



DSL-G604T
Wireless ADSL Router
User's Guide

(Sep. 2005)
DSL604TAUB3
v2.00B02.AU

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.

Warranty and Registration

WARRANTIES EXCLUSIVE

IF THE D-LINK PRODUCT DOES NOT OPERATE AS WARRANTED ABOVE, THE CUSTOMER'S SOLE REMEDY SHALL BE, AT D-LINK'S OPTION, REPAIR OR REPLACEMENT. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. D-LINK NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION MAINTENANCE OR USE OF D-LINK'S PRODUCTS.

D-LINK SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY THE CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLIGENCE, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING OR OTHER HAZARD.

LIMITATION OF LIABILITY

IN NO EVENT WILL D-LINK BE LIABLE FOR ANY DAMAGES, INCLUDING LOSS OF DATA, LOSS OF PROFITS, COST OF COVER OR OTHER INCIDENTAL, CONSEQUENTIAL OR INDIRECT DAMAGES ARISING OUT OF THE INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE OR INTERRUPTION OF A D-LINK PRODUCT, HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY. THIS LIMITATION WILL APPLY EVEN IF D-LINK HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. IF YOU PURCHASED A D-LINK PRODUCT IN THE UNITED STATES, SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

Limited Warranty

Hardware:

D-Link warrants each of its hardware products to be free from defects in workmanship and materials under normal use and service for a period commencing on the date of purchase from D-Link or its Authorized Reseller and extending for the length of time stipulated by the Authorized Reseller or D-Link Branch Office nearest to the place of purchase.

This Warranty applies on the condition that the product Registration Card is filled out and returned to a D-Link office within ninety (90) days of purchase. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card.

If the product proves defective within the applicable warranty period, D-Link will provide repair or replacement of the product. D-Link shall have the sole discretion whether to repair or replace, and replacement product may be new or reconditioned. Replacement product shall be of equivalent or better specifications, relative to the defective product, but need not be identical. Any product or part repaired by D-Link pursuant to this warranty shall have a warranty period of not less than 90 days, from date of such repair, irrespective of any earlier expiration of original warranty period. When D-Link provides replacement, then the defective product becomes the property of D-Link.

Warranty service may be obtained by contacting a D-Link office within the applicable warranty period, and requesting a Return Material Authorization (RMA) number. If a Registration Card for the product in question has not been returned to D-Link, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided. If Purchaser's circumstances require special handling of warranty correction, then at the time of requesting RMA number, Purchaser may also propose special procedure as may be suitable to the case.

After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. The package must be mailed or otherwise shipped to D-Link with all costs of mailing/shipping/insurance prepaid. D-Link shall never be responsible for any software, firmware, information, or memory data of Purchaser contained in, stored on, or integrated with any product returned to D-Link pursuant to this warranty.

Any package returned to D-Link without an RMA number will be rejected and shipped back to Purchaser at Purchaser's expense, and D-Link reserves the right in such a case to levy a reasonable handling charge in addition mailing or shipping costs.

Software:

Warranty service for software products may be obtained by contacting a D-Link office within the applicable warranty period. A list of D-Link offices is provided at the back of this manual, together with a copy of the Registration Card. If a Registration Card for the product in question has not been returned to a D-Link office, then a proof of purchase (such as a copy of the dated purchase invoice) must be provided when requesting warranty service. The term "purchase" in this software warranty refers to the purchase transaction and resulting license to use such software.

D-Link warrants that its software products will perform in substantial conformance with the applicable product documentation provided by D-Link with such software product, for a period of ninety (90) days from the date of purchase from D-Link or its Authorized Reseller. D-Link warrants the magnetic media, on which D-Link provides its software product, against failure during the same warranty period. This warranty applies to purchased software, and to replacement software provided by D-Link pursuant to this warranty, but shall not apply to any update or replacement which may be provided for download via the Internet, or to any update which may otherwise be provided free of charge.

D-Link's sole obligation under this software warranty shall be to replace any defective software product with product which substantially conforms to D-Link's applicable product documentation. Purchaser assumes responsibility for the selection of appropriate application and system/platform software and associated reference materials. D-Link makes no warranty that its software products will work in combination with any hardware, or any application or system/platform software product provided by any third party, excepting only such products as are expressly represented, in D-Link's applicable product documentation as being compatible. D-Link's obligation under this warranty shall be a reasonable effort to provide compatibility, but D-Link shall have no obligation to provide compatibility when there is fault in the third-party hardware or software. D-Link makes no warranty that operation of its software products will be uninterrupted or absolutely error-free, and no warranty that all defects in the software product, within or without the scope of D-Link's applicable product documentation, will be corrected.

TABLE OF CONTENTS

About This User's Guide.....	6
Before You Start	6
Installation Requirements.....	6
INTRODUCTION	8
Router Description and Operation.....	8
Front Panel	11
Rear Panel	12
Wireless LAN Basics	12
About 802.11g Wireless.....	13
HARDWARE INSTALLATION	15
Location	15
Network Connection	15
Choosing the Best Location for Wireless Operation.....	17
Power On Router.....	18
Factory Reset Button.....	18
CONFIGURING THE ROUTER FOR THE FIRST TIME	19
Configuring IP Settings on Your Computer.....	19
Configure IP Settings	20
ACCESSING THE CONFIGURATION MANAGER.....	23
Configure the Router with the Configuration Wizard.....	24
HOME.....	30
Wireless.....	30
WAN Configuration.....	31
WAN Configuration.....	32
LAN Configuration	41
DHCP	42
DNS.....	43
Dynamic DNS	44
ADVANCED CONFIGURATION	45
UPnP	45
Virtual Server	46
LAN Clients	46
SNMP.....	47
Filters	49
Bridge Filters.....	50
Routing.....	50
DMZ.....	51
Firewall	52
RIP	54
PPP.....	54
ADSL	55
ATM VCC.....	56
Wireless Management.....	57
Wireless Performance	60

TOOLS	62
Admin	62
Time	63
Remote Log.....	64
System.....	66
Firmware	67
Miscellaneous.....	68
Test.....	69
STATUS	71
Device Info.....	71
DHCP Clients.....	72
Log	73
Statistics	75
ADSL	76
HELP	78
TECHNICAL SPECIFICATIONS	79
IP ADDRESS SETUP	81
IP CONCEPTS	84
MICROFILTERS AND SPLITTERS	88

About This User's Guide

This manual provides instructions on how to install the DSL-G604T ADSL Router and use it to connect a computer or Ethernet LAN to the Internet.

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

Information you will need from your ADSL service provider:

Username	This is the Username that is used to log on to your ADSL service provider's network. It is commonly in the form – user@isp.com .	Record your info here.
Password	This is the Password that is used, in conjunction with the Username above, to log on to your ADSL service provider's network.	
Connection Protocol	This is the method that your ADSL service provider uses to send and receive data between the Internet and your computer.	
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.	

Information you will need about your DSL-G604T ADSL Router:

Username	This is the Username you will be prompted to enter when you access the DSL-G604T's configuration screens using a Web browser. The default Username is admin .	Record your info here.
Password	This is the Password you will be prompted to enter when you access the DSL-G604T's configuration screens using a Web browser. The default Password is admin .	
LAN IP address for the DSL-G604T	This is the IP address you will enter into the Address field of your Web browser to access the DSL-G604T's configuration screens using a Web Browser. The default IP address is 10.1.1.1 .	
LAN Subnet Mask for the DSL-G604T	This is the subnet mask used by the DSL-G604T, and will be used throughout your LAN. The default subnet mask is 255.0.0.0 .	

Information you will need about your LAN or computer:

Ethernet NIC	If your computer has an Ethernet NIC, you can connect the DSL-G604T to this Ethernet port using an Ethernet cable. You can also use the Ethernet port on the DSL-G604T to connect to other Ethernet devices, such as a Wireless Access Point.	Record your info here.
DHCP Client status	Your DSL-G604T ADSL Router 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 range of IP addresses the DSL-G604T will assign are from 10.1.1.2 to 10.1.1.254 . 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-G604T ADSL Router.

Introduction

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

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. For ADSL services, it is not necessary to install expensive new cabling or condition the line in any way.

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

ADSL provides a dedicated service over a single telephone line operating at speeds of up to 8 Mbps downstream and up to 640 Kbps upstream, depending on local telephone line conditions. A secure point-to-point connection is established between the user and the central office of the service provider. D-Link ADSL devices incorporate the recommendations of the ADSL Forum regarding framing, data format, and upper layer protocols.

Router Description and Operation

The DSL-G604T ADSL Router is designed to provide a simple, cost-effective and secure ADSL Internet connection for your small- to medium-sized private network. The DSL-G604T combines the benefits of high-speed ADSL connection technology and TCP/IP routing with a conventional Ethernet interface in one compact and convenient package. ADSL connection technology enables many interactive multi-media applications such as video conferencing and collaborative computing. The Router is easy to install and use. The DSL-G604T connects to an Ethernet LAN via a standard Ethernet 10BASE-T interface using RJ-45 connectors. The ADSL connection is made using ordinary twisted-pair telephone line with standard RJ-11 connectors. This arrangement means that several PCs can be networked and connected to the Internet using a single WAN interface and IP address.

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. Appendix B provides illustrated examples of how to install two common styles of low pass filters.

Operating Systems

The DSL-G604T 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 Mozilla, Firefox, Opera, Microsoft Internet Explorer® version 5.0, Netscape Navigator® version 4.7, or later versions. The web browser must have JavaScript enabled. JavaScript is enabled by default on many browsers. Make sure JavaScript has not been disabled by other software (such as virus protection or web user security packages) that may be running on your computer.

Ethernet Port (NIC Adapter)

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

Additional Software

It may be necessary to install software on your computer that enables the computer to access the Internet. Additional software must be installed if you are using what is called a “bridged” connection. For a bridged connection, the information needed to make and maintain the Internet connection is stored on your computer, not in the Router. This type of connection is similar to the arrangement used for analogue dial-up modems, but the connection speed is much faster. Various terms are used to describe a bridged ADSL connection including the term “RFC 1483 Bridge” which is used in this guide.

About Bridged Ethernet Connections (RFC 1483)

Using this method, the DSL-G604T acts as a transparent bridge, and is invisible to other devices on both the WAN and LAN side of the bridge. It is therefore necessary to provide some means of acquiring global IP settings for your account.

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, server or 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.

Account Information (User Name and Password)

Most users will need to supply a user name and password used to access the service provider’s network (and ultimately, the Internet). This information is stored either in the Router’s memory or on your computer depending on the type of ADSL connection you have.

ACCOUNT INFORMATION (PPP Connections Only)
User Name:
Password:

Router Features

The D-Link DSL-G604T ADSL Router provides the following features:

- Data rates up to 24 Mbps for downstream and 1Mbps for upstream

- Friendly web-based graphical user interface for configuration and management
- Supports up to eight simultaneous virtual connections for a single ADSL account
- Supports T1.413 issue 2, G.dmt and G.lite for the ADSL standard
- Supports G.dmt.bis and G.lite.bis for the ADSL2 standard
- Supports G.dmt.bisplus for the ADSL2+ standard
- Supports G.992.5 for the ADSL standard
- Auto-handshake and rate adaptation for different ADSL flavours
- Widest range of DSLAM interoperability
- Built-in MIBs for SNMP management
- Upgradeable firmware through HTTP

Packing List

Open the shipping carton and carefully remove all items. In addition to this User's Guide, ascertain that you have:

- One DSL-G604T ADSL2/2+ Modem/Router
- One twisted-pair telephone cable used for ADSL connection
- One CAT-5 Ethernet cable
- One AC power adapter suitable for your electric service
- This Manual on CD ROM
- One Quick Installation Guide

Front Panel

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**, **WLAN Link/Act**, and **Ethernet Link/Act** indicators.

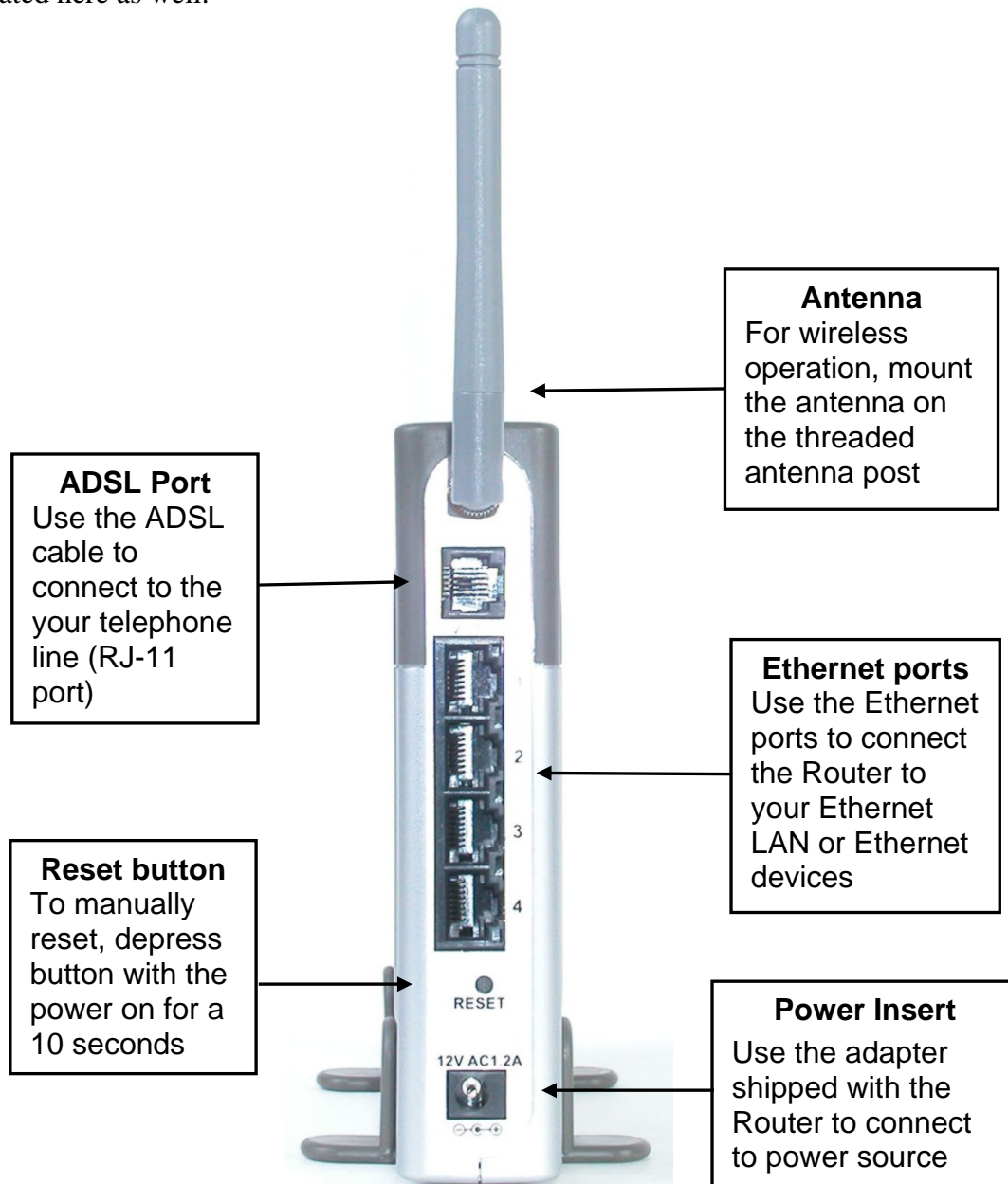


Power	Steady green light indicates the unit is powered on. When the device is powered off this remains dark.
Status	Lights steady green during power on self-test (POST). Once the connection status has been settled, the light will blink green. If the indicator lights steady green after the POST, the system 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.
WLAN (Link/Act)	Steady green light indicates a wireless connection. A blinking green light indicates activity on the WLAN interface.
Ethernet (Link/Act) 1 - 4	A solid green light indicates a valid link on startup. This light will blink when there is activity currently passing through the Ethernet ports.

Rear Panel

Connect the AC power adapter cord and network cables on the rear panel. The power switch and reset button are also located on the back of the device. Connect the antennas to the antenna posts.

All cable connections to the Router are made at the rear panel. The power switch and factory reset button is located here as well.



Wireless LAN Basics

Some basic understanding of 802.11g 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

Wireless LAN or 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. Digital data is 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. See the technical specifications for more details on wireless operation.

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 802.11g 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-G604T 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. By default the DSL-G604T 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. You may disable SSID broadcasting in the web manager's wireless menu.

Wireless Security

Various security options are available on the DSL-G604T including open or WEP, WPA, and WPA-PSK. Authentication may use an open system or a shared key. For details on these methods and how to use them, please read the wireless LAN configuration information in chapters 3 (Basic Router Configuration) and 4 (Advanced Router Configuration) below.

About 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.

Hardware Installation

The DSL-G604T functions on two separate networks, as an Ethernet LAN and as an ADSL WAN. When deciding where to put the Router, the user must take into account the fact that it is connected to these two networks with three types of media. Ethernet cables connect the Router to computers and network devices, Wireless cards connect the computers and network devices to the Router, and the ADSL line connects it to a wall socket. In addition, the device must be near an AC 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

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

Network Connection

Complete the connection to the network through the ADSL port and the Ethernet port on the back of the Router.

Connect ADSL Line

Use the ADSL cable included with the Router to connect it to a telephone wall socket. 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. It is the physical link to the ISP's network backbone and ultimately to the Internet.

Connect Router to Ethernet

The Router may be connected to any 10/100BASE-TX Ethernet LAN. 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 higher than 10Mbps, 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 metres.

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 cross-over cable.

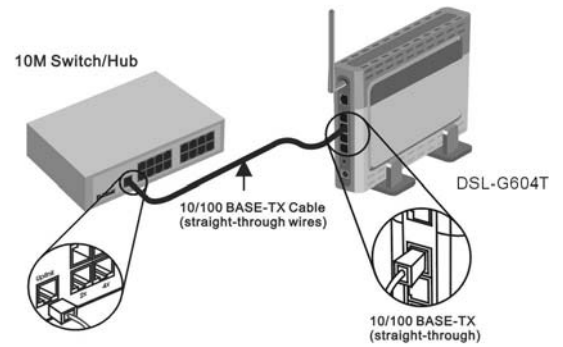


Figure 2- 1. Hub or Switch to Router

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.

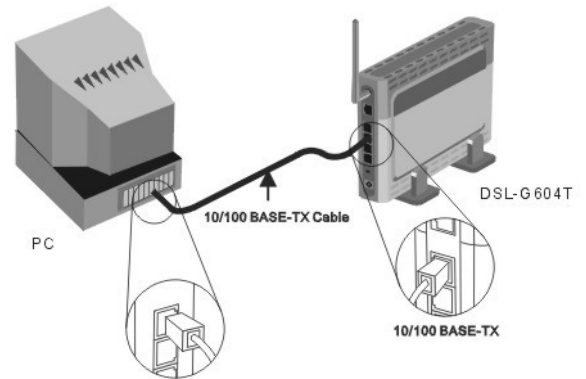
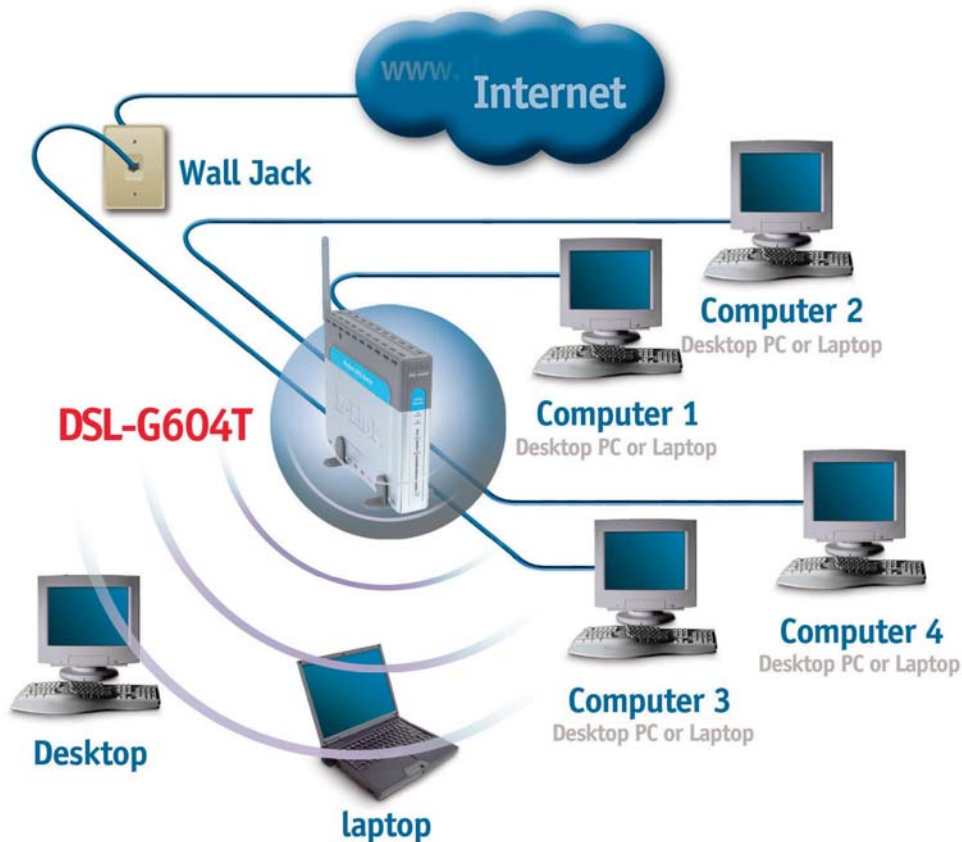


Figure 2- 2. Computer to Router Connection

The illustration below shows the DSL-G604T connected to Ethernet LAN devices, Wireless LAN devices and the Internet.



Choosing the Best Location for Wireless Operation

Many environmental factors can affect the effective wireless function of the DSL-G604T. 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 metres indoors and up to 300 metres 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 signal range. Typical ranges vary depending on the types of materials and background RF noise in your home or business. For optimum 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 minimised.
2. **Consider the direct line between access points and workstations:** A wall that is 0.5 metres thick, at a 45-degree angle appears to be almost 1 metre thick. At a 2-degree angle, it is over 14 metres 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 metres) 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

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 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 10 seconds while the device is powered on. Use a ballpoint pen 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 10.1.1.1 and the subnet mask is 255.0.0.0.

Configuring the Router for the First Time

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 the Router configuration including the IP settings. 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. This chapter discusses the steps to first establish the WAN connection. The remaining features, not directly concerned with establishing the initial connection, are explained in Chapter 4, *Web-based Management*.

It is recommended that you install and configure the Router using one non-networked computer. This allows you to verify that the ADSL service is functioning and that you are able to communicate with the device. Once the initial ADSL connection is established, you can proceed to build an Ethernet LAN around the device or incorporate it into an existing LAN.

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 “neighbourhood” 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 of the computer. 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

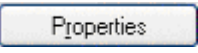
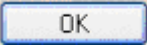
In order to configure your system to receive IP settings from the Router it must first have the TCP/IP protocol installed. If you have an Ethernet port on your computer, it probably already has TCP/IP protocol installed. If you are using Windows XP the TCP/IP is enabled by default for standard installations. 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.

Configure IP Settings





You must now enable your computer to access the Router's configuration software. To do this you will need to configure the IP settings on your computer. Follow these instructions to configure the IP settings for the operating system installed on your computer.

Windows XP


1. In the Windows task bar, click the Start button, and then click **Control Panel**.
2. Double-click the Network Connections icon.
3. In the LAN or High-Speed Internet window, right-click on icon corresponding to your network interface card (NIC) and select **Properties**. (This icon may be labelled *Local Area Connection*).
4. The Local Area Connection dialog box displays with a list of currently installed network items.
5. Make sure that the check box to the left of the item labelled Internet Protocol TCP/IP is checked, and click .
6. In the Internet Protocol (TCP/IP) Properties dialog box, click the button labelled **Use the following IP address**:
7. Type in IP settings as follows, IP address: **10.1.1.2** and Subnet mask: **255.0.0.0**.
8. Click  twice to confirm your changes, and close the Control Panel.


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 to step 3.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click .
6. In the Select Network Component Type dialog box, select **Protocol**, and then click .
7. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click .
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  to restart your computer with the new settings.

Next, configure IP information:


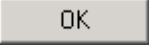
1. In the Control Panel, double-click the Network and Dial-up Connections icon.
2. In Network and Dial-up Connections window, right-click the Local Area Connection icon, and then select **Properties**.
3. In the Local Area Connection Properties dialog box, select **Internet Protocol (TCP/IP)**, and then click .
4. In the Internet Protocol (TCP/IP) Properties dialog box, click the button labelled **Use the following IP address**:
5. Type in IP settings as follows, **IP address: 10.1.1.2** and Subnet mask: **255.0.0.0**.

6. Click  twice to confirm and save your changes, and then close the Control Panel.






Windows Me

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 on the Network icon, 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 to step 3.
5. If Internet Protocol (TCP/IP) does not display as an installed component, click .
6. In the Select Network Component Type dialog box, select **Protocol**, and then click .
7. Select **Microsoft** in the Manufacturers box.
8. Select **Internet Protocol (TCP/IP)** in the Network Protocols list, and then click .
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  to restart your computer with the new settings.


Next, configure the IP information:


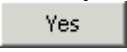
1. In the Control Panel, double-click the Network and Dial-up Connections icon.
2. In Network and Dial-up Connections window, right-click the Network icon, and then select **Properties**.
3. In the Network Properties dialog box, select **TCP/IP**, and then click .
4. In the TCP/IP Settings dialog box, click the **Specify IP address** option.
5. Type in IP settings as follows, **IP address: 10.1.1.2** and **Subnet mask: 255.0.0.0**.
6. Click  twice to confirm and save your changes, and then close the Control Panel.

Windows 95, Windows 98 and Windows 98SE


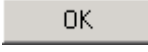
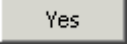
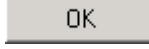
1. First, check for the IP protocol and, if necessary, install it:
2. In the Windows task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
3. Double-click the Network icon.
4. The Network dialog box displays with a list of currently installed network components. If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

Next, configure the IP information:


1. Open the Control Panel window, and then click the Network icon.
2. Select the network component labelled TCP/IP, and then click .


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 **Specify an IP address** option.
6. Type in IP settings as follows, **IP address: 10.1.1.2** and Subnet mask: **255.0.0.0**.
7. Click  twice to confirm and save your changes.
8. You will be prompted to restart Windows.
9. Click .

Windows NT 4.0

1. First, check for the IP protocol and, if necessary, install it:
2. In the Windows NT task bar, click the Start button, point to **Settings**, and then click **Control Panel**.
3. In the Control Panel window, double click the Network icon.
4. In the Network dialog box, click the Protocols tab.
5. 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 step 3.
6. If TCP/IP does not display as an installed component, click .
7. In the Select Network Protocol dialog box, select **TCP/IP**, and then click .
8. You may be prompted to install files from your Windows NT installation CD or other media. Follow the instructions to install the files.
9. 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.
10. Click  to continue, and then click  if prompted to restart your computer.

Next, configure the IP information:

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 .
4. In the Microsoft TCP/IP Properties dialog box, click the **Specify an IP address** option.
5. Type in IP settings as follows, **IP address: 10.1.1.2** and Subnet mask: **255.0.0.0**.

Click  twice to confirm and save your changes, and then close the Control Panel.

Accessing 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, **10.1.1.1** in the address bar of the browser. The URL in the address bar should read: **http://10.1.1.1**. Once entered, the user will be prompted to enter the username and password to access the Configuration Manager, as show below. A new window will appear and you will be prompted for a user name and password to access the web-based manager. Use the default user name “admin” and password “admin” for first time setup. You should change the web-based manager access 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 Router 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.



Figure 3-1. Enter Network Password dialog box.

Configure the Router with the Configuration Wizard

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

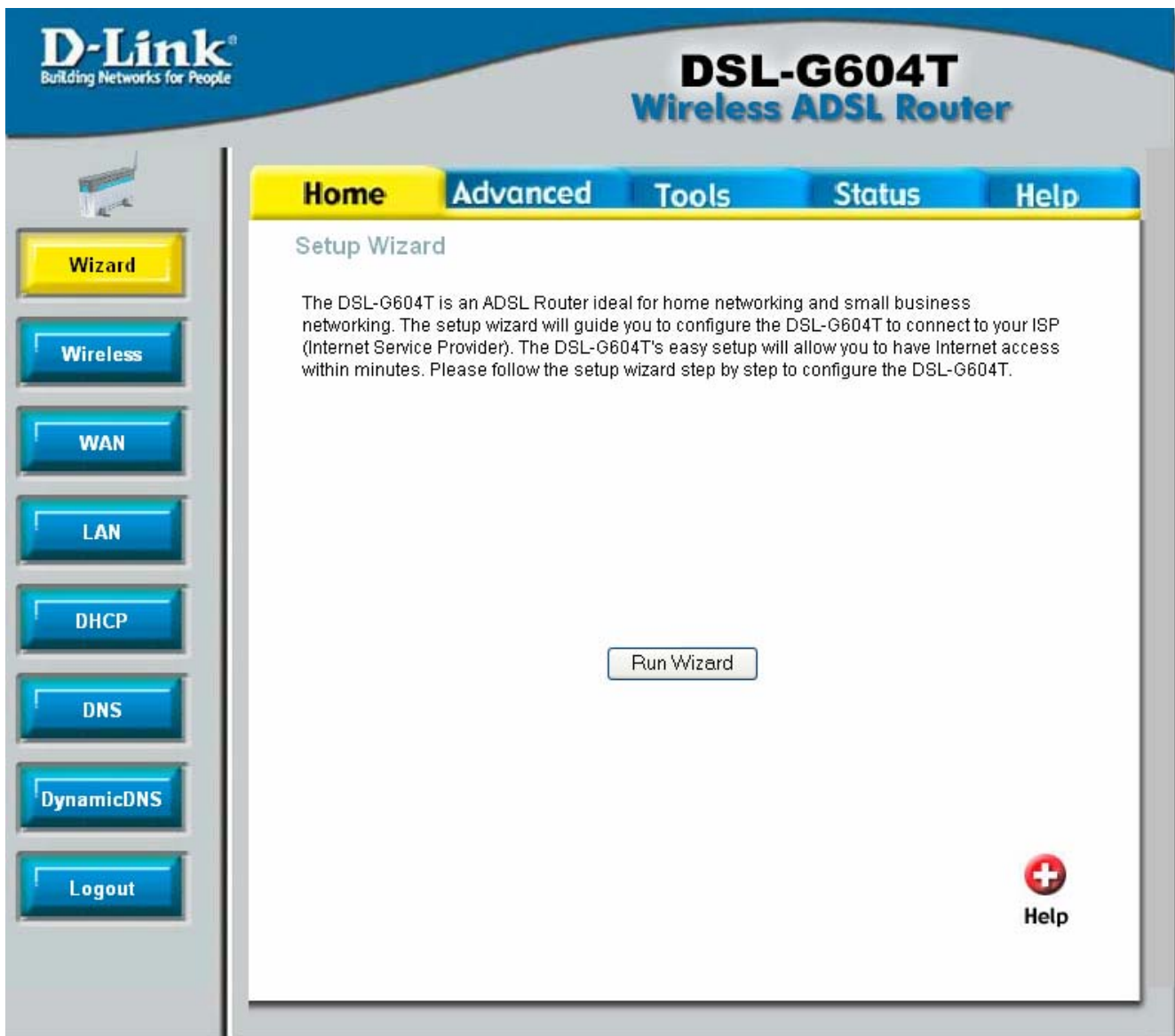


Figure 3-2. Home – Setup

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 modems owned by your service provider. These computers and modems then provide access to the Internet. The Router must be configured to communicate with the systems that give it access to the larger network. The quickest way for you to connect to the Internet is by using the **Setup Wizard**. Click the **Run Wizard** button the following window will appear:

The **Setup** window has four options listed, which will run through in the order given. Each step will be explained in detail. Click **Next** to access Step 1. You may click **Back** during the Setup procedure to return to the previous screen in the Setup Wizard, or **Exit** to exit the Setup Wizard at any time during the procedure.

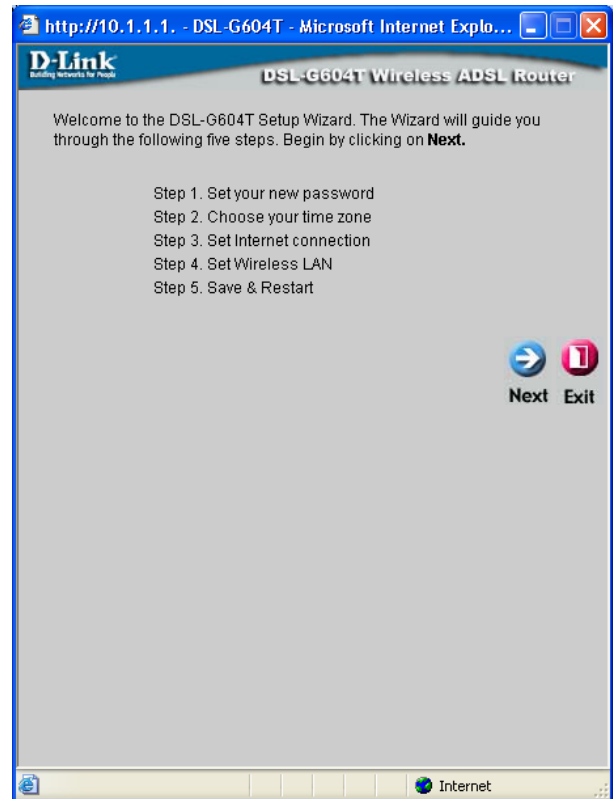


Figure 3-3. Opening Setup window

Step 1: Set your new Password

In Step 1, you must choose a new password to access the Web Interface with. Once you have entered the appropriate password click **Next** to go on to Step 2.

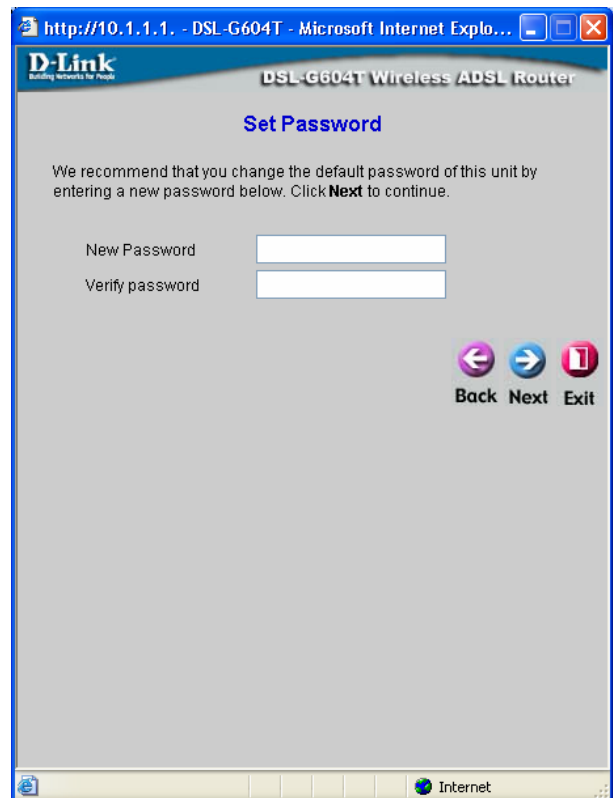


Figure 3-4. Set Password window

Step 2: Setting the Time Zone

In Step 2, you must choose the time zone that best corresponds to the area you are living in by using the pull down menu. Choose the appropriate setting and click **Next** to go on to Step 3.

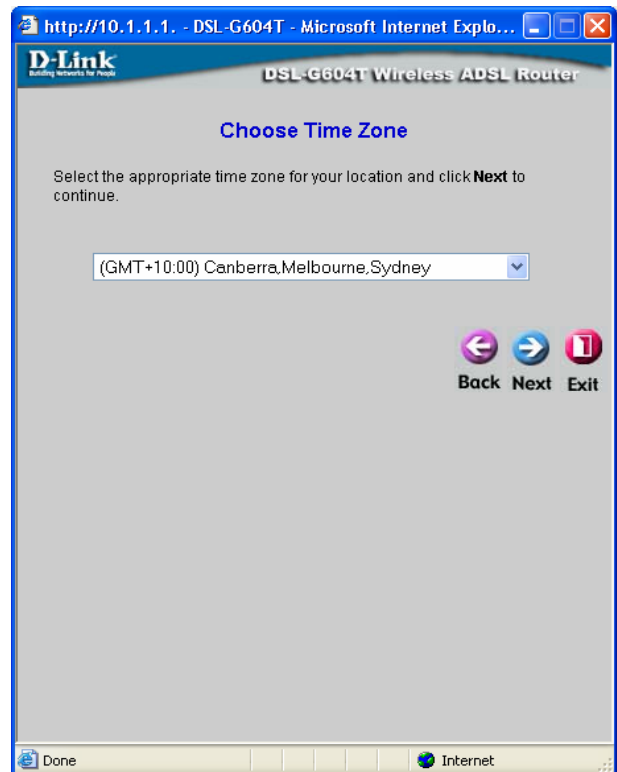


Figure 3-5. Set Time Zone window

Step 3: PPPoE/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, and they involve an authentication process that requires a username and password to gain access to the network. PPPoE (Point to Point Protocol over Ethernet), as described in RFC 2516, is a method of using PPP through the Ethernet network. PPPoA (Point to Point Protocol over ATM) configuration requires the same basic information as the previously discussed PPPoE and both configuration menus are identical. To configure the connection for PPPoE/PPPoA, perform the steps listed below. After setting the values listed, click the **Next** button to go to Step 4 of the Configuration Wizard.

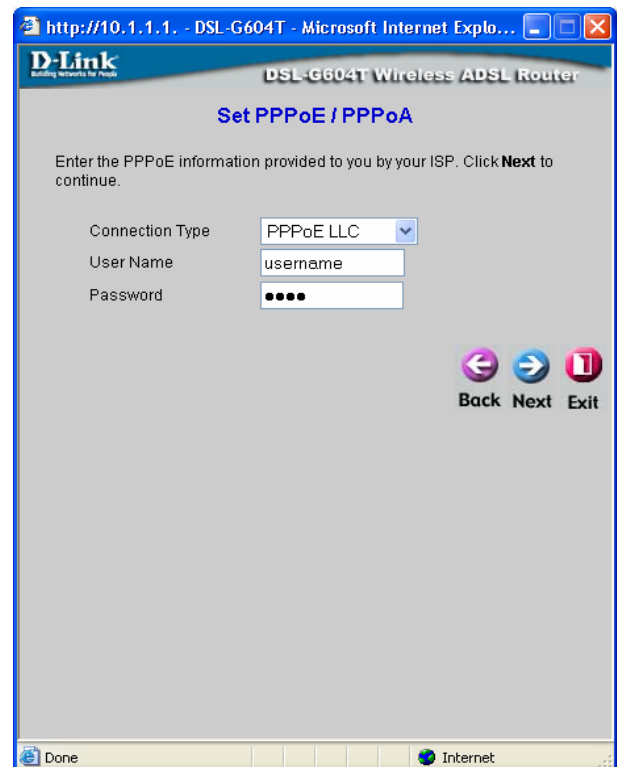


Figure 3-6. Set PPPoE window

VPI/VCI	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.
Username & Password	Type the Username and Password used to verify the identity of your account. Typically, the Username is an account number assigned by your ISP. See your ISP for further information.
Connection Type	Choose between PPPoE LLC , PPPoA LLC or PPPoE VC-Mux depending on the instructions of your ISP.

Step 4: Set Wireless LAN Connection

To set the Wireless LAN connection, we need to enable the Wireless LAN feature. Click on the “Enable Wireless LAN” box then click **Next**. If you do not want to setup a wireless connection at this time click the **Next** button to go to Step 5 of the Configuration Wizard.

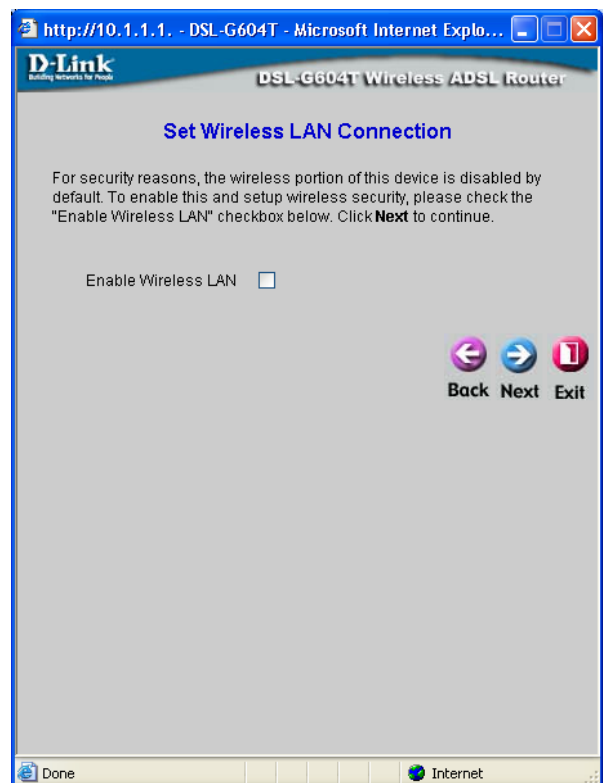


Figure 3-7. Set Wireless Configuration window

Step 4-1: Set Wireless LAN Connection

To configure the Wireless LAN Connection, enter the SSID and the Channel number to be used for the Wireless LAN. The **SSID** can be changed to suit your wireless network. Remember that any wireless device using the access point must have the same SSID and use the same channel. The SSID must be a continuous character string (i.e. no spaces) of up to 16 characters in length. The **Channel** may be changed to channels that are available in your region. Channels available for Wireless LAN communication are subject to regional and national regulation. It is recommended to setup some form of security in order to keep your network safe from unwanted connections. We advise that you use a minimum of 64/128 bit WEP. Click **Next** to go to step 5 of the Configuration Wizard.

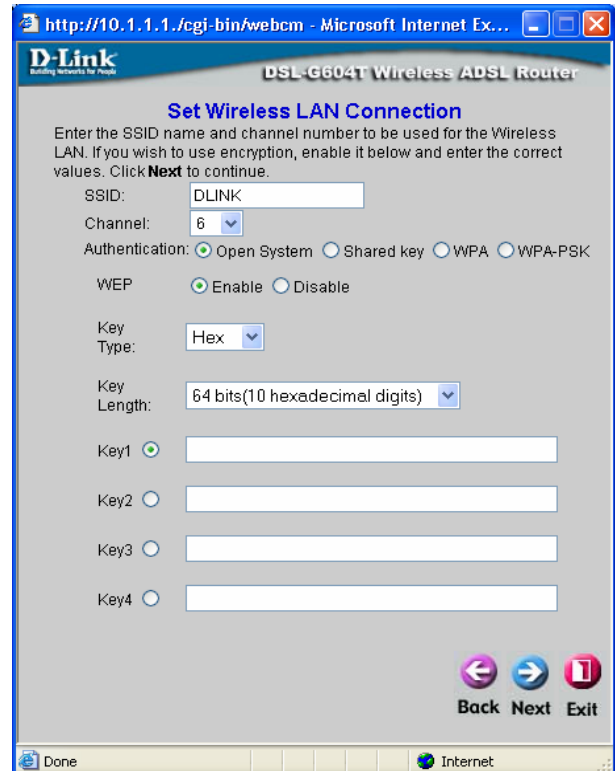


Figure 3-8. Set Wireless Configuration window

Step 5: Setup Completed

In the following window, you must restart the system to save the settings implemented or go back to choose another option to configure.

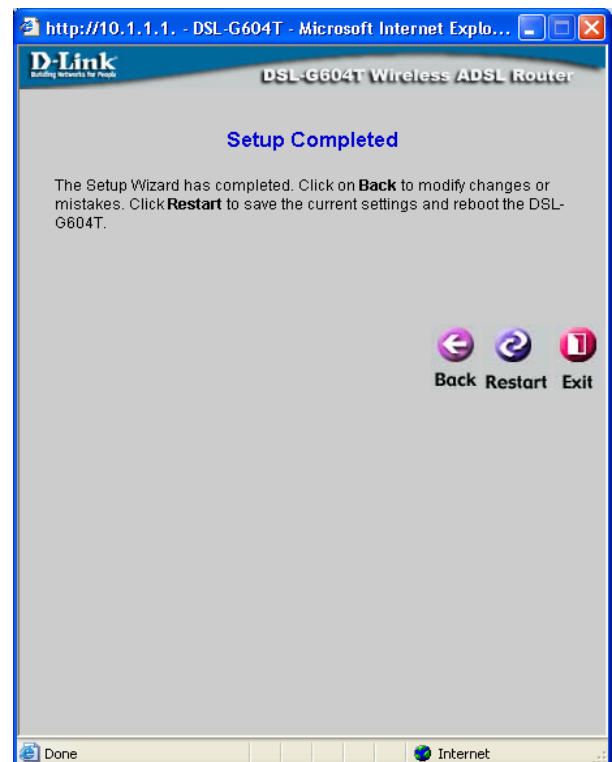


Figure 3-9. Setup Completed window

Home

This tab in the Web Manager will allow the user to set up various configurations in order to connect your Router to the Internet. Much of the information necessary in these screens must be supplied to you by your ISP. Remember to use the key words in bold when asking your ISP for information. This will make your ISP's job easier and therefore your configuration of the modem, much simpler and quicker. Screens to configure under the **Home** tab include **Wireless**, **WAN**, **LAN**, **DHCP**, **DNS**, and **Dynamic DNS**.

Wireless

Click on the **Wireless** link in the **Home** menu to view the window displayed below. To view information about wireless management and wireless performance please see chapter 5. The three essential settings for wireless LAN operation are the **SSID**, **Channel** and **Security**.

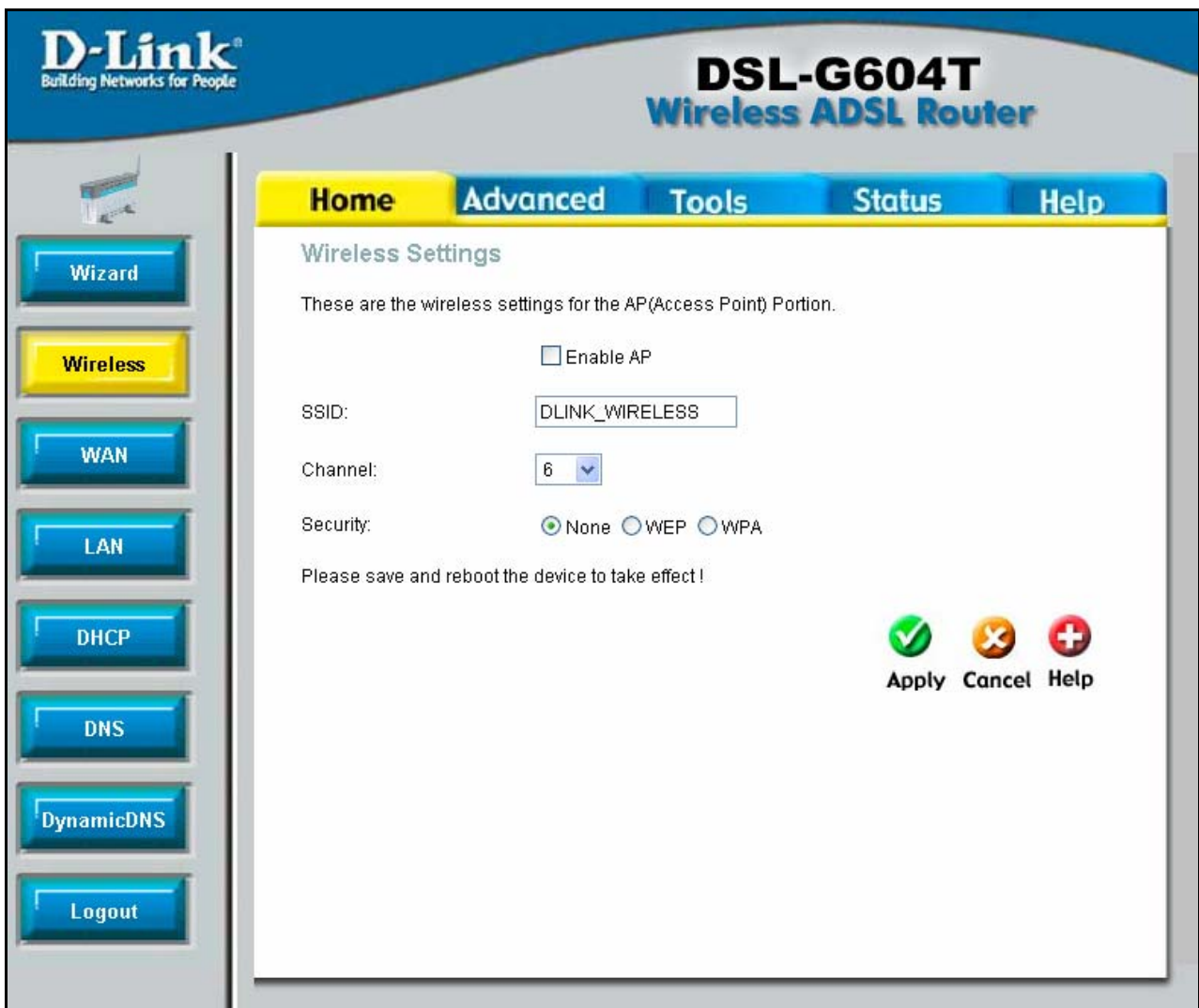


Figure 4- 1. Wireless window

Configure Basic Wireless Settings

Follow the instructions below to change basic wireless settings.

1. **To disable the wireless interface:** click in the **Enable AP** check box to remove the check mark and click the **Apply** button. This will immediately disable the wireless access point, it is not necessary to restart the access point to make this change.
2. **If the wireless interface has been disabled:** click the **Enable AP** check box to place a check mark in it. Click the **Apply** button. It is not necessary to restart the access point unless you have also changed the channel or SSID.
3. The **SSID** can be changed to suit your wireless network. Remember that any wireless device using the access point must have the same SSID and use the same channel. The SSID can be a continuous character string (i.e. no spaces) of up to 16 characters in length. To disable SSID sharing, use the Advanced Wireless Setup menu (see next chapter). Click the **Apply** button to save any change to the SSID.
4. The **Channel** may be changed to channels that are available in your region. Channels available for wireless LAN communication are subject to regional and national regulation. Click the **Apply** button to save any change to the Channel.
5. The options for **Security** include None, WEP and WPA.
 - If **None** is selected, wireless transmissions will not be protected.
 - **WEP** (Wireless Encryption Protocol or Wired Equivalent Privacy) 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. Decryption of the data contained in each packet can only be done if the both the receiver and transmitter have the correct key.
 - **WPA** (Wi-Fi Protected Access) security for wireless communication has been developed to overcome some of the shortcomings of WEP. WPA combines the key generation of WEP with the authentication services of a RADIUS (802.1x) server.

WAN Configuration

WAN is short for Wide Area Network. The WAN settings can be referred to as the Public settings. All IP information in the WAN settings is public IP addresses, which is accessible on the Internet. There are 8 PVCs pre-configured on this modem and upon initial connection, the appropriate settings should automatically be set for you. Altering any of these fields should only be done if specified by your ISP, who should have all the configuration settings necessary for your connection.

D-Link
Building Networks for People

DSL-G604T
Wireless ADSL Router

Home Advanced Tools Status Help

WAN Settings

Please select the appropriate options to connect to your ISP.

Static IP Address **Choose this option to set static IP information provided to you by your ISP.**

PPPoE/PPPoA **Choose this option if your ISP uses PPPoE/PPPoA. (For most DSL users)**

Bridge Mode **Choose this option if your ISP uses Bridge Mode.**

PPPoE/PPPoA

User Name

Password

Connection Type

MRU bytes

Default Route

Connection Status Disconnected

ATM VC Setting

PVC

VPI

VCI

Virtual Circuit

Apply Cancel Help

Figure 4- 2. Home – WAN window

WAN Configuration

WAN is short for Wide Area Network. The WAN settings can be referred to as the Public settings. All IP information in the WAN settings is public IP addresses, which is accessible on the Internet. There are 8 PVCs pre-configured on this modem and upon initial connection, the appropriate settings should automatically be set for you. Altering any of these fields should only be done if specified by your ISP, who should have all the configuration settings necessary for your connection.

D-Link
Building Networks for People

DSL-G604T
Wireless ADSL Router

Home | Advanced | Tools | Status | Help

Wizard | Wireless | **WAN** | LAN | DHCP | DNS | DynamicDNS | Logout

ATM VC Setting

PVC: Pvc0
VPI: 8
VCI: 35
Virtual Circuit: Enabled
WAN Setting: PPPoE/PPPoA

PPPoE/PPPoA

User Name: username
Password: ●●●●
Connection Type: PPPoE LLC
MTU: 1400 bytes
MRU: 1492 bytes
Default Route: Enabled
NAT: Enabled
Firewall: Enabled
IP Control: Dynamic IP
Static IP: 0.0.0.0

ATM

Service Category: UBR
PCR: kbps
SCR: kbps

Apply Cancel Help

Figure 4- 3. Home – WAN window

ATM VC Setting

The first section of the WAN configuration pages offers fields to set general values for any Virtual Channel chosen for connection to your ISP. This section holds the following fields to configure.

PVC: Leave this set at the default value 1 the first time the Router is set up. The modem has been pre-configured for 8 PVCs. The PVC for you should be enabled when you have made your first connection to the Internet. The configured settings for this can be viewed under the **Status** tab, under **Device Info**.

VPI: If instructed to change this, type in the VPI value for the initial connection.

VCI: If instructed to change this, type in the VCI value for the initial connection.

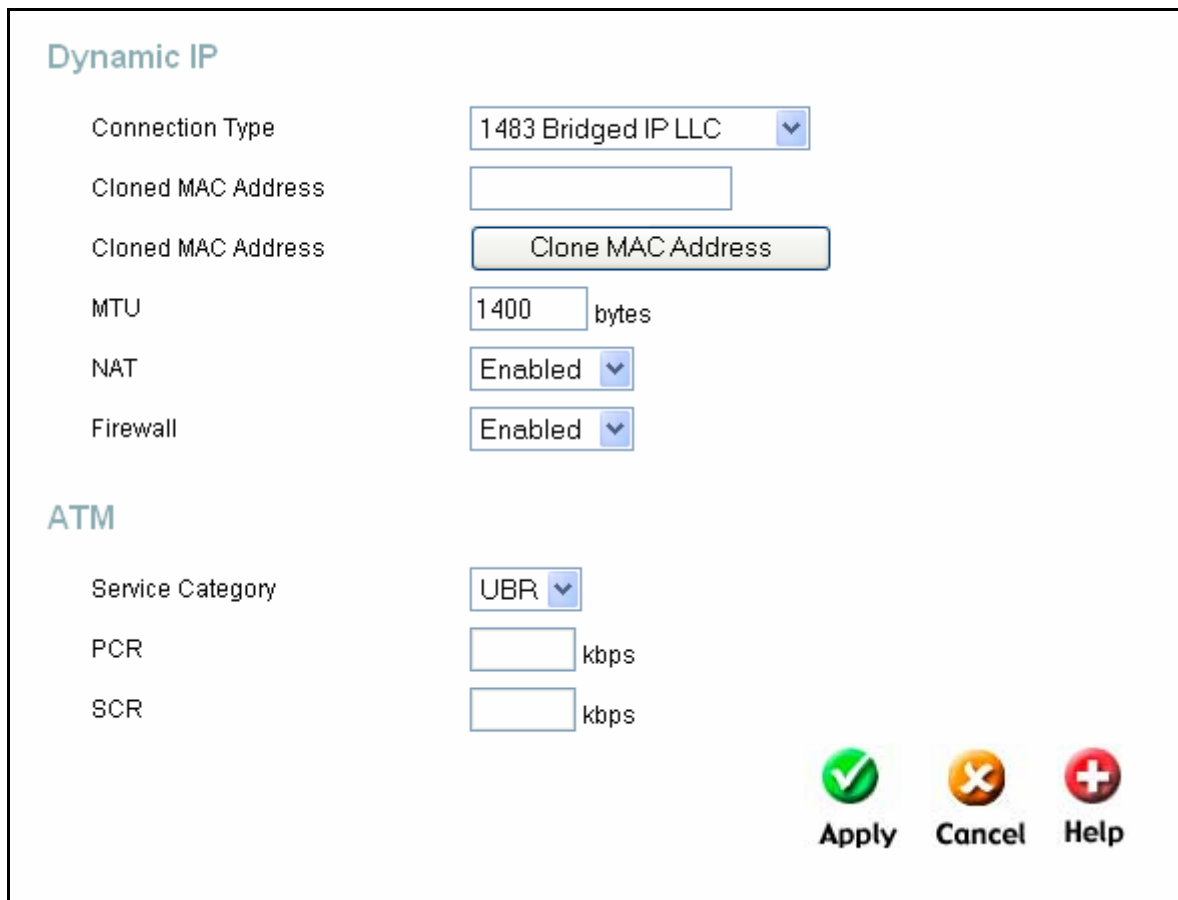
Virtual Circuit: This enables the PVC connection on your modem. Select Enable from the pull down menu to enable the selected PVC.

WAN Settings

The WAN Settings section of this window will allow users to select the type of connection to be used by the router to establish a connection between you and your ISP. Choosing a WAN type will change the window and new settings will appear for the user to configure. The proper selection should be given to you by your ISP.

Dynamic IP Address

Selecting this option in the WAN Settings will change your screen to look like the one seen below. Users choosing this option should have software located on their computer or other networking device to establish a connection between you and your ISP. The Connection Type is chosen by using the pull-down menu. The two choices available to the user here are **1483 Bridged IP LLC** and **1483 Bridged IP Vc-Mux**, and this correct choice should also be provided to you by your ISP. The **Cloned MAC Address** field is used to copy the MAC Address of your Ethernet Adapter to the router. Simply enter the **MAC Address** into the space provided and click the **Clone Mac Address** button. The Maximum Transmission Unit (**MTU**) is a link layer restriction on the maximum number of bytes of data in a single transmission. The default size is 1400 bytes per packet. **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. To enable NAT on the Router, use the pull-down menu and select **Enabled**. The **Firewall** allows the Router to enforce policies to protect against certain kinds of attacks. To enable the firewall on the Router, use the pull-down menu and select **Enabled**.



Dynamic IP

Connection Type: 1483 Bridged IP LLC

Cloned MAC Address:

Cloned MAC Address: Clone MAC Address

MTU: 1400 bytes

NAT: Enabled

Firewall: Enabled

ATM

Service Category: UBR

PCR: kbps

SCR: kbps

Apply Cancel Help

Figure 4- 4. WAN Settings window for Dynamic IP Address

Click **Apply** to set the Dynamic IP settings for your DSL-G604T.

Static IP Address

Selecting this option in the WAN Settings will change your screen to look like the one seen below. A Static IP address is used whenever a known static IP is assigned. The accompanying information such as the Subnet mask, ISP Gateway Address and DNS servers should also be specified in order to be able to connect. These are the servers would enable you to have access to other web servers. Valid IP addresses range from 1.0.0.1 to 255.255.255.255. All information to be entered in this window must be provided to you by your ISP.

Static IP

Connection Type: 1483 Bridged IP LLC ▼

IP Address:

Subnet Mask:

Gateway Address:

Primary DNS Address:

Secondary DNS Address:

MTU: bytes

NAT: Enabled ▼

Firewall: Enabled ▼

ATM

Service Category: UBR ▼

PCR: kbps

SCR: kbps




 **Apply**
 **Cancel**
 **Help**

Figure 4- 5. WAN Settings window for Static IP Address

This window holds the following fields for the user to configure.

Connection Type	This field allows the user to choose the connection type used to connect your router to your ISP. The user may choose between 1483 Bridged IP LLC , 1483 Bridged IP VC-Mux , 1483 Routed IP LLC and 1483 Routed IP VC-Mux . The correct choice should be told to you by your ISP.
IP Address	Enter the IP address based on the information provided to you by your ISP.
Subnet Mask	Enter the Subnet Mask based on the information provided to you by your ISP.
Gateway Address	Enter the Default Gateway based on the information provided to you by your ISP.
Primary DNS Address	This entry is for the IP address of your primary domain name server, which should also be provided to you by your ISP. The router will first try the Primary DNS Address to resolve a website's URL IP address. If this IP address fails, the router will then try the Secondary DNS Address .
Secondary DNS Address	The IP address of the secondary domain name server will be used to resolve a website's URL IP address if the Primary DNS Address fails. The information in this field should also be provided by your ISP.
MTU	The Maximum Transmission Unit (MTU) is a link layer restriction on the maximum number of bytes of data in a single transmission. The default size is 1400 bytes per packet.

NAT	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. Use the pull-down menu to Enable or Disable NAT on the Router
Firewall	The Firewall allows the Router to enforce policies to protect against certain kinds of attacks. To enable the firewall on the Router, use the pull-down menu and select Enabled .

Click **Apply** to set the Static IP address for the DSL-G604T.

PPPoE/PPPoA

Selecting this option in the WAN Settings will change your screen to look like the one seen below. 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, and they involve an authentication process that requires a username and password to gain access to the network. PPPoE (PPP over Ethernet), as described in RFC 2516, is a method of using PPP through the Ethernet network. PPPoA (PPP over ATM) configuration is over ATM and requires the same basic information as the previously discussed PPPoE. Both configuration menus are identical. To configure the connection for PPPoE/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.

PPPoE/PPPoA

User Name:

Password:

Connection Type: ▼

MTU: bytes

MRU: bytes

Default Route: ▼

NAT: ▼

Firewall: ▼

IP Control: ▼

Static IP:

ATM

Service Category: ▼

PCR: kbps

SCR: kbps

Figure 4- 6. WAN Settings window for PPPoE/PPPoA

This window holds the following fields for the user to configure.

Username & Password	Type the Username and Password used to verify the identity of your account. Typically, the Username is an account number assigned by your ISP. See your ISP for further information.
Connection Type	Choose between PPPoE LLC , PPPoA LLC or PPPoE VC-Mux , depending on the instructions of your ISP.
MTU	The Maximum Transmission Unit (MTU) is a link layer restriction on the maximum number of bytes of data in a single transmission. The default size is 1400 bytes per packet. NAT improves network security in effect by hiding the private network behind one global and visible IP address.
MRU	The Maximum Receive Unit (MRU) field indicates the maximum number of bytes that can be received by the Router. This MRU's default size is 1492 bytes per packet. Upon initial negotiation with your ISP, the router will tell the ISP that the amount entered here is the largest packet that can be accepted by the router.
Default Route	Click the corresponding radio button if you wish to enable or disable the Default Route. The Default Route is used for outgoing packets, which have an unresolved IP address. If the router is unable to match the destination address on a received packet with a destination address in the routing table, the router uses the default route.
NAT	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. Use the pull-down menu to Enable or Disable NAT on the Router.
Firewall	The Firewall allows the Router to enforce policies to protect against certain kinds of attacks. To enable the firewall on the Router, use the pull-down menu and select Enabled .
IP Control	This field allows the user to control the WAN IP address of the router. There are three choices for the user: Dynamic IP – Select this option if you wish to have an IP address automatically assigned to the router. Unnumbered IP – Select this option if your ISP has assigned a block of IP addresses for use. Static IP – Select this option if you know the IP address assigned to the router. After selecting this option, the user must enter the known Static IP address in the following field. A Static IP address is used whenever a known static IP is assigned.
Static IP	This field states the Static IP Address of the Router can only be configured when Static IP is chosen in the previous field.

Click **Apply** to implement the PPPoE settings for the DSL-G604T.

Bridge Mode

Selecting this option in the WAN Settings will change your screen to look like the one seen below.

Bridge Mode is for users who have software on their computer or other network device to accept the connection from your ISP. The **Connection Type** setting is selected by using the pull-down menu. The two choices available to the user here are **1483 Bridged IP LLC** and **1483 Bridged IP Vc-Mux**, and this correct choice should be provided to you by your ISP.

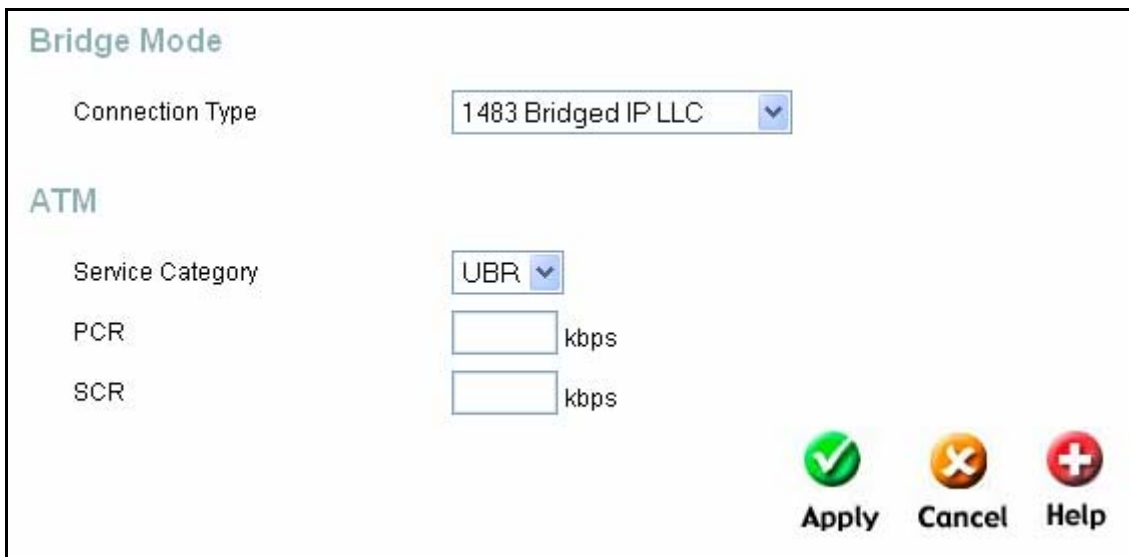


Figure 4- 7. WAN Settings window for Bridge Mode

Click **Apply** to implement the Bridge Mode settings for the DSL-G604T.

ATM

This section of the WAN window allows the user to adjust ATM Quality of Service (QoS) or traffic parameters to suit specific traffic requirements. For applications or circumstances where packet loss or packet delay are a concern, ATM QoS can be adjusted to minimize problems. For most accounts, it will not be necessary to change these settings. Altering QoS settings can adversely affect performance of some commonly used Internet applications.

If you plan to change QoS or traffic parameters, contact your ISP or network services provider for information on what types of adjustment are available or possible for your account. Your ISP may not support the class of service you want to use.

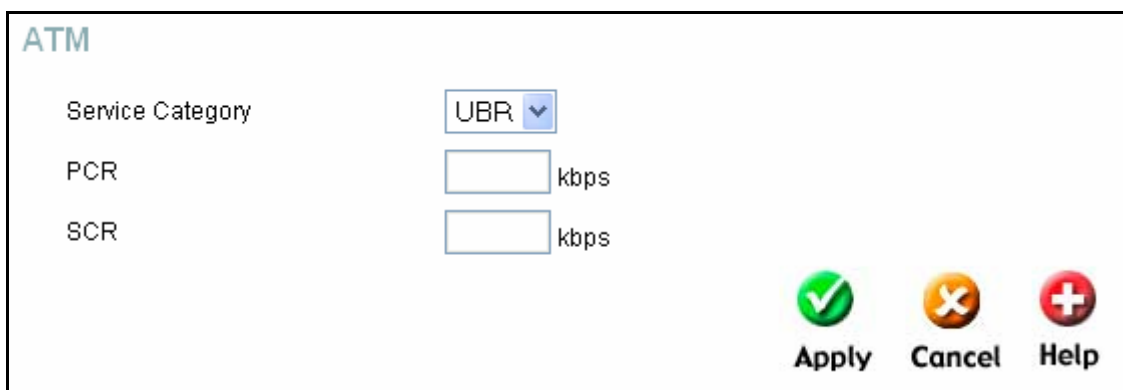


Figure 4- 8. ATM settings for the WAN interface

Service Category: This field represents the QoS (Quality of Service) feature for the ADSL router. The choices available from the pull down menu include UBR (Unspecified Bit Rate), CBR (Constant Bit Rate) and VBR (Variable Bit Rate). These values should already be set for you and should not be changed unless specified by your ISP.

- **UBR** – Unspecified Bit Rate, this is the default category used for general-purpose Internet traffic where normal levels of packet loss and delay are acceptable. For some applications or for multiple connection accounts, it may be desirable to specify the PCR.

- **CBR** – Constant Bit Rate, usually used in circumstances where very low packet loss and very low Cell Delay Variable (CDV) are desirable.
- **VBR** – Variable Bit Rate, usually used when network traffic is characterized by bursts of packets at variable intervals, and some moderate packet loss and delay is acceptable. This category is typically used for audio and video applications such as teleconferencing. The network must support QoS Class 2 to use VBR.

PCR: PCR (Peak Cell Rate) refers to the Bandwidth control on your ADSL router. This field allows you to enter a value representing the maximum bps (bits per second) the ADSL router can receive. This field is limited by the stream coming from your ISP.

SCR: SCR (Sustained Cell Rate) refers to the Bandwidth control on your ADSL router. This field allows you to enter a value representing the minimum bps (bits per second) the ADSL router can receive. After making the changes to this screen, click **Apply** to let your changes take effect.

LAN Configuration

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DSL-G604T and may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

IP Address: The IP address of the LAN interface. The default IP address is 10.1.1.1.

Subnet Mask: The subnet mask of the LAN interface. The default subnet mask is 255.0.0.0.

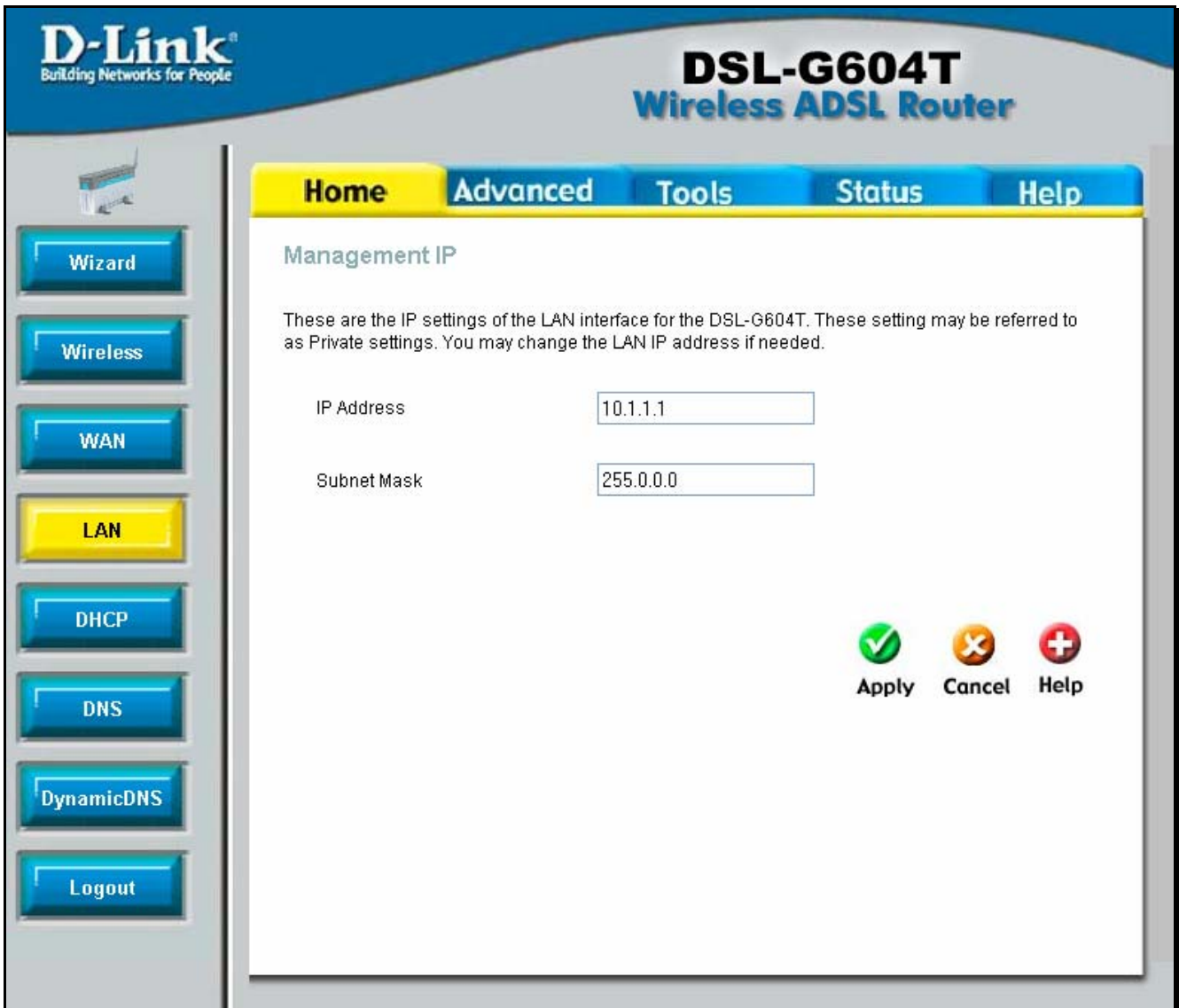


Figure 4- 9. LAN Settings window

Click **Apply** to implement changes made to this window.

DHCP

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. If DHCP is not enabled on the Router, it is necessary for the user to assign a static IP address at each computer on your LAN.

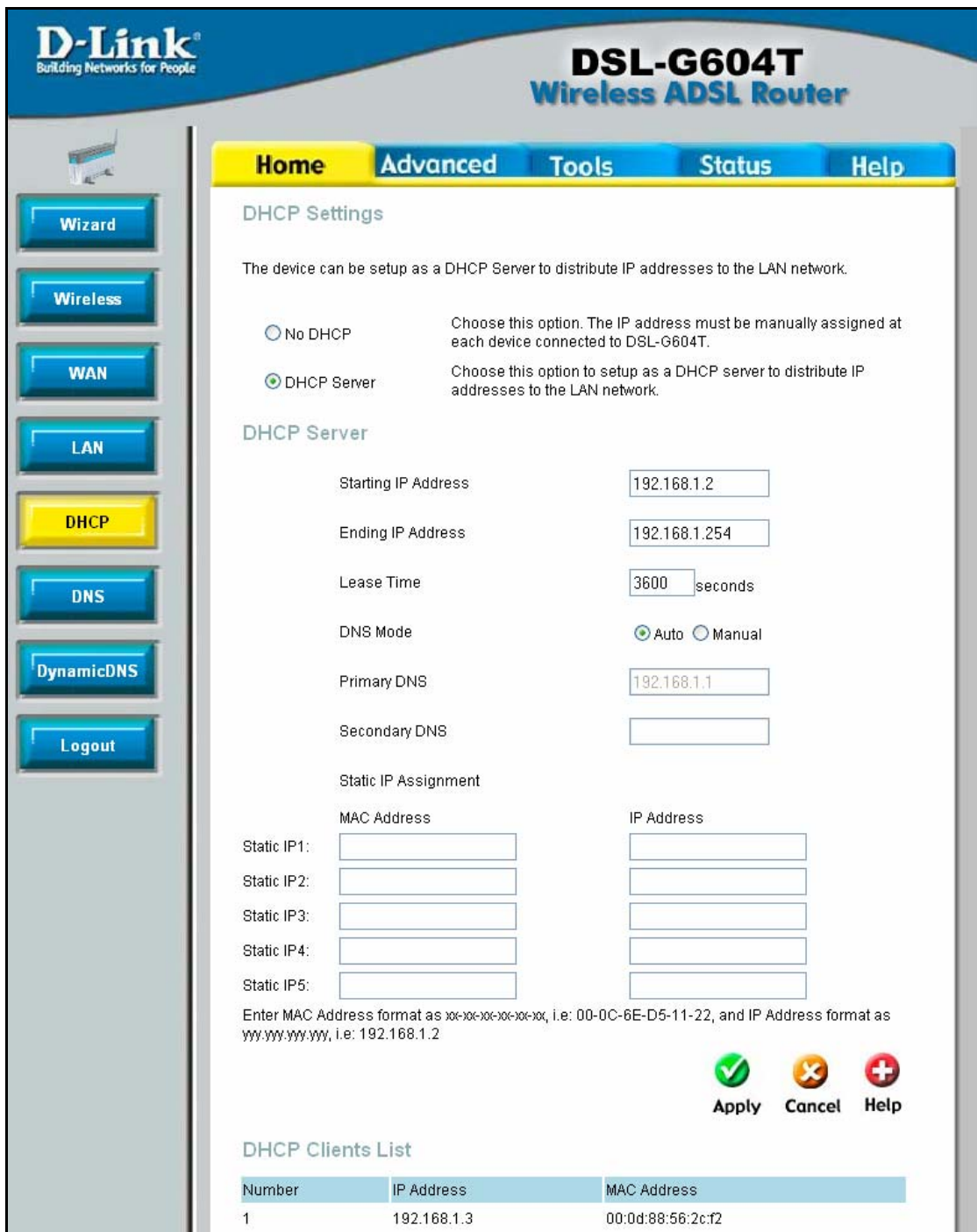


Figure 4- 10. DHCP configuration window

To setup DHCP for your LAN, first enable the Router as a DHCP server by clicking the corresponding **DHCP Server** radio button in the window above and enter the **Starting IP Address** and **Ending IP address** to create a pool of IP addresses to be assigned to other end nodes (computers, routers, etc.) on the LAN. The **Lease Time** field is the time the Server will set for devices using DHCP to re-request an IP Address. When using the Router in DHCP mode you may also configure **DNS** settings for the LAN. Click the **DNS Mode** radio button to auto to allow the Router to automatically relay DNS settings to properly configured DHCP clients. Click Manual to manually enter the Primary and Secondary DNS IP addresses. When the Router has been enabled as DHCP Server the administrator of the server can assign a **Static IP** address to each computer on the LAN from the workstation where the DCHP server has been enabled. To assign a Static IP address to a computer on the LAN, enter the IP and MAC address in the Static IP Assignment field. Click **Apply** to implement information set in this table.

DNS

DNS or Domain Name Server is a system that translates Domain Names into IP addresses. Setting up a DNS will allow the router to contact the DNS to ask it to translate and find a web site you have entered. The following window allows you to set two DNS servers by their IP addresses and these IP addresses should be supplied to you by your ISP.

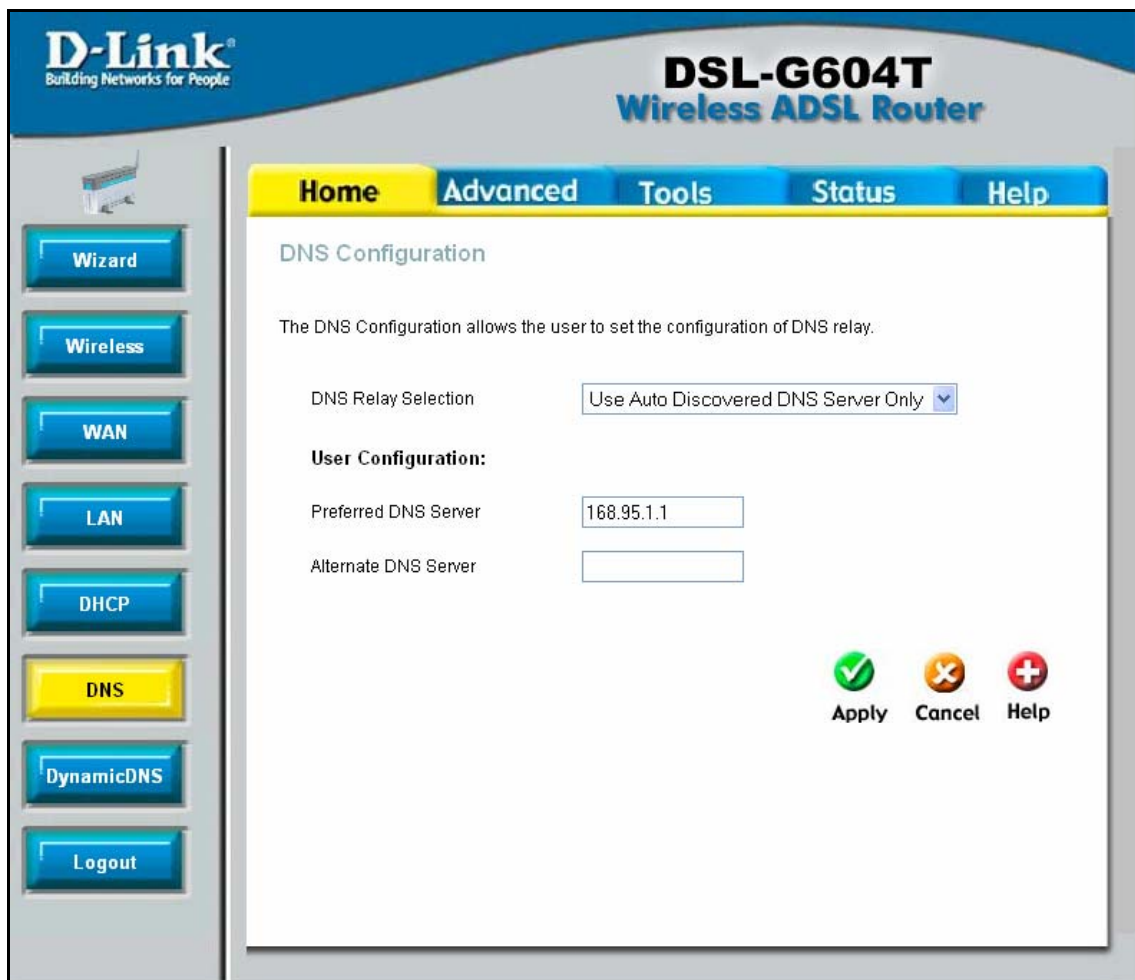


Figure 4- 11. DNS window

To configure the DNS for the Router, use the DNS Relay Selection pull down menu to select the DNS configuration for the router. There are three choices:

- **Disable DNS** – Selecting this option will disable the DNS function of your router.
- **Use Auto Discovered DNS Server Only** – This choice will enable the router to automatically find the DNS Server for your setup.
- **Use User Discovered DNS Server Only** – This choice will enable the DNS Servers entered in the Preferred DNS Server and Alternate DNS Server fields. These two IP addresses must be stated to you by your ISP.

The router will first try the **Preferred DNS Server** to resolve a website’s URL IP address. If that IP address fails to resolve the URL, the Router will then try the **Alternate DNS Server**. Your ISP must provide this information to you. Click **Apply** to set the DNS configurations into the memory of the Router.

Dynamic DNS

The Router supports DDNS, a service that maps Internet domain names to IP addresses. DDNS serves a similar purpose to DNS in that DDNS allows anyone hosting a Web or FTP server to advertise a public name to prospective users. Unlike DNS that only works with static IP addresses, DDNS works with dynamic IP addresses, such as those assigned by an ISP or other DHCP server. DDNS is popular with home network users, who typically receive dynamic, frequently-changing IP addresses from their service provider. To use DDNS, one simply signs up with a provider and installs network software on their host to monitor its IP address. Please see your ISP for further information.

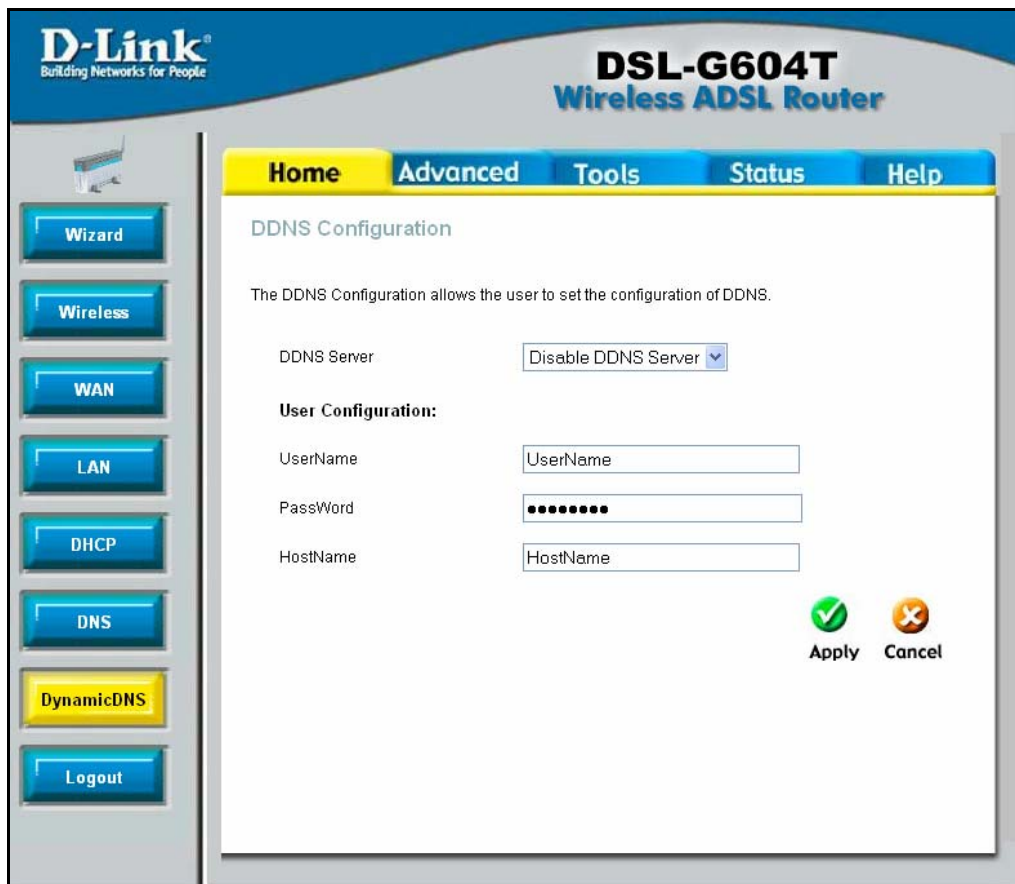


Figure 4- 12. Dynamic DNS window

Advanced Configuration

The **Advanced** tab has fifteen windows for you to view and configure: **UPnP**, **Virtual Server**, **LAN Clients**, **SNMP**, **Filters**, **Bridge Filters**, **Routing**, **DMZ**, **Firewall**, **RIP**, **PPP**, **ADSL**, **ATM VCC**, **Wireless Management**, and **Wireless Performance**.

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, Firewall, phone line and power line networking.

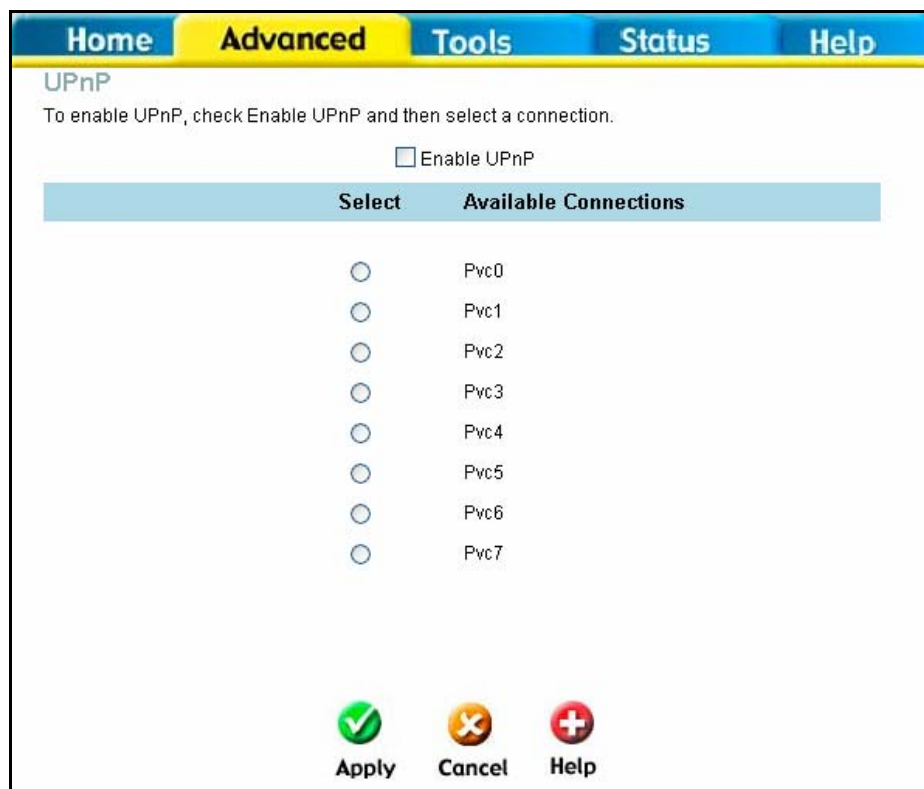


Figure 5- 1. UPnP window

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.

Virtual Server

To view the following window, click on the **Advanced** tab at the top of the window and then click the **Virtual Server** button to the left. The **Virtual Server** will allow remote users access to various services outside of their LAN through a public IP address, such as FTP (File Transfer Protocol) or HTTPS (Secure Web). Select a connection type and enter an IP address for the virtual server. After configuring the Router for these features, the Router will redirect these external services to an appropriate server on the users' LAN. To choose a particular service click a radio button from the category list and highlight the service from the Available Rules list. Click **Add**, and then reboot to apply the rule.

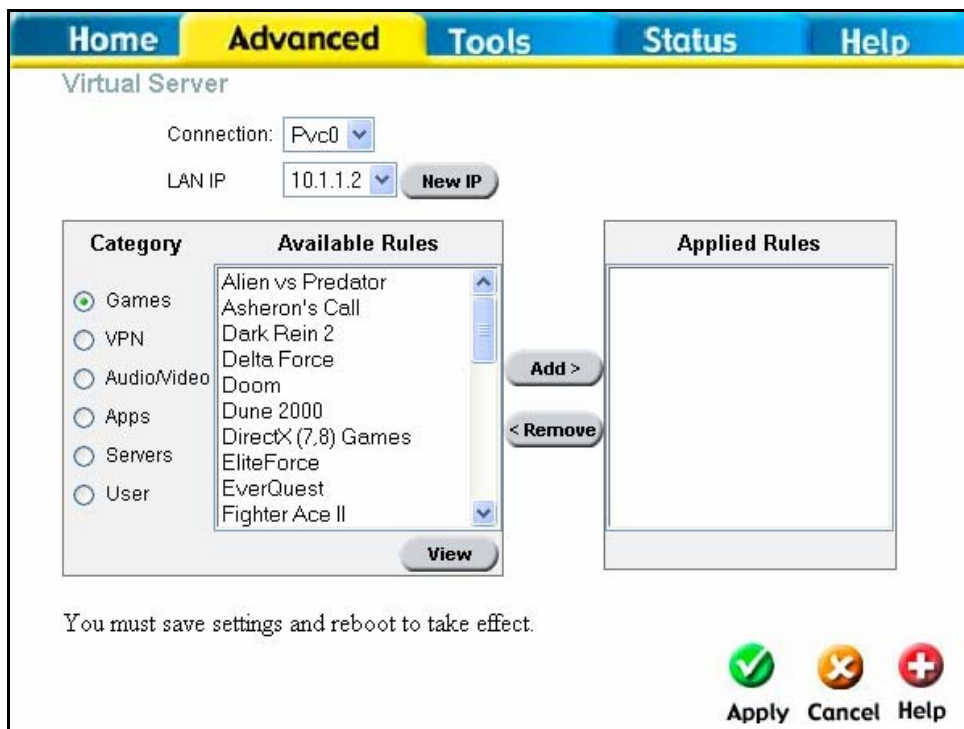
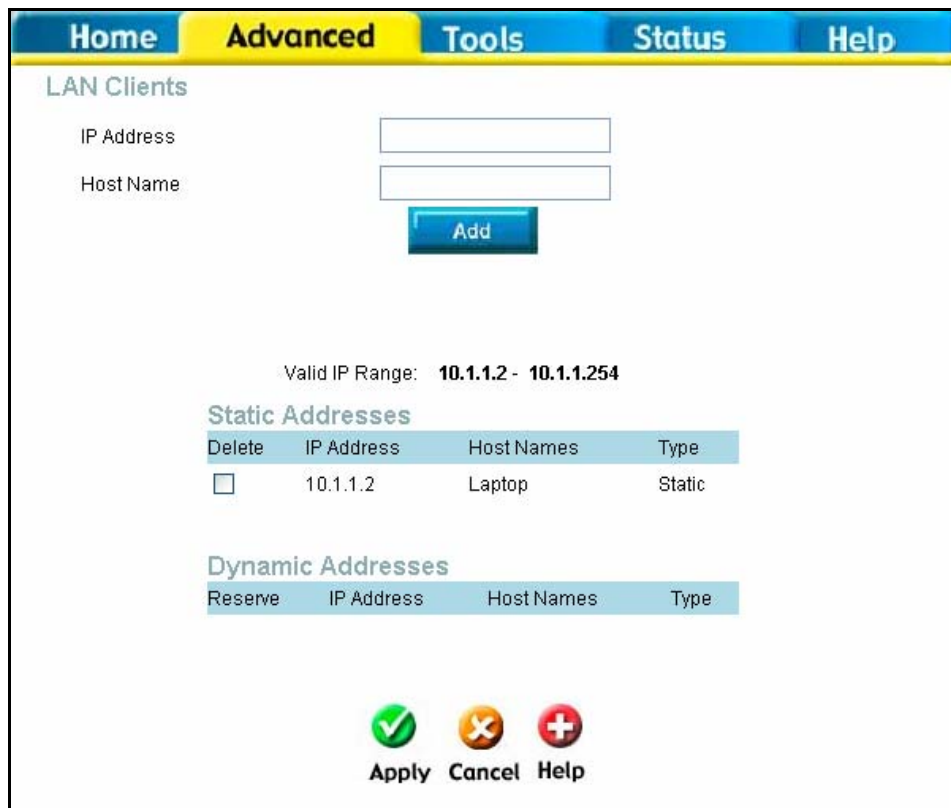


Figure 5- 2. Virtual Server window

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.



LAN Clients

IP Address

Host Name

Valid IP Range: **10.1.1.2 - 10.1.1.254**

Static Addresses

Delete	IP Address	Host Names	Type
<input type="checkbox"/>	10.1.1.2	Laptop	Static

Dynamic Addresses

Reserve	IP Address	Host Names	Type
---------	------------	------------	------

Figure 5- 3. LAN Clients Window

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 10.0.0.1 to 10.255.255.254. 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 LAN IP address for the device does not expire. This will create a permanent entry for the device in the ARP table and in effect, it becomes a static IP address. Click to check the **Reserve** box for the address or addresses you want to reserve and click the **Apply** button. These reserved addresses will no longer be available for DHCP assignment and will be listed in the Static IP Addresses table.

SNMP

This menu can be accessed directly by clicking on the **SNMP** button or hyperlink in the **Advanced** setup menu. Simple Network Management Protocol (SNMP) is an OSI Layer 7 Application designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, performance monitoring, and detection of potential problems in the Router or network.

Home	Advanced	Tools	Status	Help
SNMP Management				
<input type="checkbox"/>	Enable SNMP Agent			
<input type="checkbox"/>	Enable SNMP Traps			
Name:	<input type="text" value="DSL-G604T"/>			
Location:	<input type="text" value="DLink"/>			
Contact:	<input type="text" value="support@dlink.com"/>			
Vendor OID: 1.3.6.1.4.1.294				
Community				
<u>Name</u>	<u>Access Right</u>			
<input type="text" value="public"/>	<input type="text" value="ReadOnly"/> <input type="button" value="v"/>			
<input type="text"/>	<input type="text"/> <input type="button" value="v"/>			
<input type="text"/>	<input type="text"/> <input type="button" value="v"/>			
Traps				
<u>Destination IP</u>	<u>Trap Community</u>	<u>Trap Version</u>		
<input type="text"/>	<input type="text"/>	<input type="text"/> <input type="button" value="v"/>		
<input type="text"/>	<input type="text"/>	<input type="text"/> <input type="button" value="v"/>		
<input type="text"/>	<input type="text"/>	<input type="text"/> <input type="button" value="v"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>				

Figure 5- 4. SNMP window

Under **SNMP Management**, enable or disable **SNMP Agent** or **SNMP Traps** by using the check boxes. An SNMP Agent is software that runs locally on the device. A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device. Traps are messages that alert network personnel of events that occur on the Switch. The events can be as serious as a reboot (someone accidentally turned OFF the Switch), or less serious like a port status change. The Router generates traps and sends them to the trap recipient (or network manager). Typical traps include trap messages for Authentication Failure, Topology Change and Broadcast/Multicast Storms. In the **Name**, **Location** and **Contact** fields, enter the appropriate information of the Network Administrator. Under **Community**, enter the name of an SNMP community string that defines the relationship between the SNMP manager and an agent. The community string acts like a password to permit or deny access to an agent on the Router. The defining characteristic associated with the community string is the **Access Right**. The agent's access right can be set as either read/write or read-only. Under **Traps** enter the **Destination IP address** and **Trap Community Name** so that the agent sends traps to the management server. The **Trap Version** can also be set to either *SNMP V1* (to specify that SNMP version 1 will be used) or *SNMPv2c*, which supports both centralized and distributed network management strategies. *SNMP V2c* includes improvements in the Structure of Management Information (SMI) and adds some security features.

Filters

The following window will aid the router's administrator in configuring filters for IP addresses. There are two types of filters that the administrator can configure. **Outbound Filters** are for administrators who wish to deny clients on their LAN from accessing certain virtual ports or IP addresses on the Internet. **Inbound Filters** are for administrators who wish to deny IP addresses or virtual ports from outside the router (on the Internet) from accessing the Internal LAN of the router. Click the corresponding radio button to configure Outbound or Inbound Filters. Both screens are identical in configuration.

Figure 5- 5. Filters window

To configure filters for the router, configure the following fields and click **Apply**.

Source IP	Enter an IP address or range of addresses from which to block or allow packets. This field may also be used to block a set of subnet masks by using the corresponding pull down menu.
Destination IP	Enter an IP address or range of addresses to which to block or allow packets from being sent. This field may also be used to block a set of subnet masks by using the corresponding pull down menu.
Source Port	Enter a port or range of ports from which to block or allow packets. This field can only be configured if TCP or UDP is selected in the Protocol field. The Safe Range option in the pull down menu is for ports that have a higher value than 1024.
Destination Port	Enter a port or range of ports to which to block or allow packets from being sent. This field can only be configured if TCP or UDP is selected in the Protocol field. The Safe Range option in the pull down menu is for ports that have a higher value than 1024.
Protocol	Use the pull down menu to select the protocol type to be used for this filter. The user may choose between TCP , UDP or TCP UDP .

Action	This field states allows the user to choose the course of action for this filter to take. The user may choose Allow to allow packets to be forwarded to end nodes configured in the previous fields. The user may choose Deny to block packets from being forwarded to end nodes configured in the previous fields.
---------------	---

Properly configured filters for the router will appear in the table in the bottom half of the filters window. Click **Apply** to set the filters configured for this router.

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.

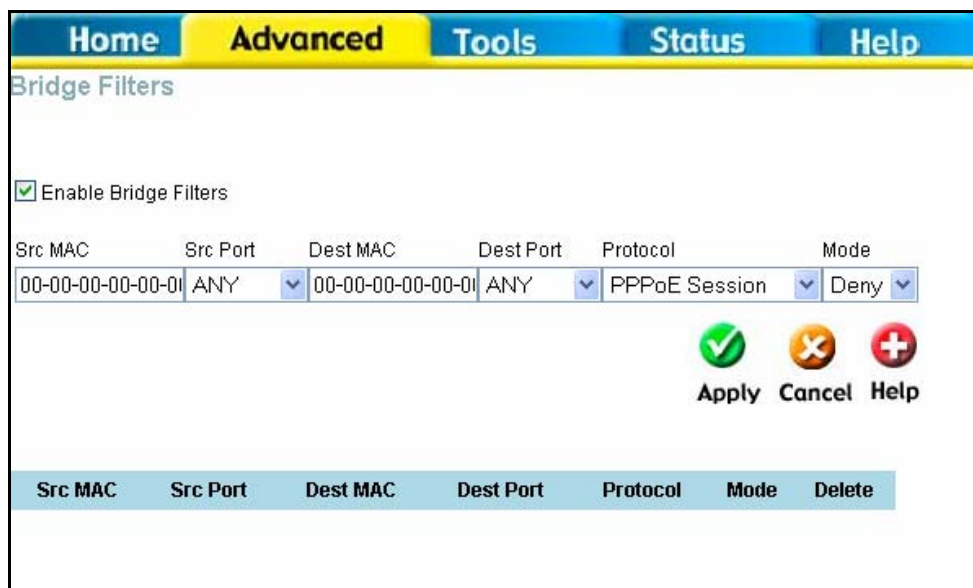


Figure 5- 6. Bridge Filters window

To add a bridge filter rule, check **Enable Bridge Filters**, type in a Source MAC, a Destination MAC or both in the entry fields. Select *Any* to apply the rule to any protocol that the router receives. The user may also specify a protocol to be filtered by using the pull-down menu, and then choose either *Allow*, to allow the specified protocol to pass through the router, or *Deny* to filter the protocol from the router. The protocols that may be specifically allowed or denied to pass through the WAN interface are *IPv4*, *IPv6*, *RARP*, *PPPoE Discovery* and *PPPoE Session*. Click the **Add** button. The rule will appear in the entry field below as it is currently configured. 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.

Routing

Clicking the **Routing** tab will lead you to this window, which is used to manually enter a routing entry for the Router. Routing entries are used when known gateways and hops on the network are known to the user. Unless instructed by your ISP or if you have a greater knowledge of networking, this window should not be necessary to configure as the LAN IP settings should be sufficient for your connection.

Figure 5- 7. Routing window

The user may configure the following fields for Static routing on the router:

Destination	Enter the host IP address or the remote network that will be used for static routing on the router.
Netmask	Enter the Subnet Mask to be used for static routing.
Gateway	Enter the gateway device's IP address. This is an IP address of a device that will allow the user to contact the remote network or Host IP address. This field cannot be configured or used if the following field, Connection , has been selected.
Connection	Choose a PVC from the corresponding pull-down menu to be used for static routing. This field cannot be configured or used if the previous field, Gateway , has been selected.

Click **Apply** to set the routing information configured.

DMZ

Firewalls may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a firewall bypass can be set up using a DMZ IP address. The DMZ IP address is a “visible” address and does NOT benefit from the full protection of the firewall function. Therefore it is advisable that other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to use isolate the device with the DMZ IP address from the rest of the LAN. For example, if you want to use video conferencing and still use a firewall, you can use the DMZ IP address function. In this case, you must have a PC or server through which video conferencing will take place. The IP address of this PC or server will then be the DMZ IP address. You can designate the server's IP address as the DMZ by typing in the IP address in the **IP Address** space provided and then enabling its status by clicking the **Enabled** radio button and then click **Apply**. For the system that uses the DMZ IP address, you may want to manually assign an IP address to it and adjust your DHCP server addresses so that the DMZ IP address is not included in the

DHCP server range. This way you avoid possible IP address problems if you reboot the DMZ system. To configure the Router's DMZ IP address, click the **Advanced** tab at the top of the screen and then the **DMZ** tab to the left.

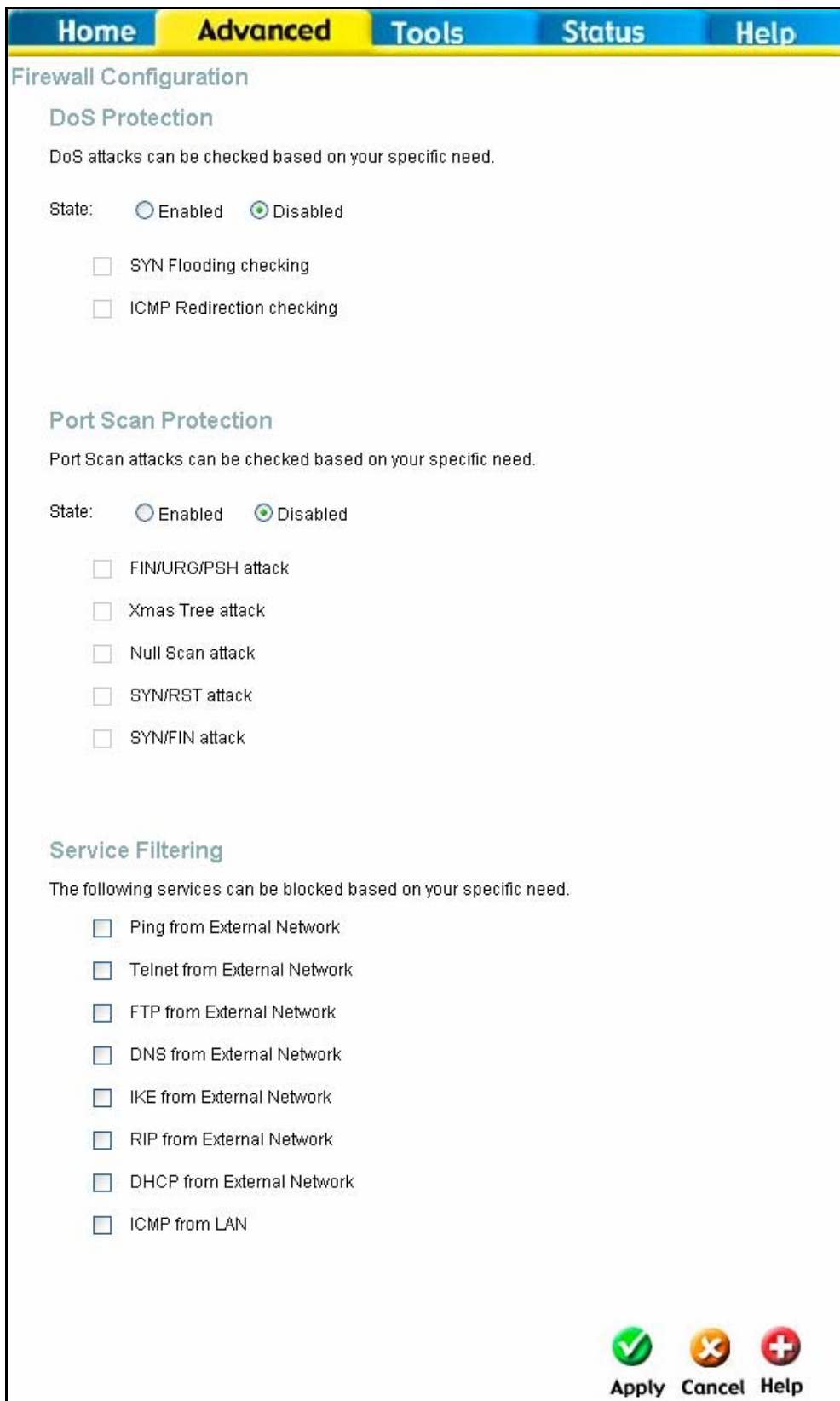


Figure 5- 8. DMZ window

Click **Apply** when your configuration is complete.

Firewall

The DSL-G604T ADSL Router comes equipped with a firewall. The **Firewall** configuration screen allows the Router to enforce specific predefined policies intended to protect against certain common types of attacks. To configure the Router's firewall, click the **Advanced** tab at the top of the screen and then the **Firewall** tab to the left.



Home **Advanced** **Tools** **Status** **Help**

Firewall Configuration

DoS Protection

DoS attacks can be checked based on your specific need.

State: Enabled Disabled

- SYN Flooding checking
- ICMP Redirection checking

Port Scan Protection

Port Scan attacks can be checked based on your specific need.

State: Enabled Disabled

- FIN/URG/PSH attack
- Xmas Tree attack
- Null Scan attack
- SYN/RST attack
- SYN/FIN attack

Service Filtering

The following services can be blocked based on your specific need.

- Ping from External Network
- Telnet from External Network
- FTP from External Network
- DNS from External Network
- IKE from External Network
- RIP from External Network
- DHCP from External Network
- ICMP from LAN

Apply Cancel Help

Figure 5- 9. Firewall window

This window has three filtering options for you to choose, **DoS (Denial of Service) Protection**, **Port Scan Protection** and **Service Filtering**. **DoS Protection** and **Port Scan Protection** may be globally enabled on the router and then may be modified to the users preference by checking the boxes in these

sections. For **Service Filtering**, the user must choose which services to be filtered by the router using the corresponding check boxes. The user may choose any combination of these to use for firewalling. Click **Apply** to set these firewall rules to the routers memory.

RIP

The DSL-G604T supports RIP v1 and RIP v2 used to share routing tables with other Layer 3 routing devices on the LAN, at your ISP's location or remote networks connected to your network through the ADSL line. The user may enable or disable RIP v1 (received and sent) or RIP v2. This will enable the router to send and receive RIP packets. Disabling the RIP function will disable the routing function of this device.



Figure 5- 10. RIP window

To configure RIP, first use the RIP pull-down menu to enable RIP on the Router. Then select the protocol to be used by using the pull-down menu. The choices are **RIP v1**, **RIPv1 Compatible** and **RIP v2**. Then the user must choose the direction by selecting **In**, **Out** or **Both**. After making the configuration choices for RIP, click the **Apply** button to set the configurations in the memory of the Router.

PPP

The following window is for users employing the PPP protocol as their connection to the ISP. This window will be specific to PVCs previously configured and will display information concerning the PVC selected in the WAN configuration window.

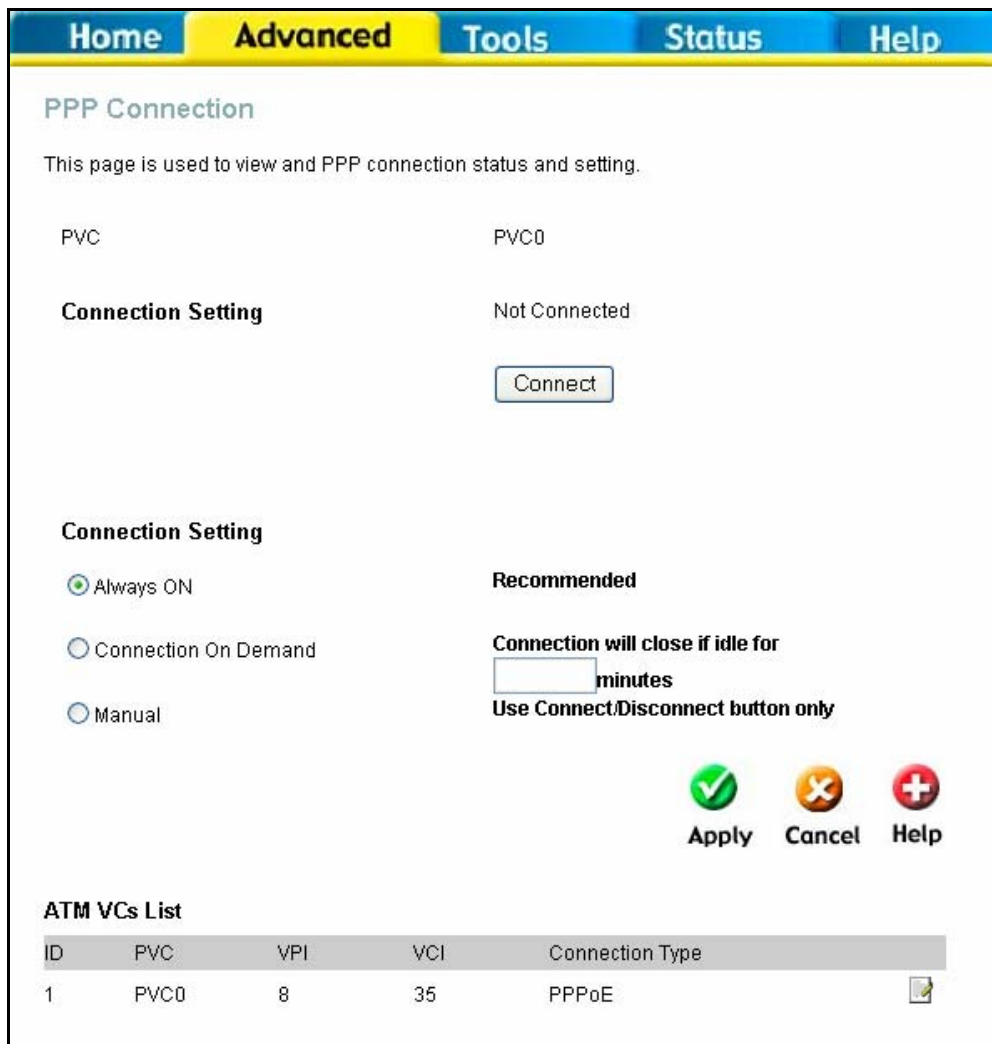


Figure 5- 11. PPP window

The window above displays the following information.

PVC	Displays the PVC currently in use on the Router. This router can be configured for eight PVCs.
Connection Setting	<p>This field has three options for the connection setting of the PPP protocol.</p> <ul style="list-style-type: none"> • Always On – Clicking this radio button will set the connection to always be connected. • Connection on Demand – Clicking this radio button will set the Router to connect to the Internet only when requested to by your computer. • Manual – Clicking this radio button will set the router to only connect when the user clicks the connect button in the previous field.
ATM VCs List	This field will display the status of PVCs currently in use on the Router.

Click **Apply** to set the changes in the memory of the Router.

ADSL

This window will allow you to set the ADSL configuration protocol for the ADSL Router. You may choose the modulation type from the pull-down window. The options are **Multi-mode, T1.413,**

G.Dmt and **G.lite**. Your ISP must provide this information to you. Click **Apply** after you have made the proper selection.

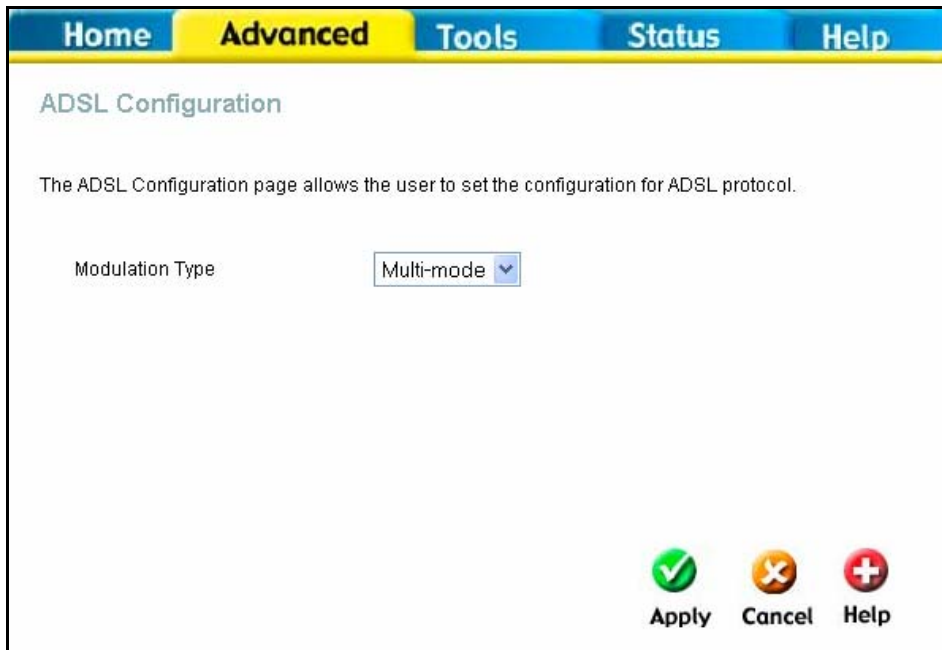


Figure 5- 12. ADSL window

ATM VCC

The ATM VCC window shows you the current WAN settings implemented on your ADSL Router under the heading ATM VCs List at the bottom of the screen. Selecting a Connection Type will change the window for the values for the Connection setting selected. These values have already been described in the **WAN** section of the **Home** setup. Click **Apply** to set changes into the Router's memory.

Home
Advanced
Tools
Status
Help

ATM VC Setting

PVC: PVC0

VPI:

VCI:

Virtual Circuit:

WAN Setting:

PPPoE/PPPoA

User Name:

Password:

Connection Type:

MTU: bytes

MRU: bytes




Default Route:

NAT:

Firewall:

IP Control:

Static IP:

 **Apply**
 **Cancel**
 **Help**

ATM VCs List









ID	PVC	VPI	VCI	Connection Type	Virtual Circuit	
1	PVC0	8	35	PPPoE/PPPoA	Enabled	
2	PVC1	0	36	Bridge Mode	Disabled	
3	PVC2	0	37	Bridge Mode	Disabled	
4	PVC3	0	38	Bridge Mode	Disabled	
5	PVC4	0	39	Bridge Mode	Disabled	
6	PVC5	0	40	Bridge Mode	Disabled	
7	PVC6	0	41	Bridge Mode	Disabled	
8	PVC7	0	43	Bridge Mode	Disabled	

Figure 5- 13. ATM VCC window

Wireless Management

The **Wireless Management** menu located in the **Advanced** directory is used to control MAC address access to the wireless access point and to view a list of MAC addresses that are currently associated

with the access point. This menu is also be used to enable and configure use of multiple SSIDs. To use more than one SSID, WEP and WPA security must first be disabled (see below).

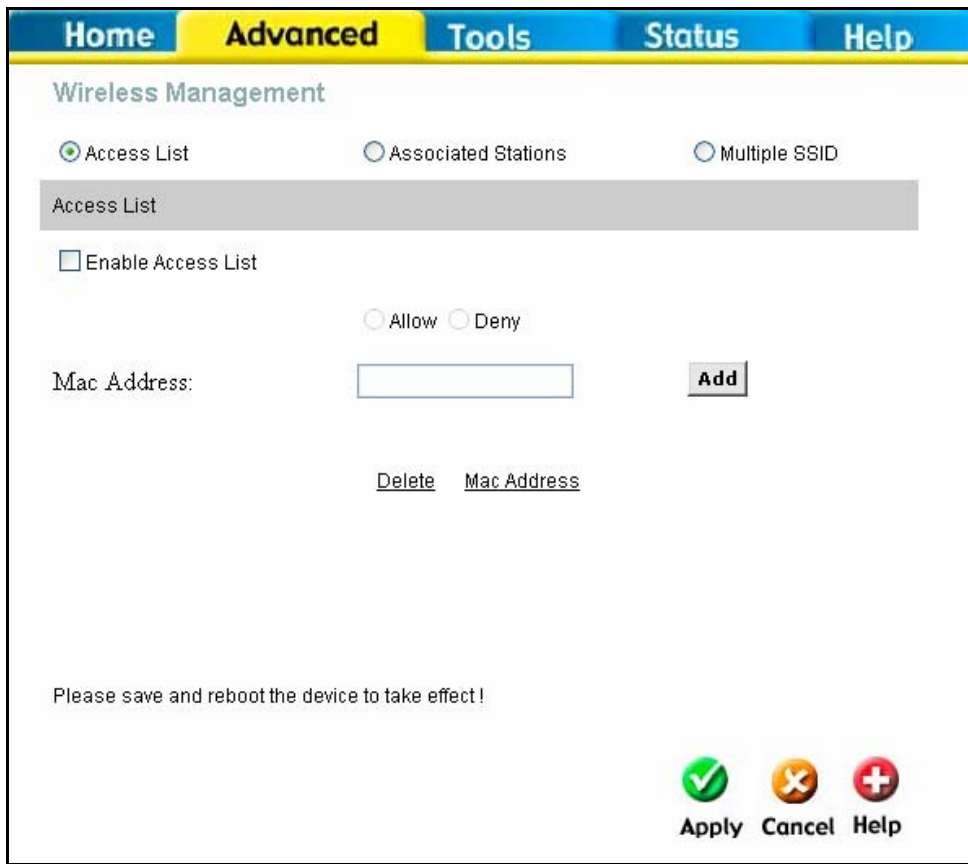


Figure 5- 14. Wireless Management

Configure Wireless Access Control

To create a list of MAC addresses that are banned or allowed association with the wireless access point:

1. Click in the **Enable Access List** option box to select it.
2. Select the action to perform on the MAC address to be specified. Choose to **Allow** or **Deny** association.
3. Type in the **MAC Address** in the entry field provided.
4. Click the **Add** button to add the MAC address to the list. The MAC address will appear listed in the table below.
5. After compiling the list of MAC addresses as desired, click the **Apply** button to enforce access control for the MAC addresses in the list.

To remove any MAC address from the list, click the radio button in the left column of the list for the MAC address to be removed and click the **Apply** button. To view a list of stations currently associated with the access point, click the **Associated Stations** radio button.

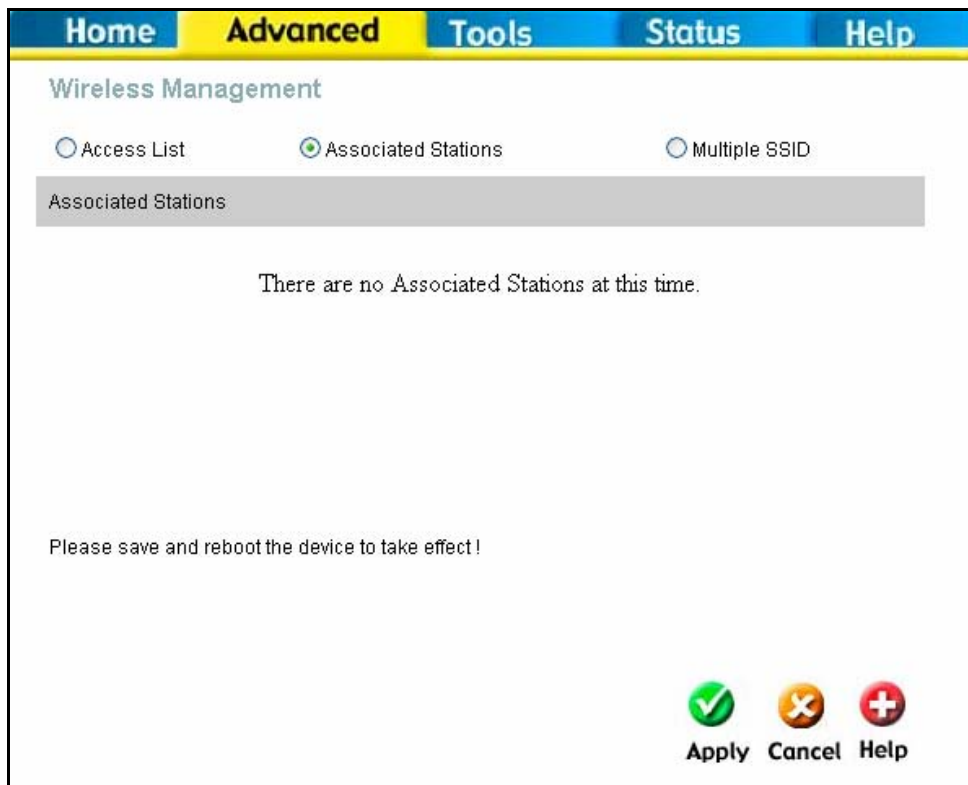


Figure 5- 15. Wireless Management –Associated Stations window

Configure Multiple SSID

Multiple SSID cannot be used if the access point has either WPE or WPA enabled. This must first be disabled in the Wireless menu located in the Home directory.

To configure multiple SSID:

1. Disable WEP or WPA in the **Wireless** menu of the **Home** directory.
2. Click in the **Enable Multiple SSID** option box to select it.
3. Enter the **SSID** you want to add.
4. Click the **Add** button to add the SSID to the list.
5. Click the **Apply** button to enable the listed SSIDs.

To remove an SSID from the list, click the radio button in the left column of the list for the SSID to be removed and click the **Apply** button.

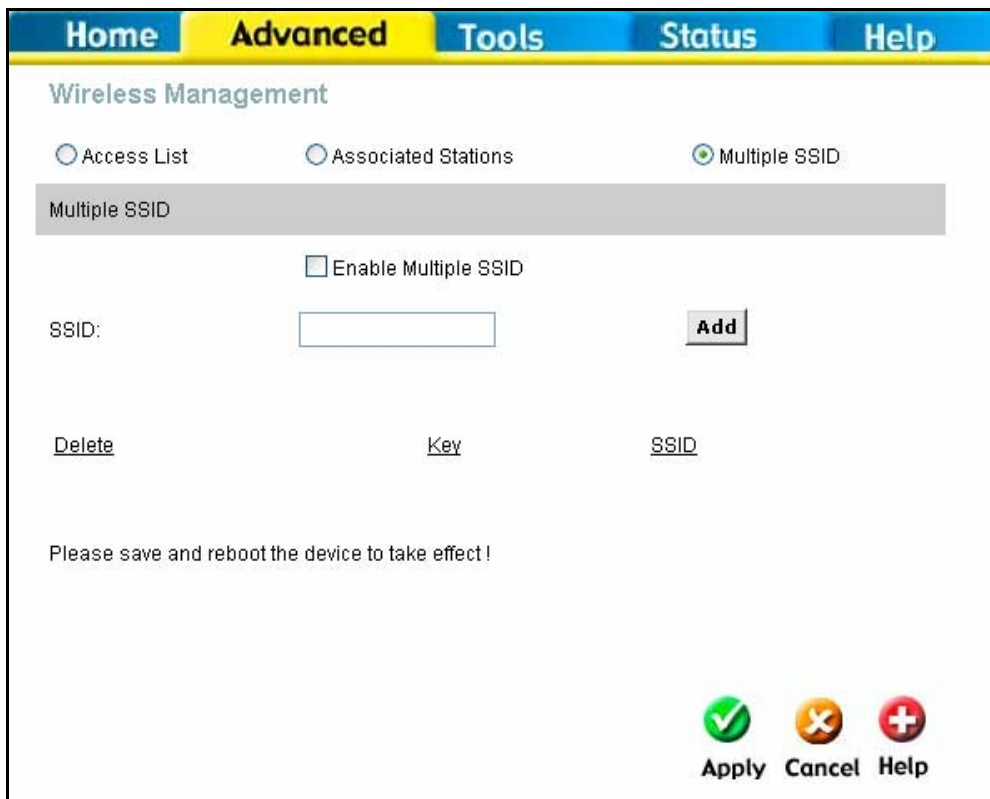


Figure 5- 16. Wireless Management –Multiple SSID window

Wireless Performance

If you want to change the wireless settings, click the **Wireless Performance** menu button in the **Advanced** directory



Note

It is recommended for most users to use the default Wireless LAN Performance settings. Any changes made to these settings may adversely affect your wireless network. Under certain circumstances, changes may benefit performance. Carefully consider and evaluate any changes to these wireless settings.

Home	Advanced	Tools	Status	Help
Wireless Performance				
These are the Wireless Performance feature for the AP(Access Point) portion.				
Beacon interval:	<input type="text" value="200"/>	(msec, range:1~1000,default:200)		
DTIM:	<input type="text" value="2"/>	(range:1~25,default:2)		
Hidden SSID:	<input type="checkbox"/> Enabled			
Antenna transmit power:	<input type="button" value="Full"/>			
RTS Threshold:	<input type="text" value="2347"/>			
Frag Threshold:	<input type="text" value="2346"/>			
b/g Mode:	<input type="button" value="Mixed"/>			
			<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>
			<input type="button" value="Help"/>	

Figure 5- 17. Wireless Performance window

Tools

The Tools tab allows you to set up basic maintenance features on the ADSL router. The windows available under this tab include **Admin**, **Time**, **Remote Log**, **System**, **Firmware**, **Micellaneous**, and **Test**.

Admin

The **Admin** window allows you to configure a new password for the ADSL Router. There is only one administrator account that can access the DSL-G604T's web management interface. To change the password enter the new password into the **New Password** field and repeat the password in the **Confirm Password** field. To change the Router's port number use the **Web Port** field. Click **Apply** to set your new password. This window will also allow the user to enable remote management of the device from a remote computer, either through the web management or through Telnet. To configure this function, click the **Enabled** radio button under the **Remote Management** heading, enter the **IP Address** of the computer you wish to allow to remotely configure the Router, along with the corresponding SubnetMask (**Netmask**). Click **Apply** to set these configurations into the memory of the Router.

D-Link
Building Networks for People

DSL-G604T
Wireless ADSL Router

Home Advanced **Tools** Status Help

Admin
Time
Remotelog
System
Firmware
Miscellaneous
Test
Logout

Administrator Settings

There is only one account that can access the DSL-G604T's Web-Management interface.

Administrator (The Login Name is "admin")

New Password

Confirm Password

WebPort (Change the port number of login web)

Remote Web Management

State Enabled Disabled

IP Address

Netmask

Remote Telnet Management

State Enabled Disabled

IP Address

Netmask

Figure 6- 1. Administrator Settings window

Time

The system time is the time used by the DSL-G604T for scheduling services. You can manually set the time, connect to a NTP (Network Time Protocol) server or synchronize the time on the router with your PC. If an NTP server is set, you will only need to set the time zone (in the set up wizard). You may also set the time from the clock on your computer by checking the corresponding radio button. To manually set the time, you will need to input the value into the fields provided. Click **Apply** to set changes.

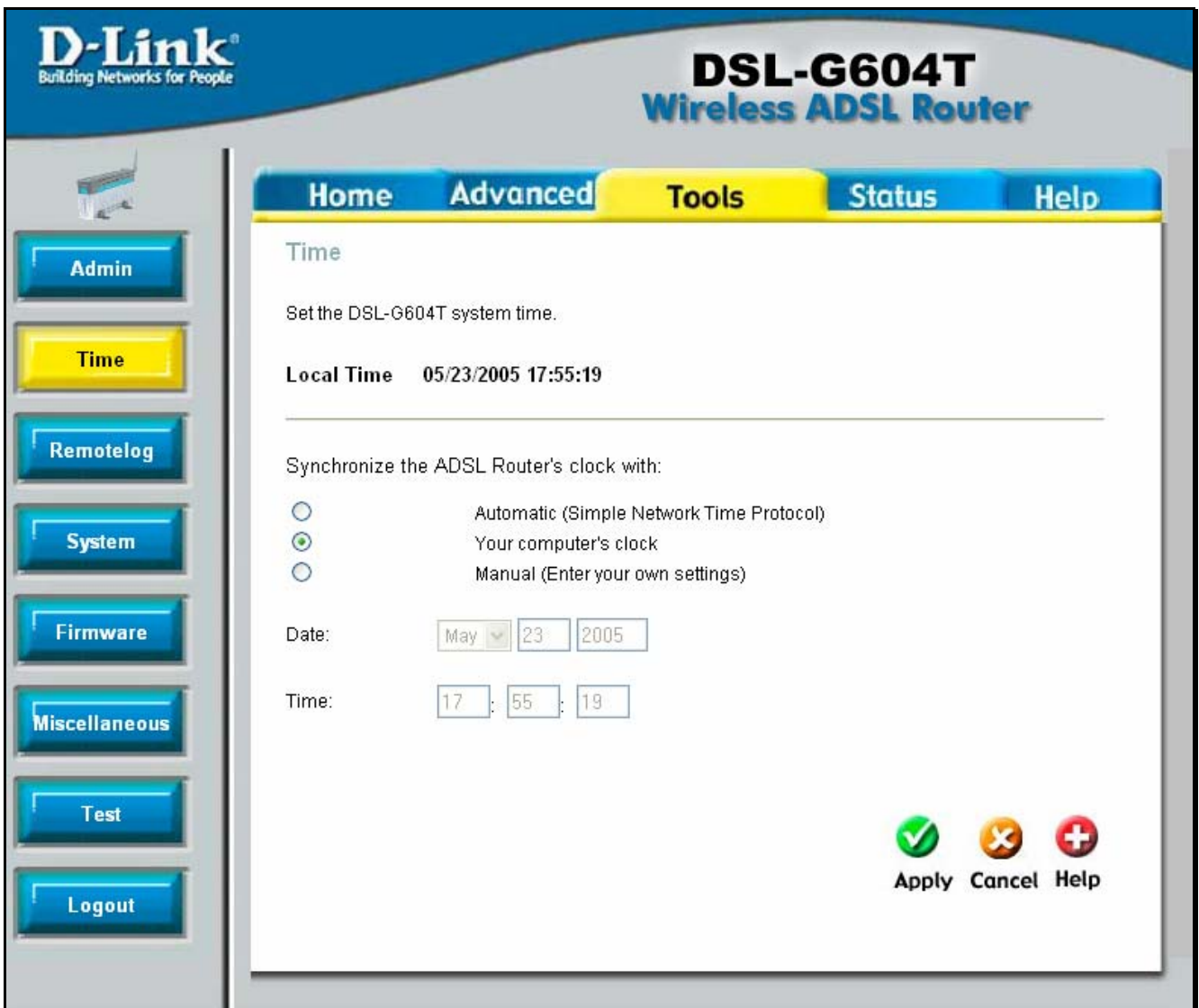


Figure 6- 2. Time window

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.

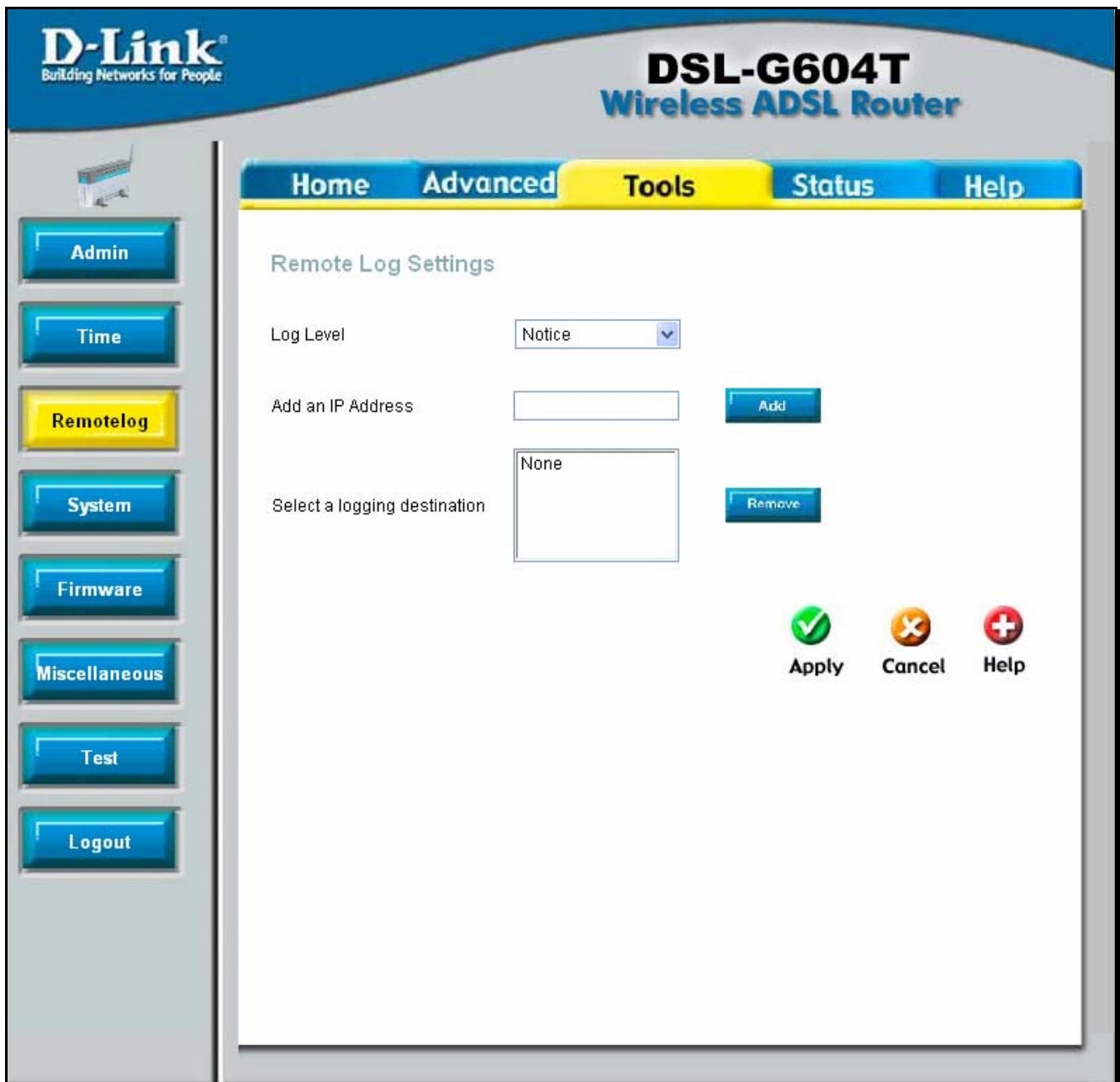


Figure 6- 3. Remote Log window

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.

System

This window offers four settings for the user to configure. The user may save the settings configured on the router by clicking the Save button. A file Download dialogue box will appear questioning the user where to save the files on your computer. Files will be saved as XML documents. The user may also upload save settings by using the **Load Settings from Local Hard Drive** field by entering the path of the file on your computer into the box. If you are not sure of the path, click **Browse** to find the file on your computer. Click **Load** to initiate the file transfer. Next, click save and reboot. You may reset the ADSL Router back to factory default settings by clicking on **Restore**. To force the Router to Restart, click **Restart AP**.



Figure 6- 4. System Settings window

Firmware

You can upgrade the firmware of the ADSL Router at this page. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to browse the local hard driver and locate the firmware to be used for the update. Once found, click **Apply** to initiate the transfer. Please check the D-Link support site for firmware updates at D-Link Technical support website of your country. Remember to restart the Router after uploading new firmware.



Figure 6- 5. Firmware Upgrade window

Miscellaneous

The **Ping Test** menu allows you to ping any IP address from the Router to test connectivity to the address. To Ping a device, enter the IP address of the device that you wish to ping into the **Ping IP Address** field and click **Ping** to start the Ping mechanism. The results of the ping will be shown under the **Ping Result** heading. The Miscellaneous Configuration menu also allows you to enable IGMP forwarding. This is **Disabled** by default. This setting will not allow IGMP (Internet Group Management Protocol) packets to be forwarded to the LAN. IGMP is used to manage multicasting on TCP/IP networks, most users will not need to enable this. Some ISPs use IGMP to perform remote configuration for client devices, such as the Router. If you are unsure, check with your ISP. To enable IGMP service to the LAN interface, select **Enabled** and click the **Apply** button. To force a system restart click **Save and Reboot**.

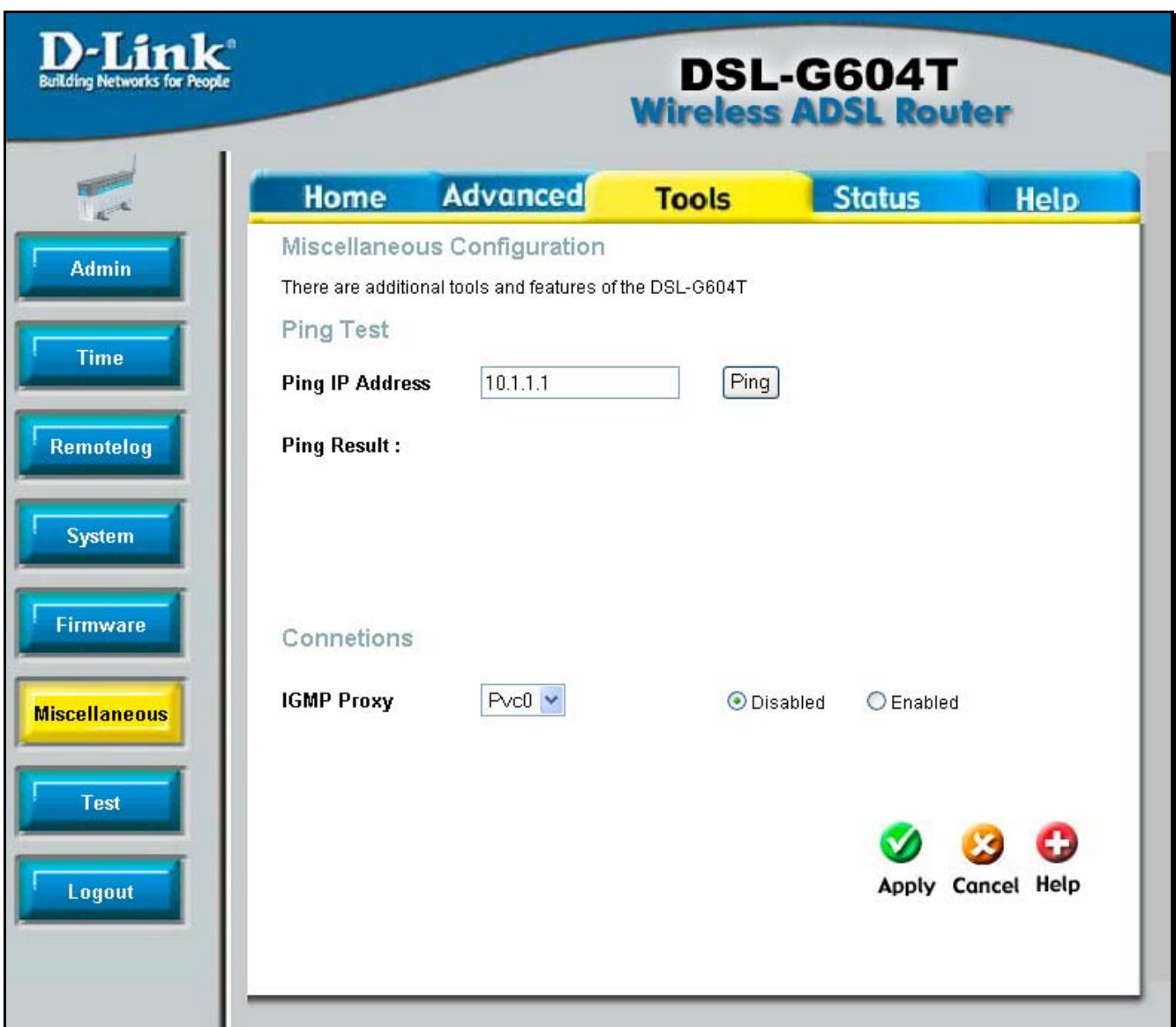


Figure 6- 6. Miscellaneous window

Test

The **Diagnostics** window allows users to test the functionality of the router by executing a series of tests. This window will aid the user in troubleshooting various problems that may occur with the functionality of the router. This window will appear differently depending on connection type chosen. The following picture shows the window that includes all possible connection tests associated with this Router.

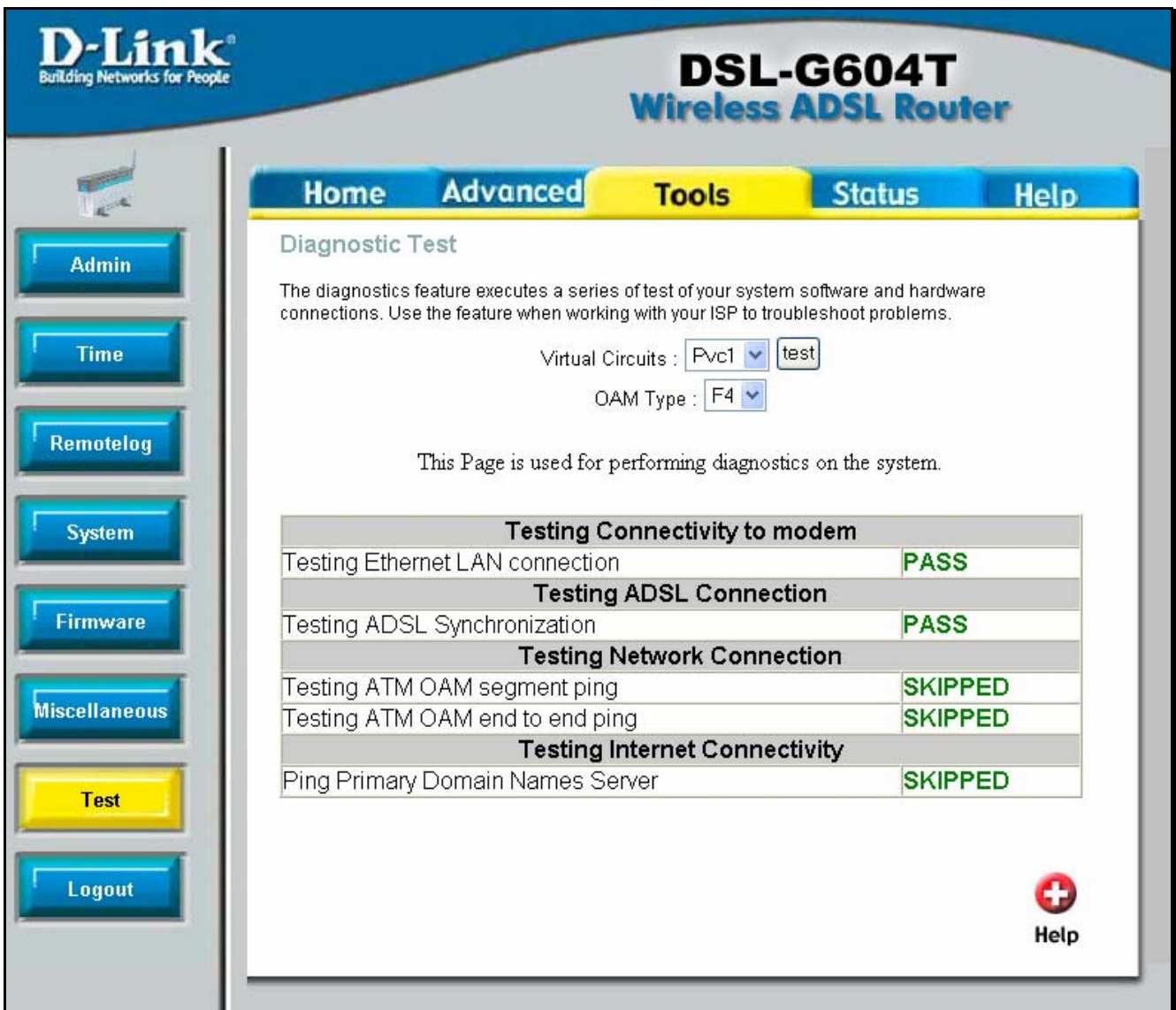


Figure 6- 7. Diagnostics window

To perform the following tests, choose the **PVC0** (Private Virtual Connection) and click **Apply**. Test results will either be displayed as **Pass** or **Fail**. The following tasks will be performed:

Testing Ethernet LAN Connection	This test will check the Ethernet connection of your Router.
Testing ADSL Synchronization	This test will check the ADSL line connected to your Router.
Testing ATM OAM segment	This test will check the PVC connectivity by sending out an OAM (Operation Administration Management) packet. If the remote device

ping	on this segment returns the ping packet, the PVC has passed the test and a Pass result will appear.
Testing ATM OAM end to end ping	This test will check the PVC connectivity by sending out an OAM (Operation Administration Management) packet. If the remote device returns the ping packet, the PVC has passed the test and a Pass result will appear.
Ping Primary Domain Name Server	This test will check to see if the Primary DNS is accessible from the Router.

Status

The **Status** tab will allow users to check information about the Router, including **Device Information**, **DHCP Clients**, **Log**, **Statistics** and **ADSL**.

Device Info

The device info window, located under the **Status** tab will allow users to view information regarding the settings of the Router, both on the LAN side and WAN side of the connection.

The screenshot displays the D-Link DSL-G604T Wireless ADSL Router web interface. The top navigation bar includes tabs for Home, Advanced, Tools, Status (highlighted), and Help. A left sidebar contains buttons for Device Info, DHCP Clients, Log, Statistics, ADSL, and Logout. The main content area shows the 'Device Information' window with the following details:

Firmware Version : V2.00B01T01.AU

LAN	
MAC Address	00:0F:3D:9E:3E:45
IP Address	10.1.1.1
Subnet Mask	255.0.0.0
DHCP Server	Disabled
NAT	Enabled

WAN	
Virtual Circuit	Pvc0
Status	Not Connected
Connection Type	pppoe
IP Address	N/A
Subnet Mask	N/A
Default Gateway	N/A
DNS Server	N/A

A red cross icon and the word 'Help' are located in the bottom right corner of the Device Information window.

Figure 7- 1. Device Info window

The following information is what is displayed in the **Device Info** window:

LAN	
MAC Address	Displays the MAC Address of the Router.
IP Address	Displays the current IP address of the Device.
Subnet Mask	Displays the Subnet Mask of the device.
DHCP Server	Displays the DHCP status implemented on the Router.
NAT	Displays the current NAT status implemented on the Router.
WAN Channel	
Virtual Circuit	Displays the number of the Private Virtual Channel located on the Router.
Status	Displays the connection status of the selected Virtual Channel.
Connection Type	Displays the connection type employed on this Virtual Circuit.
IP Address	Displays the IP address of the corresponding Virtual Circuit.
Subnet Mask	Displays the Subnet mask of the corresponding Virtual Circuit.
Default gateway	Displays the Default gateway of the corresponding Virtual Circuit.
DNS Server	Displays the DNS Server currently employed on this Virtual Circuit.

DHCP Clients

To view DHCP clients that are configured on the Router click **DHCP Clients** under the Status tab.

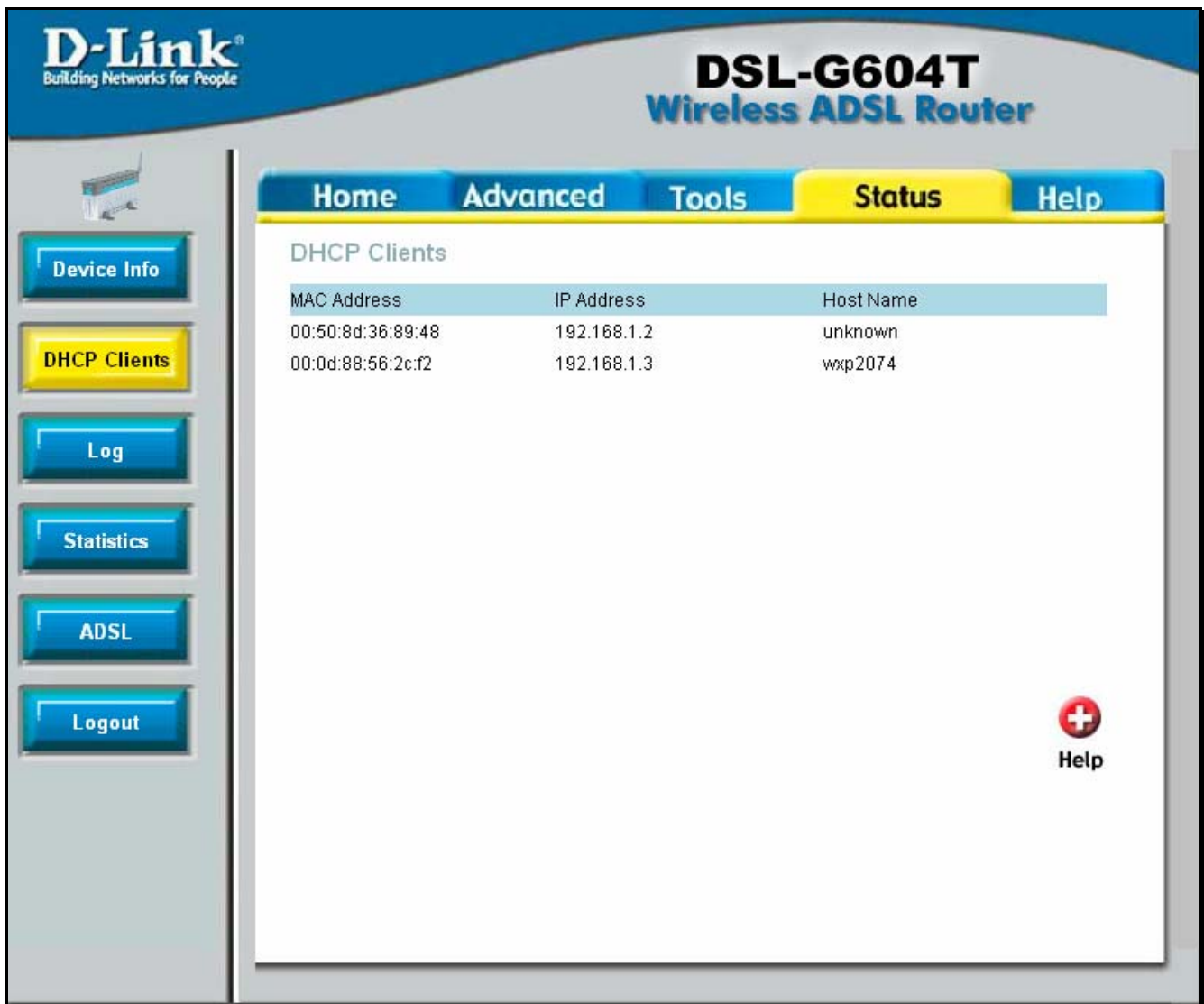


Figure 7- 2. DHCP Clients window

Log

The **Log** window allows users to view events occurring within the Router by time and date. To clear the log events, click **Clear Log**. To save the log, click **Save Log** and a pop-up window will appear to find a folder on your computer to save the log files to.

The screenshot displays the web management interface for a D-Link DSL-G604T Wireless ADSL Router. The interface features a blue header with the D-Link logo and the product name. A navigation bar includes tabs for Home, Advanced, Tools, Status (highlighted), and Help. On the left, a sidebar contains buttons for Device Info, DHCP Clients, Log (highlighted), Statistics, ADSL, and Logout. The main content area shows the 'View Log' section, which includes a description, navigation buttons (First Page, Last Page, Previous, Next, Clear Log, Save Log), and a Help icon. Below the navigation is a table with two columns: Time and Message. The table contains two entries of log messages, each detailing a connection attempt and termination.

D-Link
Building Networks for People

DSL-G604T
Wireless ADSL Router

Home Advanced Tools **Status** Help

View Log
View Log displays the activities occurring on the DSL-G604T.

First Page Last Page Previous Next Clear Log Save Log

Help

page 1 of 2

Time	Message
Jan 2 06:09:34	Modem hangup
Jan 2 06:09:34	Connection terminated.
Jan 2 06:09:34	Doing disconnect
Jan 2 06:09:34	Terminated: Modem Hang-Up
Jan 2 06:09:40	pppd 2.4.1 started by root, uid 0
Jan 2 06:09:40	Got connection: 6d02
Jan 2 06:09:40	Saved Session ID: 0
Jan 2 06:09:40	Connecting PPPoE socket: 00:60:38:ed:40:12 6d02 nas0 0x1000d378
Jan 2 06:09:40	Default Asymmetric MTU for ppp0 1500
Jan 2 06:09:40	Connect: ppp0 [-] nas0
Jan 2 06:09:40	CHAP authentication failed
Jan 2 06:09:40	Modem hangup
Jan 2 06:09:40	Connection terminated.
Jan 2 06:09:40	Doing disconnect
Jan 2 06:09:40	Terminated: Modem Hang-Up
Jan 2 06:09:44	pppd 2.4.1 started by root, uid 0
Jan 2 06:09:44	Got connection: 6d02
Jan 2 06:09:44	Saved Session ID: 0
Jan 2 06:09:44	Connecting PPPoE socket: 00:60:38:ed:40:12 6d02 nas0 0x1000d378
Jan 2 06:09:44	Default Asymmetric MTU for ppp0 1500

Figure 7- 3. Device Log window

Statistics

The Stats window will allow users to view transmitted and received packets occurring on the Router for Ethernet ADSL, and Wireless connections. To choose a interface to view statistics for, click the corresponding radio button for **ADSL**, **Ethernet**, or **Wireless**. This will change the **Statistics** screen, as shown below. To refresh the stats in this window, click **Refresh**.



Figure 7- 4. Stats window for Ethernet

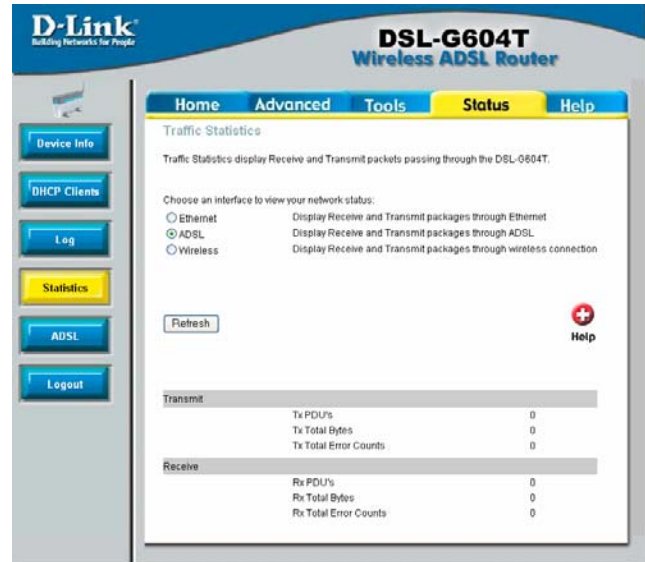


Figure 7- 5. Statistics window for ADSL

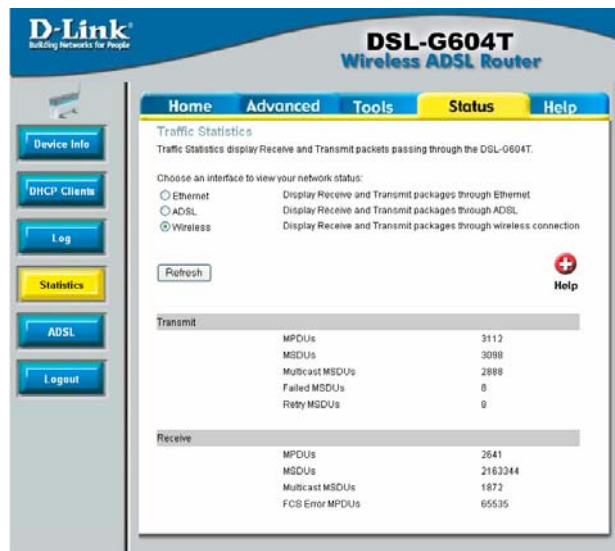


Figure 7- 6. Statistics window for Wireless

ADSL

The ADSL Line window, located under the **Status** tab, will allow users to monitor the speed of the upstream and downstream packet flow of the Router.

The screenshot shows the D-Link DSL-G604T Wireless ADSL Router web interface. The top navigation bar includes tabs for Home, Advanced, Tools, Status (highlighted), and Help. The left sidebar contains buttons for Device Info, DHCP Clients, Log, Statistics, ADSL (highlighted), and Logout. The main content area displays the ADSL Status window, which includes the following information:

ADSL Status

ADSL status shows the ADSL physical layer status.

ADSL Firmware Version: 4.03.03.00 - 3.02.00.03 - 3.02.06.00 Annex A - 01.07.02 - 0.49
 ADSL Software Version: V2.00B01T01.AU
 Line State: Connected
 Modulation: Multi-mode
 Annex Mode: ANNEX_A
 Max Tx Power: -38 dBm/Hz

Item	Downstream	Upstream	Unit
SNR Margin	22	28	dB
Line Attenuation	32	17	dB
Data Rate	512	128	kbps

A Help icon (a red circle with a white plus sign) is located in the bottom right corner of the ADSL Status window.

Figure 7- 7. Status ADSL window

The following information is displayed:

ADSL Firmware Version	The current Firmware version currently set in the Router.
Line state	Displays the current line state of the ADSL connection, either being Up or Down .
Modulation	Displays the modulation type currently set on the router for the ADSL connection.
Annex mode	This field displays the ADSL annex modes for Annex A or Annex B.
Max Tx Power	This field displays the transmit output power level of the CPE.

SNR Margin	Amount of increased noise that can be tolerated while maintaining the designed BER (bit error rate). The SNR Margin is set by the Central Office DSLAM. If the SNR Margin is increased, bit error rate performance will improve, but the data rate will decrease. Conversely, if the SNR Margin is decreased, bit error rate performance will decrease, but the data rate will increase.
Line Attenuation	Attenuation is the decrease in magnitude of the ADSL line signal between the transmitter (Central Office DSLAM) and the receiver (Client ADSL Modem), measured in dB. It is measured by calculating the difference in dB between the signal power level received at the Client ADSL router and the reference signal power level transmitted from the Central Office DSLAM.
Data Rate	This field displays the ADSL data rate.

Help

The **Help** tab will give basic information referring to various screens located in the Router. To view a specific section, click on its hyperlinked name. A new window of information will appear.

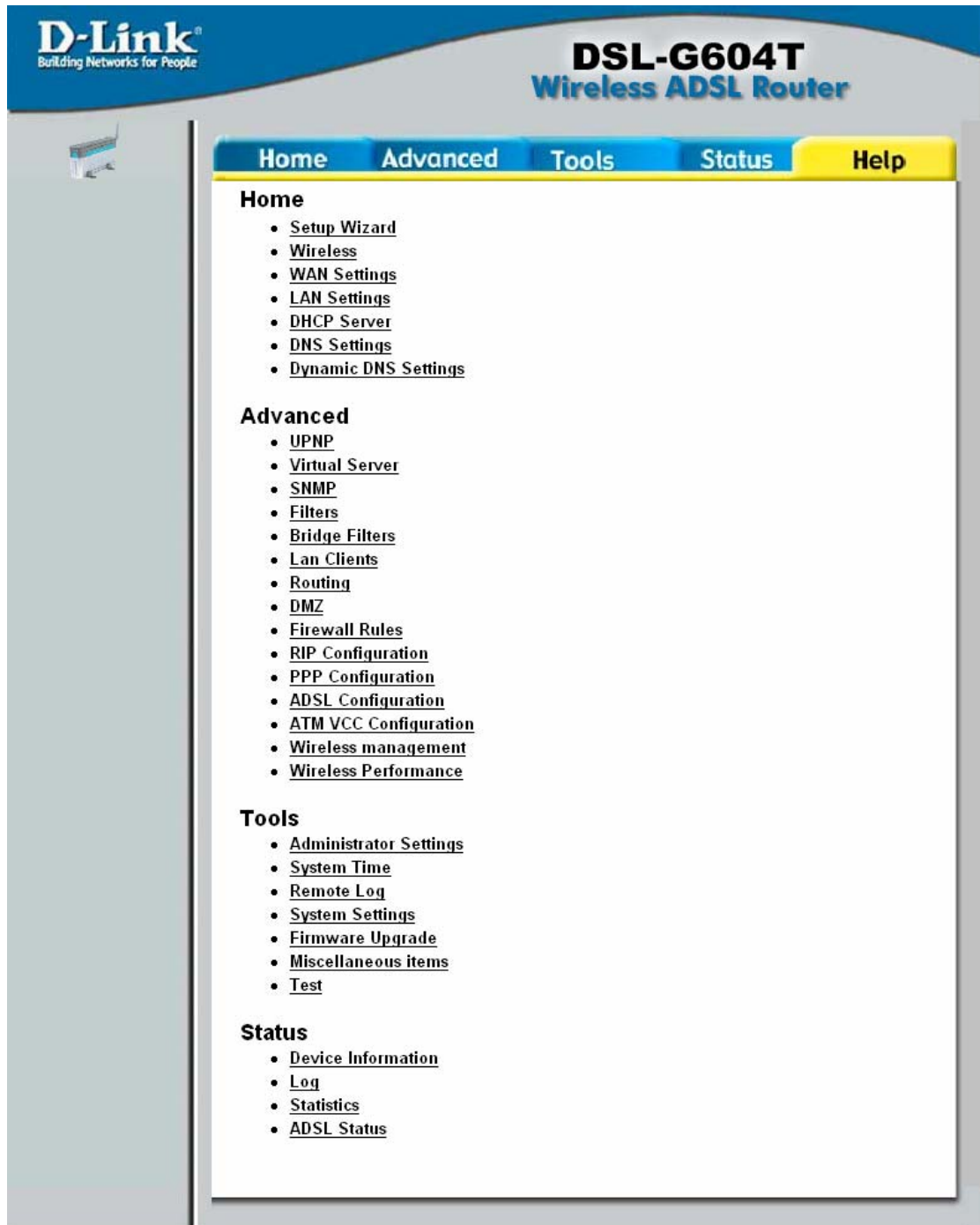


Figure 7- 8. Help Window

Technical Specifications

GENERAL	
Standards:	<p>ADSL Standards ANSI T1.413 Issue 2 ITU G.992.1 (G.dmt) AnnexA ITU G.992.2 (G.lite) Annex A ITU G.994.1 (G.hs)</p> <p>ADSL2 Standards ITU G.992.3 (G.dmt.bis) Annex A ITU G.992.4 (G.lite.bis) Annex A</p> <p>ADSL2+ Standards: ITU G.992.5 Annex A</p>
Protocols:	<p>IEEE 802.1d Spanning Tree TCP/UDP ARP RARP ICMP RFC1058 RIP v1 RFC1213 SNMP v1 & v2c RFC1334 PAP RFC1389 RIP v2 RFC1483/2684 Multiprotocol Encapsulation over ATM Adaptation Layer 5 RFC1577 Classical IP over ATM RFC1661 Point to Point Protocol RFC1994 CHAP RFC2131 DHCP Client / DHCP Server RFC2364 PPP over ATM RFC2516 PPP over Ethernet</p>
Data Transfer Rate:	<p>G.dmt full rate downstream: up to 8 Mbps G.dmt full rate upstream: up to 1 Mbps G.lite: ADSL downstream up to 1.5 Mbps G.lite: ADSL upstream up to 512 Kbps G.dmt.bis full rate downstream: up to 12 Mbps</p>

GENERAL	
	G.dmt.bis full rate upstream: up to 12 Mbps ADSL full rate downstream: up to 24 Mbps ADSL full rate upstream: up to 1 Mbps
Media Interface:	ADSL interface: RJ-11 connector for connection to 26 AWG twisted pair telephone line LAN interface: RJ-45 port for 10/100BASE-T Ethernet connection

Physical and Environmental	
DC Inputs:	Input: 120V AC 60Hz
Power Adapter:	Output: 12V AC, 1.2A
Power Consumption:	12 Watts (max)
Operating Temperature:	0° to 40°C
Storage Temperature	-20° to 70°C
Humidity:	5% to 95% (non-condensing)
Dimensions:	180 mm x 140 mm x 29 mm
Weight:	373 gm
EMI:	CE Class B, FCC Class B (Part 15)
Safety:	CSA 950, UL 1950, IEC 60950, EN 60950
Reliability:	Mean Time Between Failure (MTBF) min. 4 years

B

IP Address Setup

The DSL-G604T 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 pre-existing 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 pre-existing 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 10.1.1.1 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.

IP Setup - Example #1

Using Default IP without DHCP			
Host	IP Address	Subnet Mask	Gateway IP
Router	10.1.1.1	255.0.0.0	

Computer #1	10.1.1.2	255.0.0.0	10.1.1.1
Computer #2	10.1.1.3	255.0.0.0	10.1.1.1
Computer #3	10.1.1.4	255.0.0.0	10.1.1.1

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.

IP Setup - Example #2

Alternative IP Assignment			
Host	IP Address	Subnet Mask	Gateway IP
Router	10.0.0.1	255.0.0.0	
Computer #1	10.0.0.2	255.0.0.0	10.0.0.1

Computer #2	10.0.0.3	255.0.0.0	10.0.0.1
Computer #3	10.0.0.4	255.0.0.0	10.0.0.1

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 show 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 “sub networks” 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.

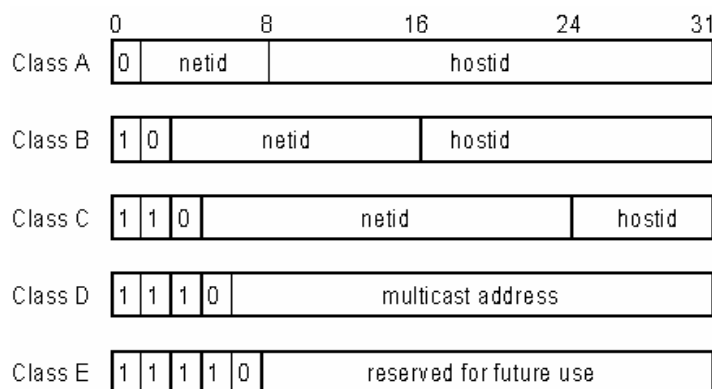
To make IP addresses easy to understand, the originators of IP adopted a system of representation called “dotted decimal” or “dotted quad” notation. Below are examples of IP addresses written in this format:

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	172.31.255.25 5
C	192.168.0.0	192.168.255.2 55

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

D

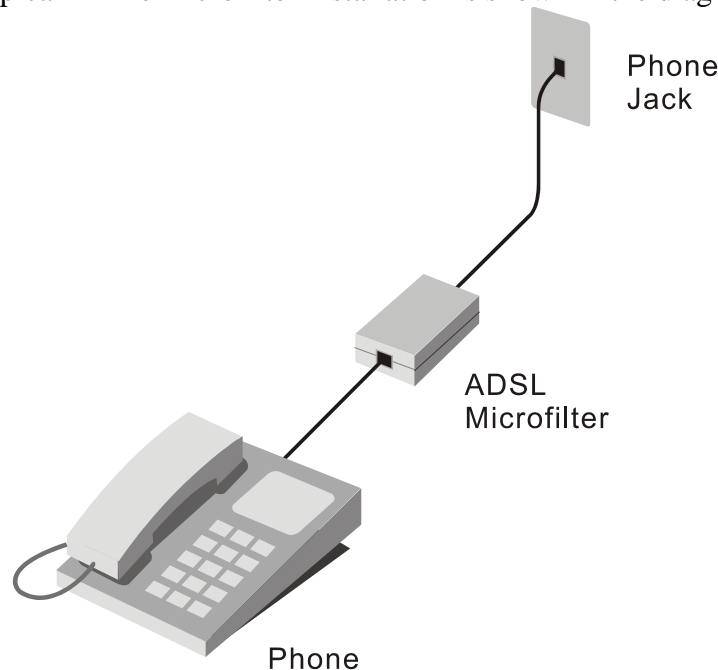
Microfilters and Splitters

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 Router 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 share the line with the ADSL service. Microfilters are easy-to-install, in-line devices, which attach to the telephone cable between the telephone and wall jack. Microfilters that install behind the wall plate are also available. A typical in-line microfilter installation is shown in the diagram below.



Microfilter Installation

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

Line Splitter

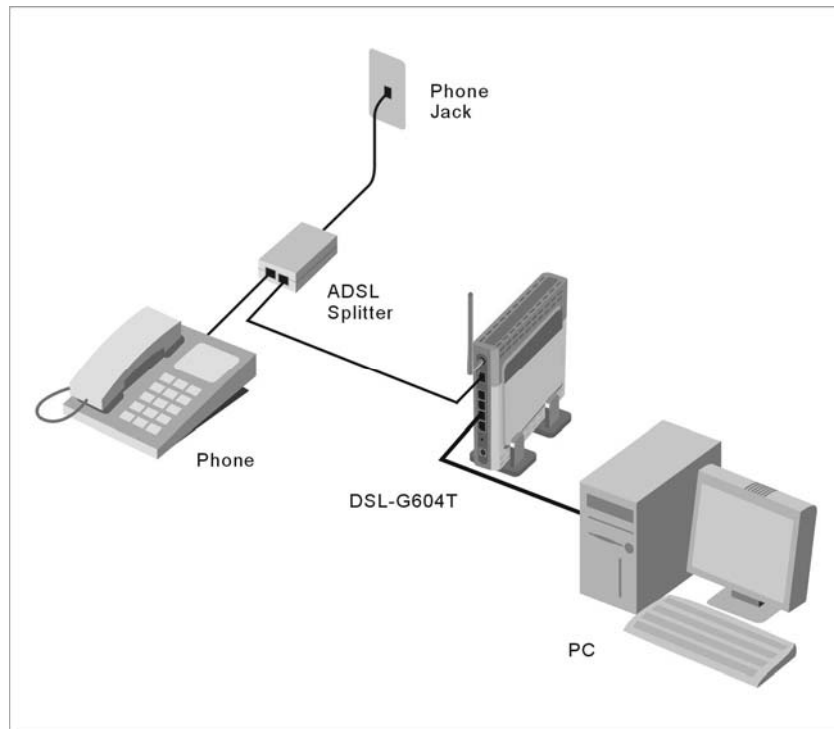
If you are instructed to use a “line splitter”, you must install the device between the Router and the phone jack. Use standard telephone cable with standard RJ-11 connectors. The splitter has three RJ-11 ports used to connect to the wall jack, the Router and if desired, a telephone or telephone device.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

Line - This port connects to the wall jack.

ADSL – This port connects to the Router.

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

The diagram below illustrates the proper use of the splitter.



Line Splitter Installation

International Offices

U.S.A

17595 Mt. Herrmann Street
Fountain Valley, CA. 92708
TEL: 714-885-6000
Fax 866-743-4905
URL: www.dlink.com

Canada

2180 Winston Park Drive
Oakville, Ontario, L6H 5W1
Canada
TEL: 1-905-8295033
FAX: 1-905-8295223
URL: www.dlink.ca

Europe (U. K.)

4th Floor, Merit House
Edgware Road, Colindale
London NW9 5AB
U.K.
TEL: 44-20-8731-5555
FAX: 44-20-8731-5511
URL: www.dlink.co.uk

Germany

Schwalbacher Strasse 74
D-65760 Eschborn
Germany
TEL: 49-6196-77990
FAX: 49-6196-7799300
URL: www.dlink.de

France

Le Florilege #.2, Allee de la Fresnerie
78330 Fontenay le Fleury
France
TEL: 33-1-30238688
FAX: 33-1-30238689
URL: www.dlink-france.fr

Netherlands

Weena 290
3012 NJ Rotterdam
Netherlands
Tel: +31-10-282-1445
Fax: +31-10-282-1331
URL: www.dlink-benelux.com

Belgium

Rue des Colonies 11
B-1000 Brussels
Belgium
Tel: +32(0)2 517 7111
Fax: +32(0)2 517 6500
URL: www.dlink-benelux.com

Italy

Via Nino Bonnet n. 6/b
20154 – Milano,
Italy
TEL: 39-02-2900-0676
FAX: 39-02-2900-1723
URL: www.dlink.it

Sweden

P.O. Box 15036, S-167 15 Bromma
Sweden
TEL: 46-(0)8564-61900
FAX: 46-(0)8564-61901
URL: www.dlink.se

Denmark

Naverland 2, DK-2600
Glostrup, Copenhagen,
TEL: 45-43-969040
FAX: 45-43-424347
URL: www.dlink.dk

Norway

Karihaugveien 89
1086 Oslo
Norway
TEL: 47-23-897189
FAX: 47-22-309085
URL: www.dlink.no

Finland

Pakkalankuja 7A
01510 Vantaa,
Finland
TEL : +358-9-2707 5080
FAX: + 358-9-2707 5081
URL: www.dlink.fi

Iberia

C/Sabino De Arana,
56 Bajos
08028 Barcelona
TEL: 34 93 4090770
FAX: 34 93 4910795
URL: www.dlinkiberia.es

Singapore

1 International Business Park
#03-12 The Synergy
Singapore 609917
TEL: 65-6774-6233
FAX: 65-6774-6322
URL: www.dlink-intl.com

Australia

1 Giffnock Avenue,
North Ryde, NSW 2113
Australia
TEL: 61-2-8899-1800
FAX: 61-2-8899-1868
URL: www.dlink.com.au

India

D-Link House, Kurla Bandra Complex
Road,
Off CST Road, Santacruz (East), Mumbai -
400098.
India
TEL: 91-022-26526696/56902210
FAX: 91-022-26528914
URL: www.dlink.co.in

Middle East (Dubai)

P.O.Box: 500376
Office No.:103, Building:3
Dubai Internet City
Dubai, United Arab Emirates
Tel:+971-4-3916480
Fax:+971-4-3908881
URL: www.dlink-me.com

Turkey

Regus Offices
Beybi Giz Plaza, Ayazaga Mah. Meydan
Sok. No:28
Maslak 34396, Istanbul-Turkiye
TEL: +90 212 335 2553
FAX: +90 212 335 2500
URL: www.dlink.com.tr

Egypt

19 El-Shahed Helmy, El Masri
Al-Maza, Heliopolis
Cairo, Egypt.
TEL: +202 414 4295
FAX: +202 415 6704
URL: www.dlink-me.com

Israel

11 Hamanofim Street
Ackerstein Towers, Regus Business Center
P.O.B 2148, Hertzelia-Pituach 46120.
Israel
TEL: +972-9-9715700
FAX: +972-9-9715601
URL: www.dlink.co.il

LatinAmerica

Isidora Goyechea 2934 of 702,
Las Condes
Santiago – Chile S.A.
TEL: 56-2-232-3185
FAX: 56-2-232-0923
URL: www.dlink.cl

Brasil

Av das Nacoes Unidas,
11857 - 14 - andar - cj 141/142
Brooklin Novo
Sao Paulo - SP - Brazil
CEP 04578-000
TEL: +55 11 55039320
FAX: +55 11 55039322
URL: www.dlinkbrasil.com.br

South Africa

Einstein Park II
Block B
102-106 Witch-Hazel Avenue
Highveld Technopark
Centurion
Gauteng
Republic of South Africa
TEL: 27-12-665-2165
FAX: 27-12-665-2186
URL: www..d-link.co.za

Russia

Grafsky per., 14, floor 6
Moscow
129626 Russia
TEL: 7-095-744-0099
FAX: 7-095-744-0099 #350
URL: www.dlink.ru

China

No.202,C1 Building, Huitong Office Park,
No.71, Jianguo Road, Chaoyang District,
Beijing,
100025, China.
TEL +86-10-58635800
FAX: +86-10-58635799
URL: www.dlink.com.cn

Taiwan

2F, No. 119, Pao-Chung Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2910-2626
FAX: 886-2-2910-1515
URL: www.dlinktw.com.tw

Headquarters

2F, No. 233-2, Pao-Chiao Rd.
Hsin-Tien, Taipei
Taiwan
TEL: 886-2-2916-1600
FAX: 886-2-2914-6299
URL: www.dlink.com

Registration Card

Print, type or use block letters.

Your name: Mr./Ms _____

Organization: _____ Dept. _____

Your title at organization: _____

Telephone: _____ Fax: _____

Organization's full address: _____

Country: _____

Date of purchase (Month/Day/Year): _____

Product Model	Product Serial No.	* Product installed in type of computer (e.g., Compaq 486)	* Product installed in computer serial No.

(* Applies to adapters only)

Product was purchased from:

Reseller's name: _____

Telephone: _____ Fax: _____

Reseller's full address: _____

Answers to the following questions help us to support your product:

1. Where and how will the product primarily be used?

Home Office Travel Company Business Home Business Personal Use

2. How many employees work at installation site?

1 employee 2-9 10-49 50-99 100-499 500-999 1000 or more

3. What network protocol(s) does your organization use ?

XNS/IPX TCP/IP DECnet Others _____

4. What network operating system(s) does your organization use ?

D-Link LANsmart Novell NetWare NetWare Lite SCO Unix/Xenix PC NFS 3Com 3+Open

Banyan Vines DECnet Pathwork Windows NT Windows NTAS Windows '95

Others _____

5. What network management program does your organization use ?

D-View HP OpenView/Windows HP OpenView/Unix SunNet Manager Novell NMS

NetView 6000 Others _____

6. What network medium/media does your organization use ?

Fiber-optics Thick coax Ethernet Thin coax Ethernet 10BASE-T UTP/STP

100BASE-TX 100BASE-T4 100VGAnyLAN Others _____

7. What applications are used on your network?

Desktop publishing Spreadsheet Word processing CAD/CAM

Database management Accounting Others _____

8. What category best describes your company?

Aerospace Engineering Education Finance Hospital Legal Insurance/Real Estate Manufacturing

Retail/Chainstore/Wholesale Government Transportation/Utilities/Communication VAR

System house/company Other _____

9. Would you recommend your D-Link product to a friend?

Yes No Don't know yet

10. Your comments on this product? _____

PLEASE
PLACE STAMP
HERE

TO:

D-Link®