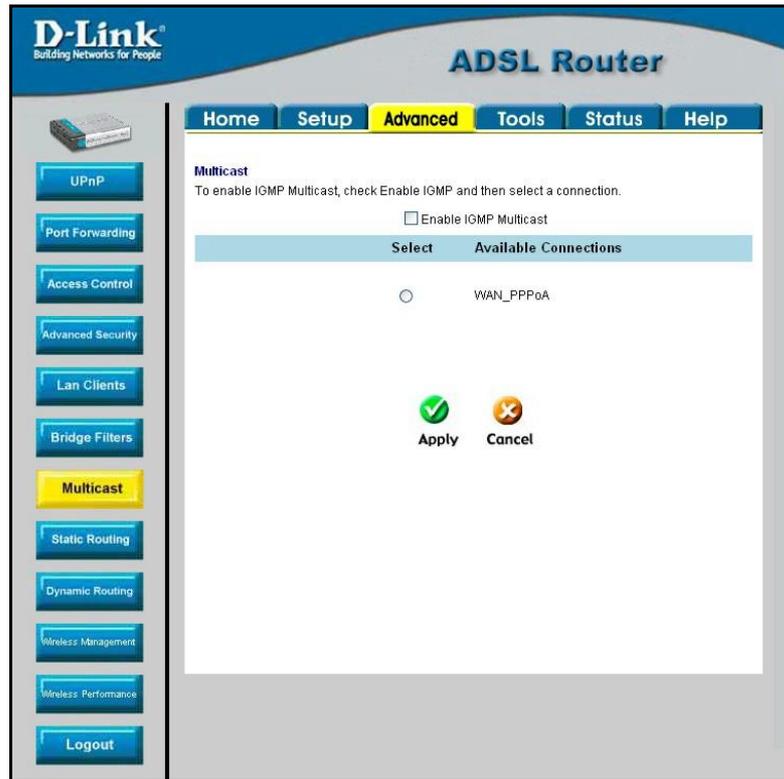


Figure 4-10. Multicast pass-through menu

To enable Multicast pass through for any WAN connection, select the connection and click the **Enable IGMP Multicast** box to select the option, then click the **Apply** button. Remember to save the configuration changes.

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.



The screenshot shows the D-Link ADSL Router web interface. The top navigation bar includes 'Home', 'Setup', 'Advanced' (highlighted), 'Tools', 'Status', and 'Help'. A left sidebar contains various configuration options, with 'Static Routing' highlighted in yellow. The main content area is titled 'Static Routing' and contains the following fields:

- Choose a connection: WAN_PPPOA (dropdown menu)
- New Destination IP: [text input]
- Mask: 255.255.255.0 (text input)
- Gateway: [text input]
- Metric: 1 (text input)

Below the fields is a table with the following headers: Connection, Destination, Mask, Gateway, Metric, Delete. At the bottom of the page are two buttons: 'Apply' (with a green checkmark icon) and 'Cancel' (with an orange 'X' icon).

Figure 4-11. Static Routing menu

To add a static route, choose a connection from the pull-down menu and then enter a **New Destination IP** address, subnet **Mask**, **Gateway** IP address and **Metric** value. 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.

Dynamic Routing

The Router supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices. It also supports use of password protection which requires password verification for RIP requests. Use the Dynamic Routing menu to enable RIP and if desired to configure password protection.

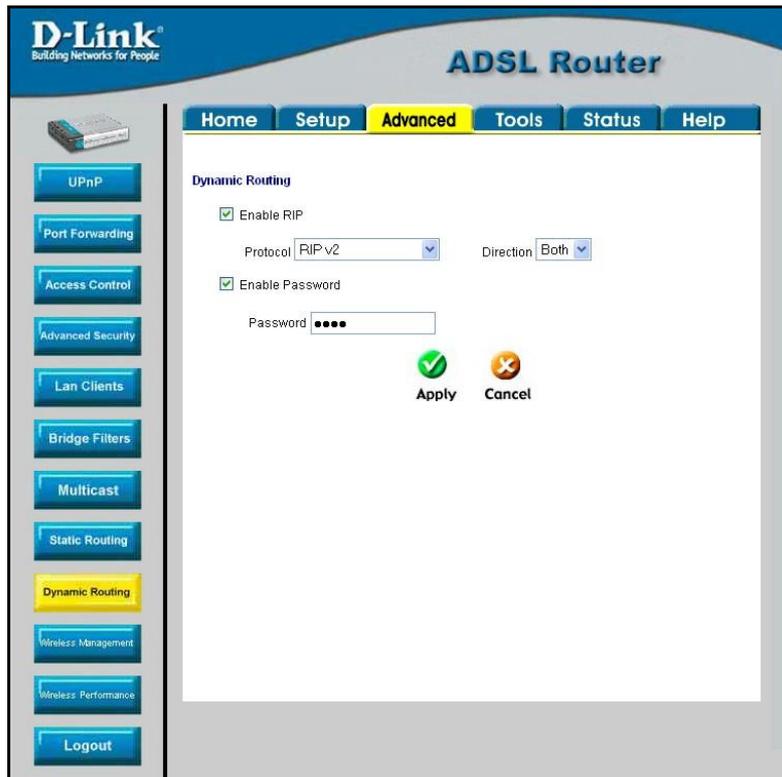


Figure 4-12. Dynamic Routing (RIP) menu

To enable RIP v1, check **Enable RIP**, select **RIP v1 Protocol**, select the **Direction** (*In*, *Out*, or *Both*), and click **Apply**. To enable *RIP v2* or *RIP v1 Compatible*, select the appropriate **Protocol** and **Direction** and click **Apply**. To use password protection for *RIP v2* or *RIP v1 Compatible* protocols, check **Enable Password**, enter a **Password**, and click **Apply**.

Wireless Management

For added security you can opt to use Access Control based on the MAC address. This feature lets you create a list of MAC addresses that are allowed or denied association with the Router through the wireless interface. When it is enabled, the access point is instructed to forward packets only from wireless devices only if the MAC address of the device is granted association. Packets received through the wireless interface from non-authorized devices, including other access points, will be dropped.

Click **Enable Access List**.

Enter a MAC Address in the box, choose **Allow** or **Ban**, then click **Apply**.



Multiple Virtual Connections

The Router can use up to eight simultaneous PVC connections. These additional connections occupy the same bandwidth used for ADSL service. Additional PVC connections can be added to establish a private connection to remote offices or maintain a server accessible through the WAN port. Provision for additional PVC profiles must be done through the telephone company or telecommunications services company. The remote user must have suitable ADSL equipment for a successful connection.

The New Connection menu is used to configure additional WAN connection that can operate simultaneously with the other connections. PPPoE type WAN connections can be disconnected or connected as needed. Non-PPPoE type connections must be deleted from the configuration settings if you want to disable them.

To set up additional virtual connections, follow the procedure described in Create a New Connection. Keep in mind that each new connection must have a VPI/VCI value set that is unique to the Router. The numbers for these values will be provided by your service provider.

PPPoE and PPPoA connections may be connected and disconnected with the **Connect** and **Disconnect** menu buttons located in the connection settings menu.

The remaining connection types (Bridge, Static, DHCP and CLIP) connect upon saving the settings and restarting the Router. These connections can be disconnected only if the connection set is deleted. To delete any WAN connection set, click on the **Delete** button in the menu for the connection.

Tools and Utility Menus

The menus listed under the Tools tab are used for **System Commands** to save settings, restart and reset the Router; to set up **Remote Log** information; for **User Management**; to update firmware and load saved configuration files (in the **Update Gateway** menu); to perform a **Ping** test; and to test the DSL network connectivity in the **Modem Test** menu.

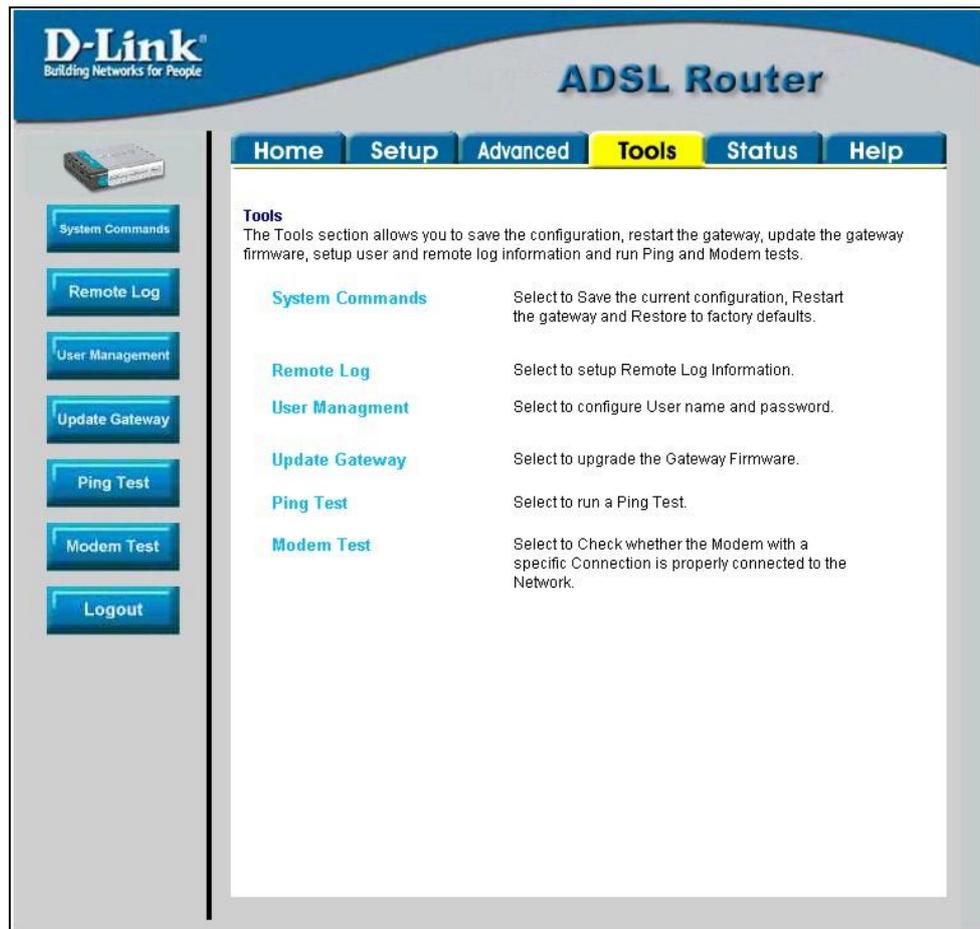
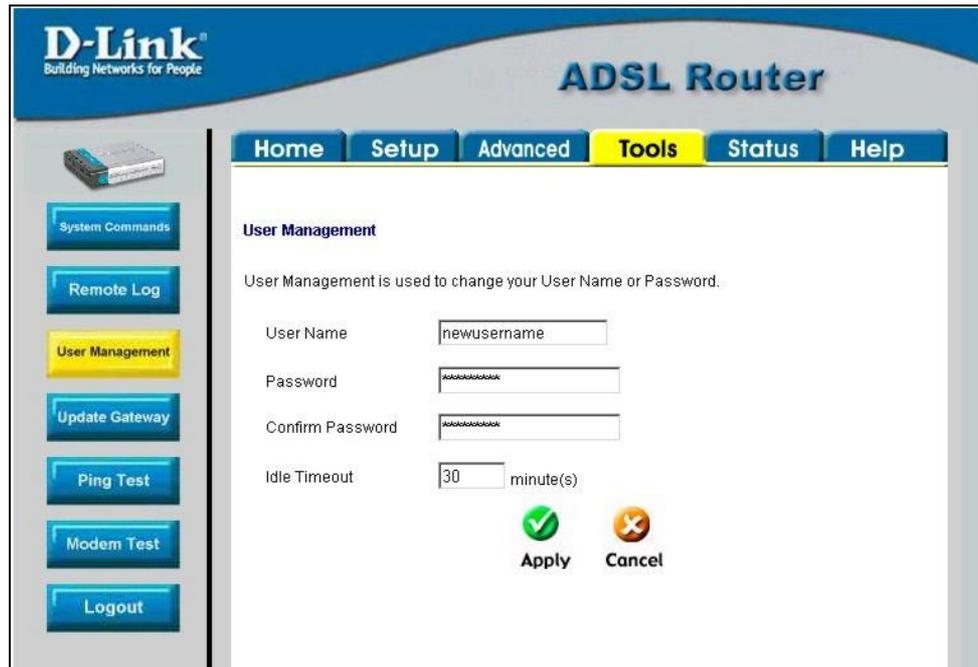


Figure 4-13. Tools and utility menu links

Click the hyperlink or menu button to view the desired menu.

User Management

It is a good idea to change the management user information used for the Router before or immediately after establishing a link to the WAN.



The screenshot shows the D-Link ADSL Router web interface. The top navigation bar includes 'Home', 'Setup', 'Advanced', 'Tools' (highlighted), 'Status', and 'Help'. A left sidebar contains buttons for 'System Commands', 'Remote Log', 'User Management' (highlighted), 'Update Gateway', 'Ping Test', 'Modem Test', and 'Logout'. The main content area is titled 'User Management' and contains the following fields and controls:

- User Name:** A text input field containing 'newusername'.
- Password:** A password input field with masked characters.
- Confirm Password:** A password input field with masked characters.
- Idle Timeout:** A numeric input field containing '30' followed by the text 'minute(s)'.
- Buttons:** 'Apply' (with a green checkmark icon) and 'Cancel' (with an orange 'X' icon).

Figure 4-14. User Management menu

To change the user name and password used for management access to the Router:

1. Type the current **User Name** in the entry field provided.
2. Type in the new **Password** in the entry field provided.
3. Type in the new password again in the **Confirm Password** field.
4. If desired, change the **Idle Timeout** value.
5. Click **Apply**.

System Commands

The System Commands are used to save settings to non-volatile memory, to reboot the Router and to restore factory default settings to the Router.

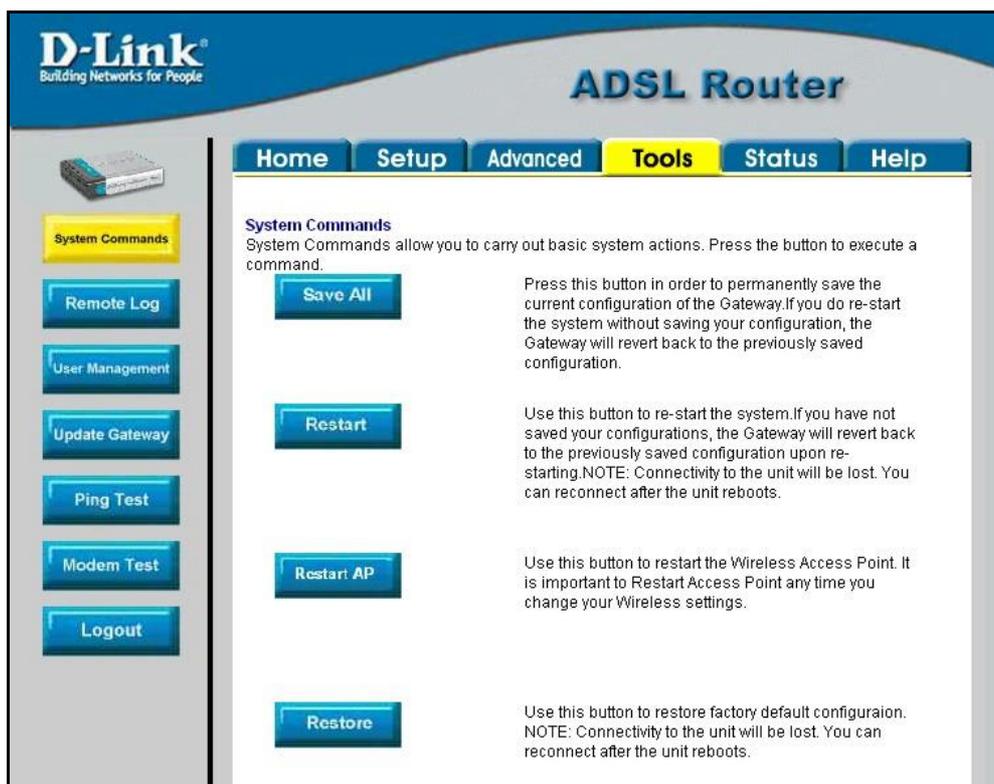


Figure 4-15. Tools – System Commands menu

Click on the appropriate menu button to perform the following system tasks:

System Function	Description
Save All	In order to save the configuration changes you have just made they must be saved to the Router's non-volatile RAM by clicking on the Save All button.
Restart	Click the Restart button to restart the Router. If you have not saved your changes, the Router will revert to the previously saved configuration upon rebooting the Router.
Restart AP	Click to restart the Wireless AP (Access Point). The Wireless AP must be restarted any time wireless configuration is changed.
Restore	The DSL-G664T can be reset to the default configuration for all settings using the Restore option. This will also change the both the LAN and WAN IP address of the device, so these will need to be reconfigured accordingly. To perform a factory reset, click the Restore button. Since the IP settings will return to their default, you will lose access to the Web Manager. To use the Web Manager interface, the LAN IP address will need to be reconfigured.

Remote Log

Use the Remote Log menu to set up logging to servers or computers that are located outside the LAN or subnet of the Router.

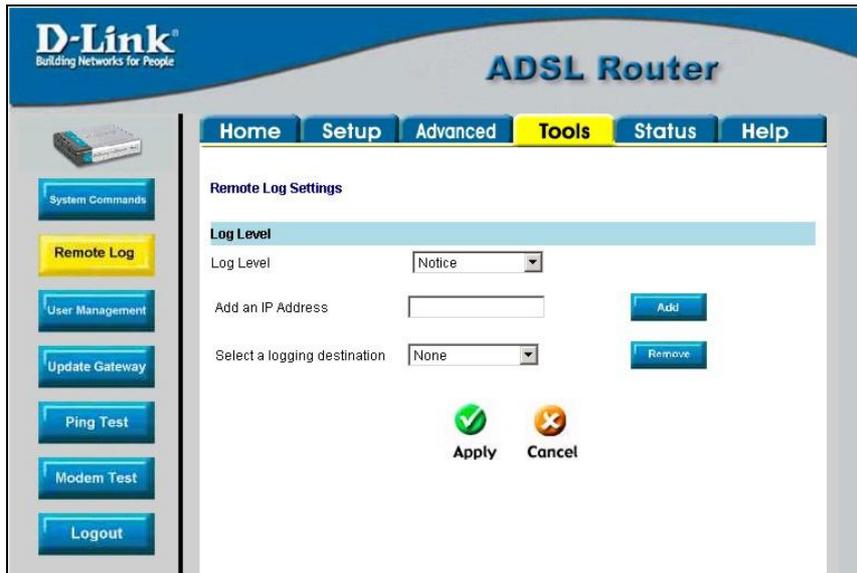


Figure 4-16. Remote Log menu

Select the **Log Level** from the pull-down menu. The levels available are: *Alert, Critical, Debug, Error, Info, Notice, Panic* and *Warning*. Type in the IP address of a receiver for the log message in the **Add an IP Address** field and click on the **Add** button. Log message receivers that are added appear listed in the **Select a logging destination** pull-down menu. These may be used at any time for other types of log messages. To remove a log message receiver from the list, select it and click on the **Remove** button. Click the **Apply** button when you have configured the log message receivers. Remember to save the settings to non-volatile memory.

Update Gateway

Use the Update Gateway feature to load the latest firmware for the device. You can obtain the latest version of the DSL-G664T firmware by logging onto the D-Link web site at www.dlink.com. Save the latest firmware version to a file on your computer or an accessible TFTP server.

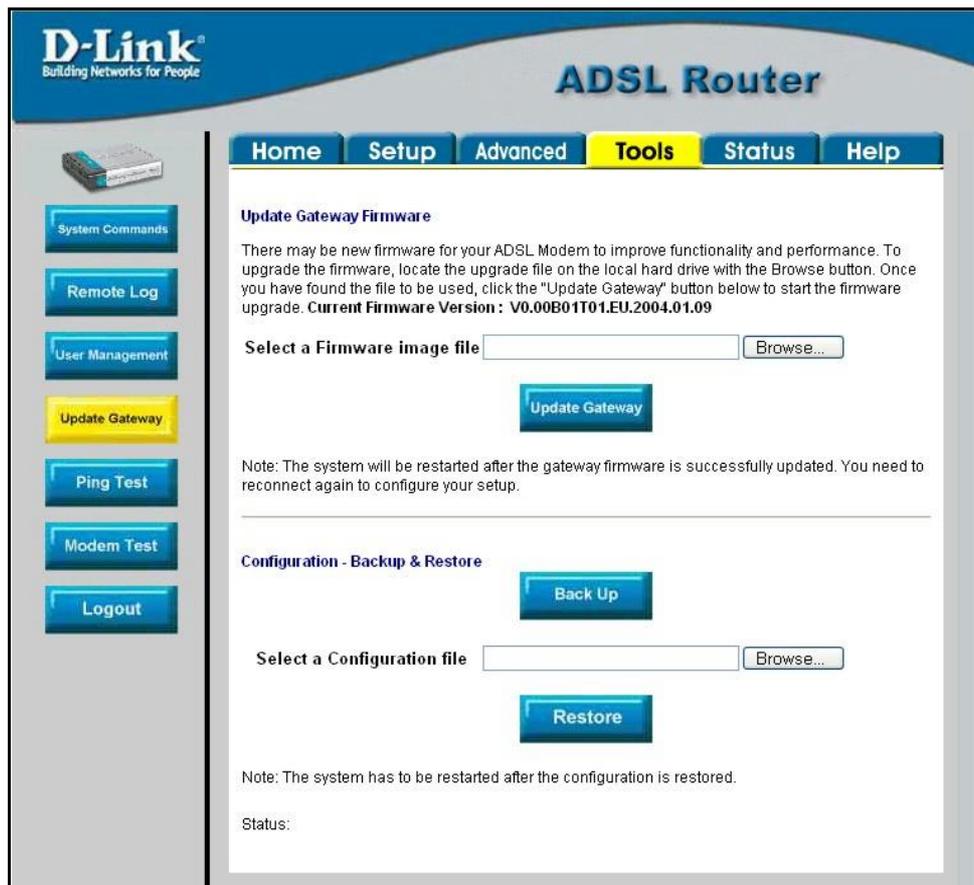


Figure 4-17. Tools – Update Gateway window

To upgrade firmware, type in the name and path of the file in the Select a Firmware image file space or click on the **Browse** button to search for the file. Click the **Update Gateway** button to begin copying the file. The file will load and restart automatically.

Use the Configuration – Backup & Restore features to store current settings to a file on your computer or to load previously saved configuration files on the device.

To save the current settings to a configuration file on your computer, type in the full name and path in the Select a Configuration file space or click on the **Browse** button to search for the file. Click the **Back Up** button to initiate this action.

To load a saved configuration file from the computer, type in the full name and path in the Select a Configuration file space or click on the **Browse** button to search for the file. Click the **Restore** button to initiate this action.

Ping Test

The Ping Test menu allows you to ping any IP address from the Router to test connectivity to the address.

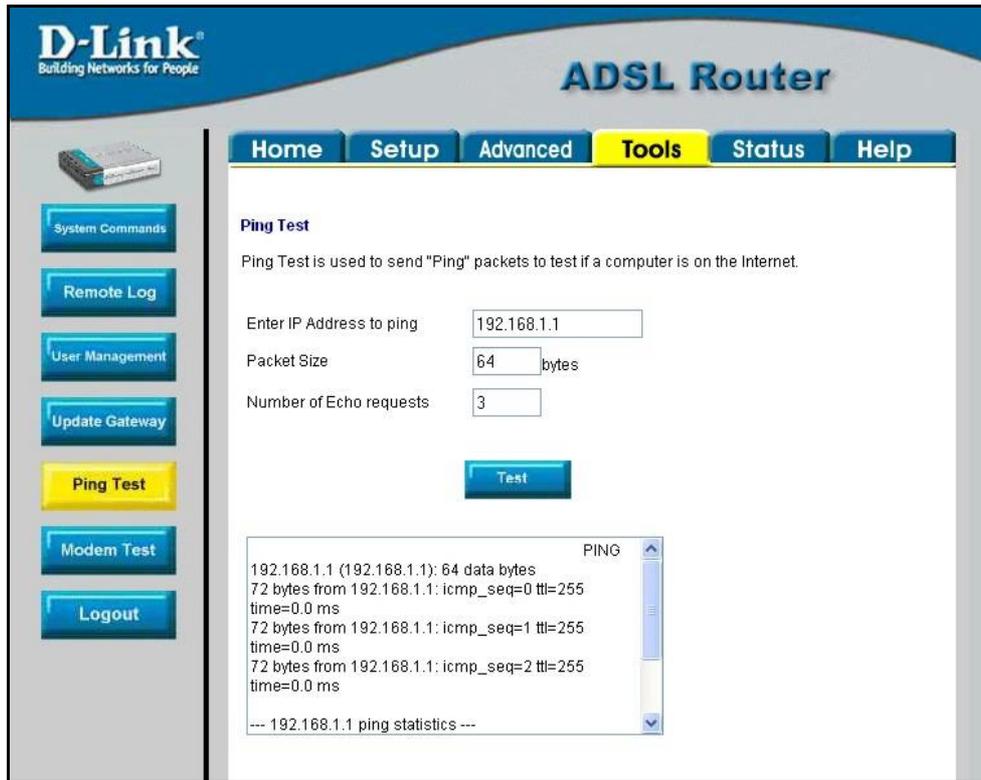


Figure 4-18. Tools – Ping Test window

To Ping a device, first enter the IP address of the device that you wish to Ping into the first field, the Packet Size (in bytes) in the second field, and finally, enter the number of times you wish the Ping function to attempt a connection to the desired device into the third field. Click **Test** to start the Ping mechanism. The results of the Ping will be shown in the result box in the bottom half of the window.

Modem Test

The Modem Test menu is used for trouble shooting connection problems on the WAN interface. You can test for connectivity on the service provider's network for any WAN connection. Test for F5 or F4 connection on the near segment or end-to-end.

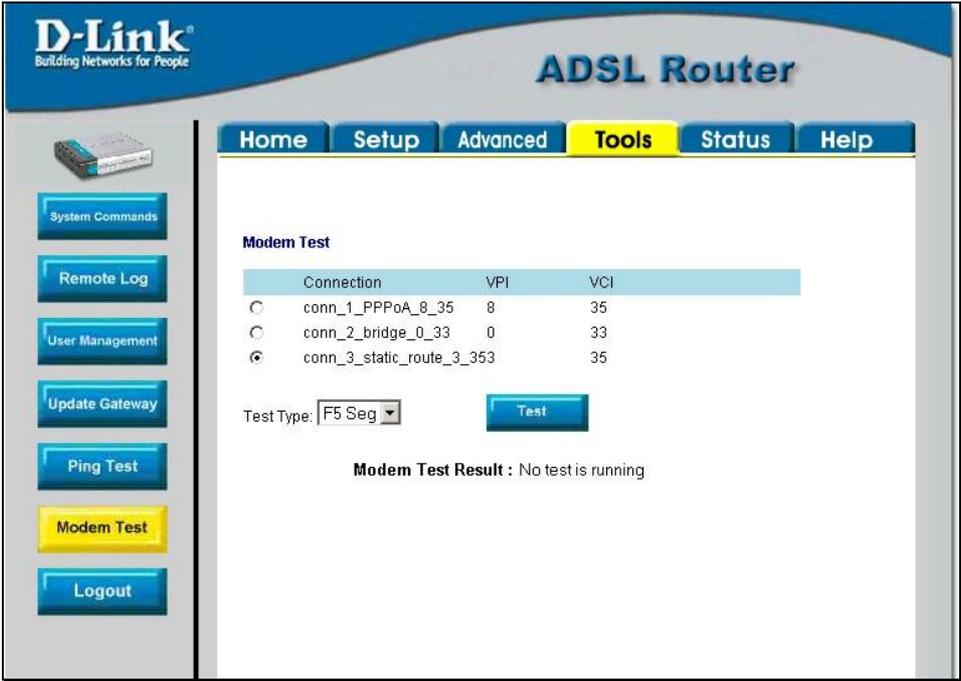


Figure 4-19. Tools – Modem Test window

To test your modem, select a **Connection**, choose a **Test Type**, and click **Test**.

Status Menus

Use the Status windows to display various performance data about the Router

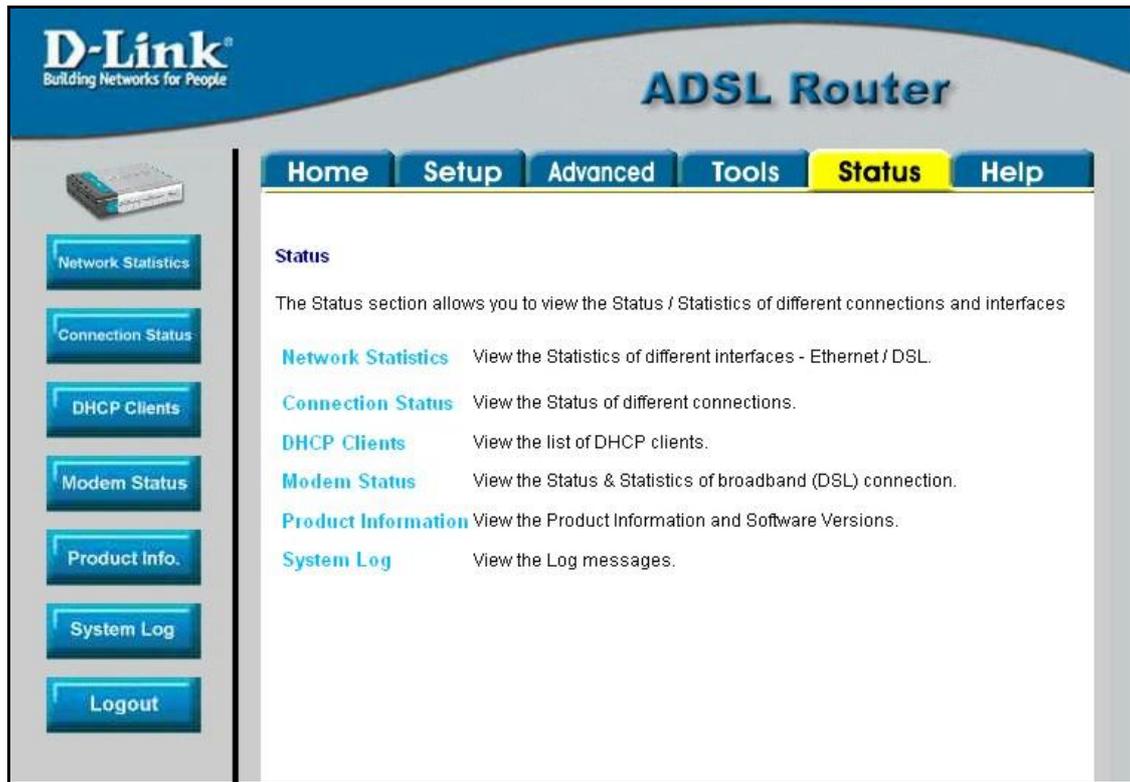


Figure 4-20. Status display links

Click the hyperlink or menu button for the desired Status window.

Network Statistics

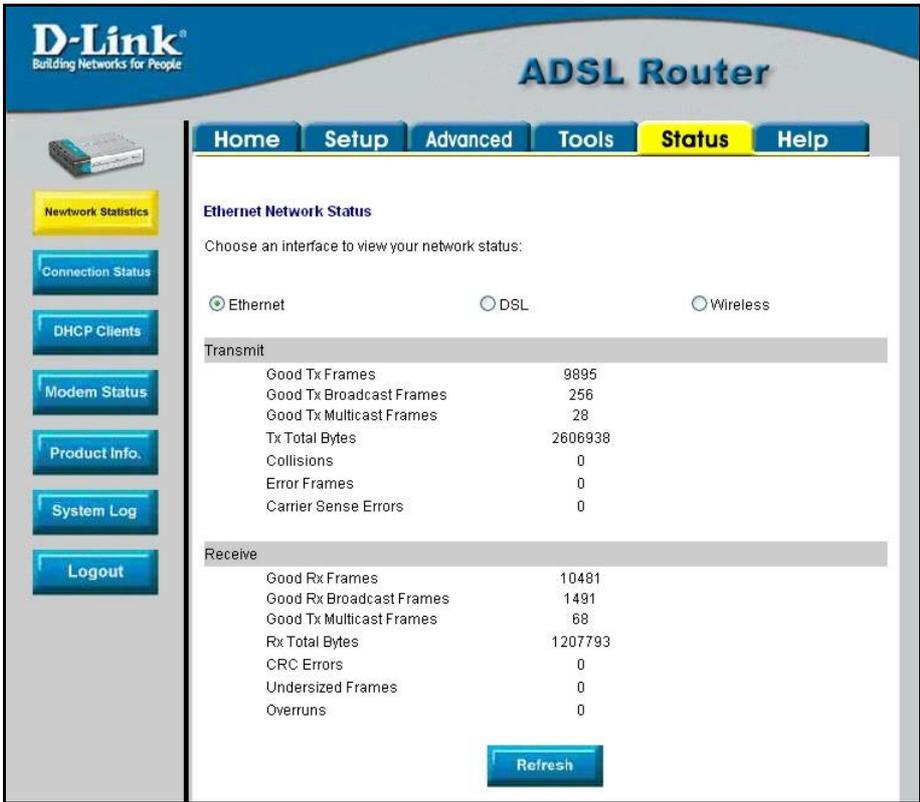


Figure 4-21. Network Statistics window

Choose the desired interface at the top of the window and then click **Refresh** to view Ethernet network statistics.

Connection Status

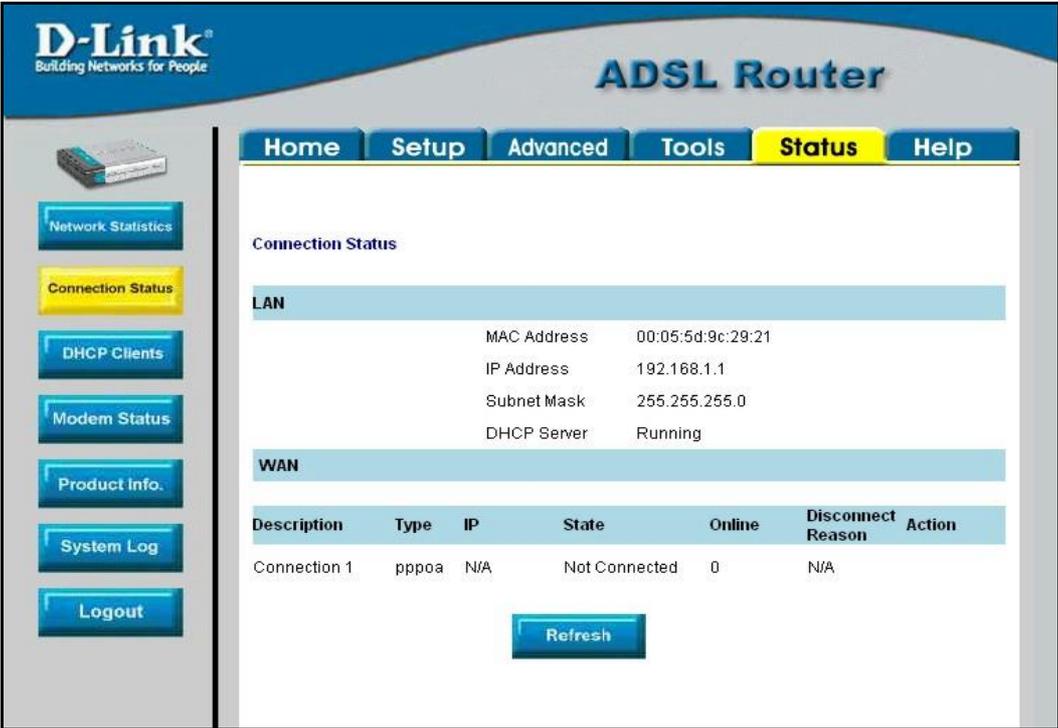


Figure 4-22. Connection Status window

Click **Refresh** to view connection status information.

DHCP Clients

This window displays the status of all current DHCP clients.

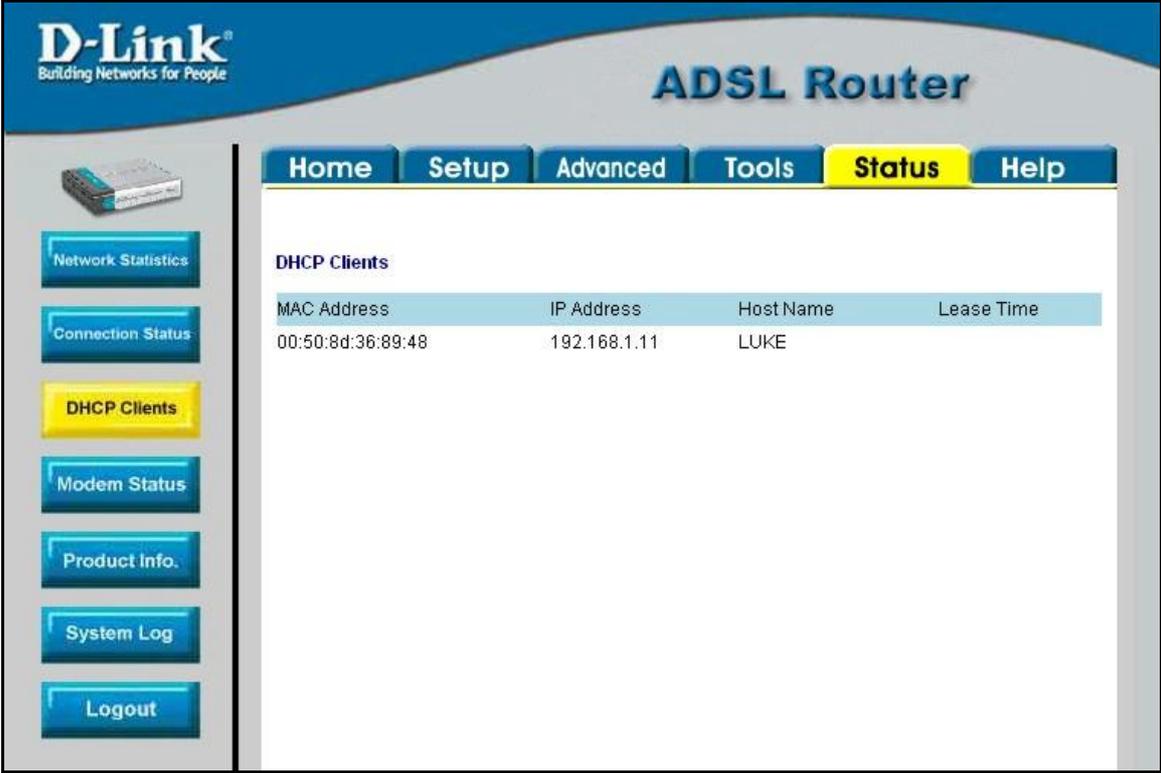


Figure 4-23. DHCP Clients window

Modem Status

This window displays DSL statistics and various modem status data.

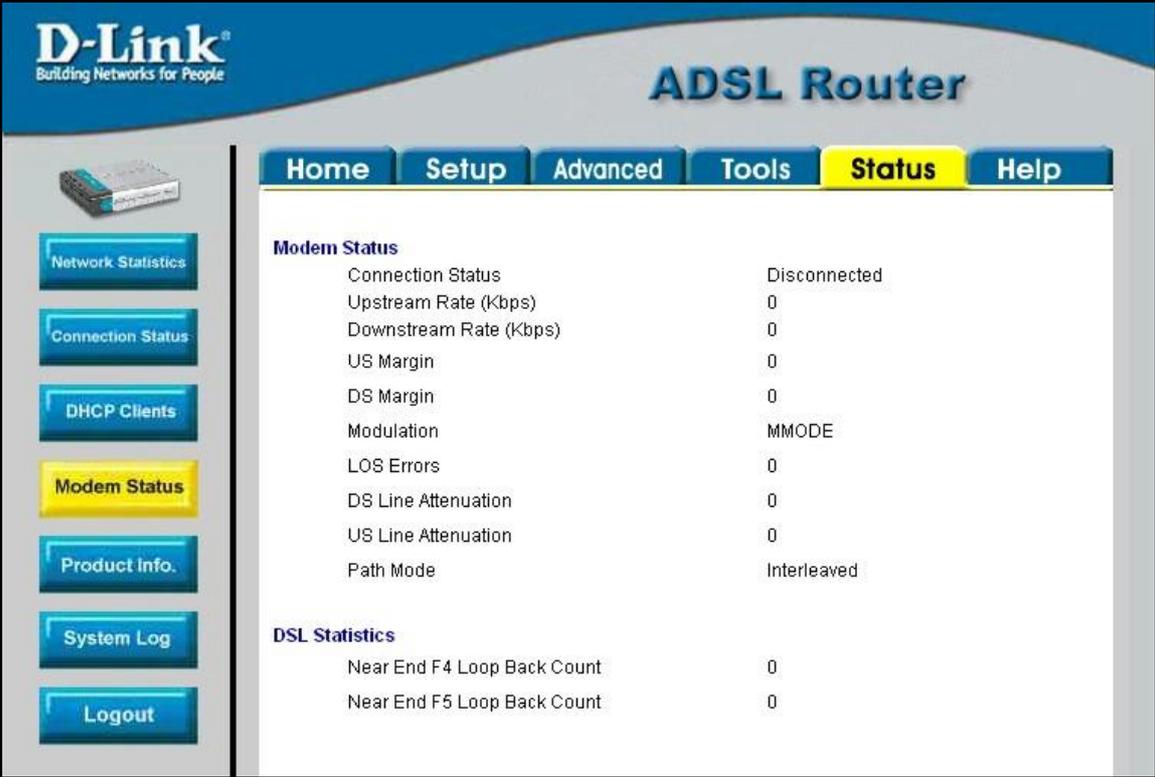


Figure 4-24. Modem Status window

Product Information

This window displays product information including hardware and firmware versions.

The screenshot shows the D-Link ADSL Router web interface. The top navigation bar includes 'Home', 'Setup', 'Advanced', 'Tools', 'Status' (highlighted), and 'Help'. A sidebar on the left contains buttons for 'Network Statistics', 'Connection Status', 'DHCP Clients', 'Modem Status', 'Product Info.' (highlighted), 'System Log', and 'Logout'. The main content area displays the 'Product Information' section, which is divided into two sub-sections: 'Product Information' and 'Software Versions'.

Product Information	
Model Number	DSL-G664T
HW Revision	Unknown
Serial Number	none
Ethernet MAC	00:0D:88:00:01:21
DSL MAC	N/A
AP MAC	00:0d:88:00:01:22

Software Versions	
Gateway	V0.00B01T01.EU.2004.01.09
ATM Driver	4.01.00.00
DSL HAL	1.01.00.00
DSL Datapumps	[1.01.00.00] Annex B
SAR HAL	01.06.06 s
PDSP Firmware	0.49
Wireless Firmware	0.3.16.13
Wireless APDK	5.5.20
Wireless Driver	1.1.2
Boot Loader	0.22.02

Figure 4-25. Product Information window

System Log

The system log displays chronological event log data.

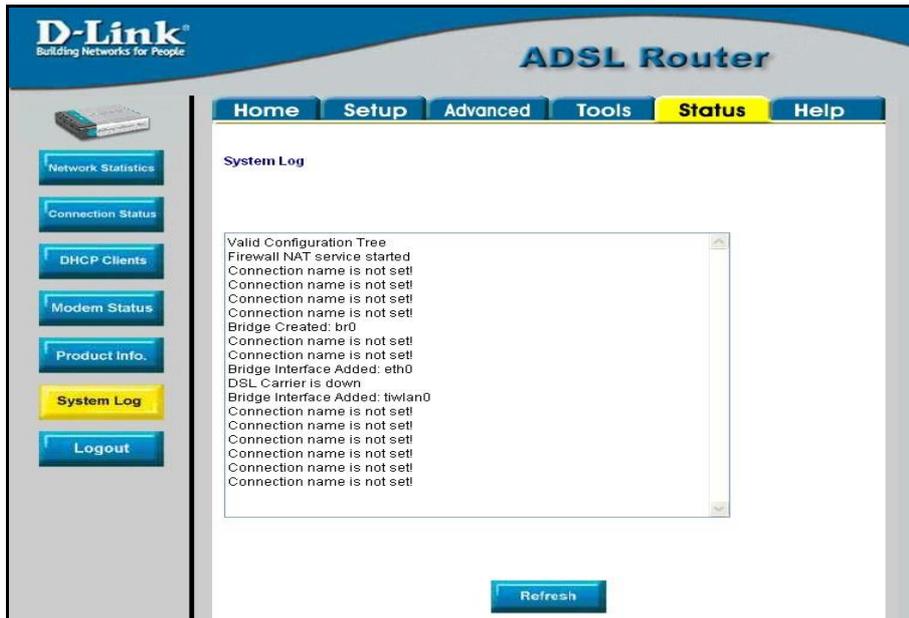


Figure 4-26. System Log window

Click **Refresh** to get the most current system log information.

Help Menu

Help menu links provide more information for configuring various Router functions.



Figure 4-27. Opening Help window



Technical Specifications

GENERAL		
Standards:	ITU G.992.1 (G.dmt) ITU G.992.2 (G.lite) 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 RJ-45 port for 10/100BASET Ethernet connection	

Physical and Environmental	
AC Inputs:	Input: 120V AC, 60 Hz
Power Adapter:	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:	180 x 141 x 30 cm (device only)
Weight:	380 grams (device only)
EMI:	CE Class B
Safety:	CSA 950, UL 1950, IEC 60950, EN 60950
Reliability:	Mean Time Between Failure (MTBF) min. 4 years



IP Address Setup

The DSL-G664T 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 accordingly. Consult the table below for IP settings on a Class C network.

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 three numbers in the IP address must always be the same with only the fourth number changing. The first three numbers define 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 computers' 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 5 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 the NAT function which is enable by default.

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.

Alternative IP Assignment			
Host	IP Address	Subnet Mask	Gateway IP
Router	10.0.0.1	255.255.255.0	
Computer #1	10.0.0.2	255.255.255.0	10.0.0.1
Computer #2	10.0.0.3	255.255.255.0	10.0.0.1
Computer #3	10.0.0.4	255.255.255.0	10.0.0.1

IP Setup - Example #2

These two examples are only examples you can use to help you get started. 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.



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.

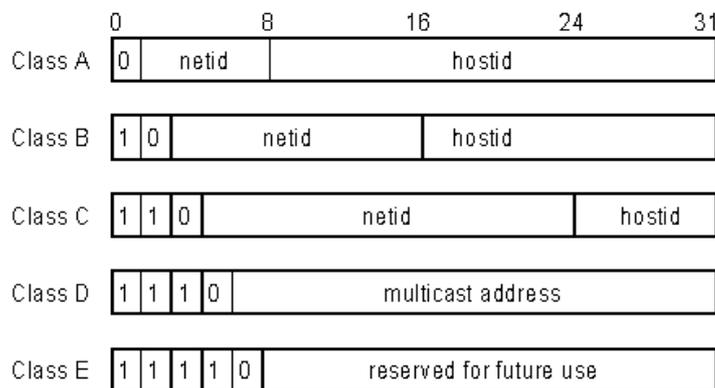
To make IP addresses easy to understand, the originators of IP adopted a system of representation called “dotted decimal” or “dotted quad” notation. Below are examples of IP addresses written in this format:

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 256 hosts.

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 all-0 or all-255. 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:

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 in a subnet mask that is to correspond to a net ID bit in the IP address must be set to 1.



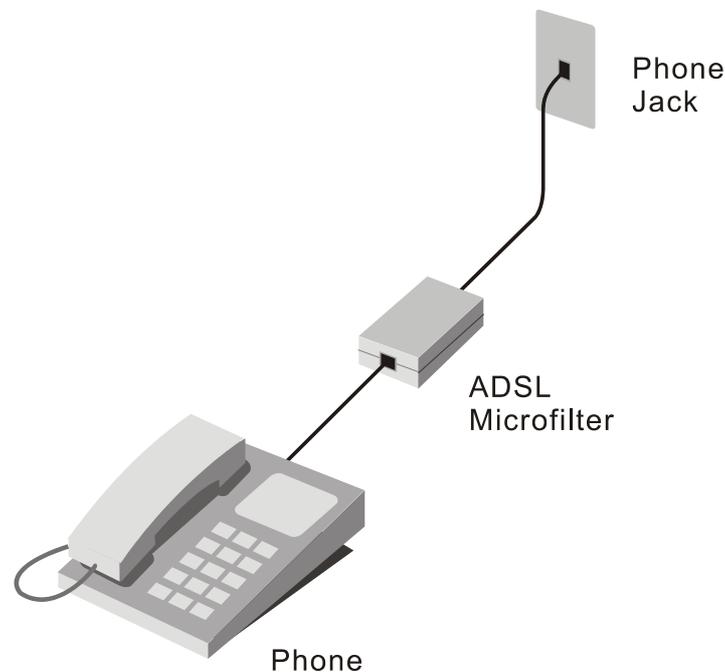
Microfilters and Splitters

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 Modem to the ADSL line.

Microfilters

Unless you are instructed to use a “line splitter” (see below), it will be necessary 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 Modem and the telephone jack. Microfilters are only intended for use with regular telephones, Fax machines and other regular telephone devices.

Line Splitter

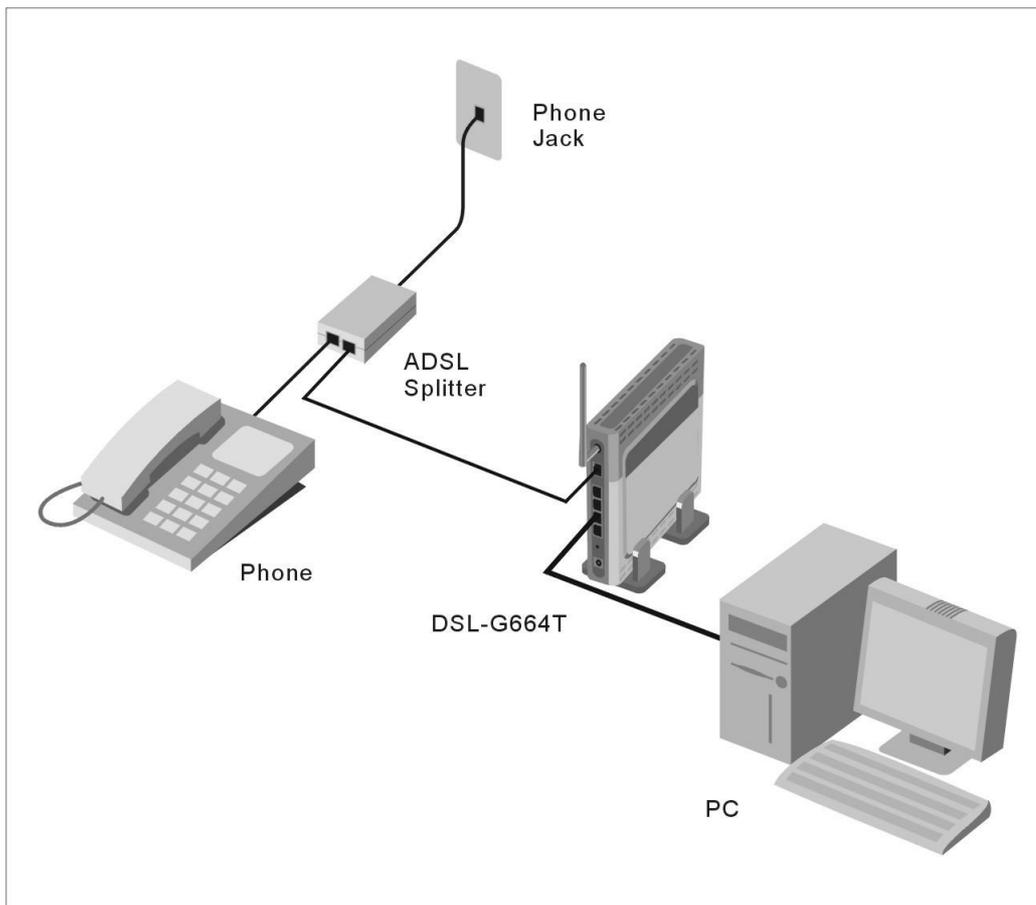
If you are instructed to use a “line splitter”, you must install the device between the Modem and the phone jack. Use standard telephone cable with standard RJ-11 connectors. The splitter has three RJ-11 ports used to connect to the wall jack, the Modem and if desired, a telephone or telephone device.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

Line - This port connects to the wall jack.

ADSL – This port connects to the Modem.

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

The diagram below illustrates the proper use of the splitter.



Line Splitter Installation