D-Link®

# *DSL-G604T*
# *Wireless ADSL Router*
# *User's Guide*

(August 2004)

DSLG604TAUA3

**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.

# Table Of Contents

About This User's Guide ..... v

**BEFORE YOU START ..... V**
**Installation Overview ..... v**
The Setup Wizard ..... v

**INSTALLATION REQUIREMENTS ..... VI**

**PACKING LIST ..... IX**

**INTRODUCTION ..... 1**
Router Description and Operation ..... 1
Standards Compatibility and Compliance ..... 3
Front Panel Display ..... 4
Rear Panel Connections ..... 5
**Wireless LAN Basics ..... 6**
About 802.11g Wireless ..... 7

**HARDWARE INSTALLATION ..... 8**
**Choosing the Best Location for Wireless Operation ..... 8**
Power on Router ..... 9
Factory Reset Button ..... 9
Wired Network Connections ..... 10

**BASIC ROUTER CONFIGURATION ..... 12**
Configuring IP Settings on Your Computer ..... 12
**Access the Configuration Manager ..... 19**
Login to Home Page ..... 19
**Configure the Router ..... 20**
Using the Setup Wizard ..... 21
**Configure WAN Connection ..... 28**
PPPoE and PPPoA Connection for WAN ..... 29
Bridged Connection for WAN ..... 30
Static IP Address for WAN ..... 31
**LAN IP Settings ..... 32**
**DHCP Server Settings for the LAN ..... 33**
DNS Server Settings ..... 34
**Basic Wireless LAN Setup ..... 35**

**ADVANCED ROUTER MANAGEMENT ..... 36**
Port Forwarding ..... 37
Filters ..... 39
DMZ ..... 41
Firewall ..... 42
Static Routing ..... 43
Dynamic Routing (RIP) ..... 44
ATM VC ..... 45
**Advanced Wireless LAN Configuration ..... 46**

Wireless Performance ..... 46
Wireless Security ..... 47
SSID and Channel ..... 48
WEP Encryption ..... 48
**Tools and Utilities ..... 51**
Change System Password ..... 52
Save Router Configuration Settings ..... 52
Save or Load Configuration File ..... 53
Restore Factory Default Settings ..... 53
Time & Date ..... 54
Firmware Upgrade ..... 55
**Router Status Information ..... 56**
Device Information Display ..... 56
**Multiple Virtual Connections ..... 57**

**TECHNICAL SPECIFICATIONS ..... 59**

**IP ADDRESS SETUP ..... 61**

**IP CONCEPTS ..... 63**

**MICROFILTERS AND SPLITTERS ..... 66**

## About This User's Guide

This user's guide provides instructions on how to install the DSL-G604T Wireless ADSL Router and use it to provide Internet access for an Ethernet or 802.11g/802.11b wireless LAN.

If you are using a computer with a functioning Ethernet port, the quickest and easiest way to set up the DSL-G604T is to insert the Installation CD into the CD-ROM drive of your computer and follow the instructions provided in the **Quick Installation Guide**.

# Before You Start

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

## *Installation Overview*

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

1. Gather information and equipment needed to install the device. Before you begin the actual installation make sure you have all the necessary information and equipment.
2. Install the hardware, connect the cables 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 service and wireless LAN.

## The Setup Wizard

Many users will be able to configure all the settings necessary to use the DSL-G604T with the Setup Wizard. For ADSL connections that use PPPoE or PPPoA connections, the simplest way to setup the DSL-G604T is to use the Setup Wizard to configure the Internet connection. Once you access the web interface used to configure the device, just launch the Setup Wizard to configure your Internet connection and enable the 802.11g/802.11b wireless function, including wireless security.

# Installation Requirements

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

## Low Pass Filters

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

## Operating Systems

The DSL-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 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.

## Wireless LAN Configuration

Wireless LAN settings for 802.11g and 802.11b wireless operation must be enabled using the Setup Wizard before it can be configured. Basic wireless settings including the Channel and SSID can be configured through the Setup Wizard. Advanced wireless security settings can also be configured with the Setup Wizard.

Security for wireless communication can be accomplished in a number of ways. The DSL-G604T supports WEP, WPA and WPA -PSK.

## Additional Software

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

If your ADSL service is delivered through a PPPoE, PPPoA or Static IP connection, the information needed to establish and maintain the Internet connection can be stored in the Router. In this case, it is not necessary to

install software on your computer. It may however be necessary to change some settings in the device, including account information used to identify and verify the connection.

## *Information you will need from your ADSL service provider:*

| | | |
|---|---|---|
| **Username** | This is the Username used to log on to your ADSL service provider's network. It is commonly in the form – user@isp.com. Your ADSL service provider uses this to identify your account. | Record info here |
| **Password** | This is the Password used, in conjunction with the Username above, to log on to your ADSL service provider's network. This is used to verify the identity of your account. | |
| **Connection and Encapsulation Type** | This is the method your ADSL service provider uses to transport data between the Internet and your computer. Most users will use the default PPPoE/PPPoA, connection type. Ithe Setup Wizard can be used to configure a PPPoE/PPPoA connection type. You may need to specify one of the following connection types (PPPoE LLC, PPPoA LLC or PPPoA VC-MUX). The other available connection and encapsulation combinations must be configured using the web manager. These include Bridge Mode (1483 Bridged IP LLC or 1483 Bridged IP VC-MUX), and Static IP (Bridged IP LLC, 1483 Bridged IP VC-MUX, 1483 Routed IP LLC, 1483 Routed IP VC-MUX or IPoA). | |
| **VPI** | Most users will not be required to change this setting. The Virtual Path Identifier (VPI) is used in conjunction with the Virtual Channel Identifier (VCI) to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN menu of the web management interface. | |
| **VCI** | Most users will not be required to change this setting. The Virtual Channel Identifier (VCI) used in conjunction with the VPI to identify the data path between your ADSL service provider's network and your computer. If you are setting up the Router for multiple virtual connections, you will need to configure the VPI and VCI as instructed by your ADSL service provider for the additional connections. This setting can be changed in the WAN menu of the web management interface. | |

**Note**

*The Setup Wizard can be used to configure the Internet connection for most users. If you are using a PPPoE or PPPoA type connection use the Setup Wizard to establish the Internet connection.*

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

| | | |
|---|---|---|
| **Username** | This is the Username needed access the Router's management interface. When you attempt to connect to the device through a web browser you will be prompted to enter this Username. The default Username for the Router is **admin**. The user cannot change this. | Record info here |
| **Password** | This is the Password you will be prompted to enter when you access the Router's management interface. The default Password is **admin**. The user may change this. | |
| **LAN IP addresses for the DSL-G604T** | This is the IP address you will enter into the Address field of your web browser to access the Router's configuration graphical user interface (GUI) using a web browser. The default IP address is 10.1.1.1 and it is referred to as the "Management IP" address in this User's Manual. This may be changed to suit any IP address scheme the user desires. This address will be the base IP address used for DHCP service on the LAN when DHCP is enabled. | |
| **LAN Subnet Mask for the DSL-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**. This can be changed later. | |

### *Information you will need about your LAN or computer:*

| | | |
|---|---|---|
| **Ethernet NIC** | If your computer has an Ethernet NIC, you can connect the DSL-G604T to this Ethernet port using an Ethernet cable. You can also use the Ethernet ports on the DSL-G604T to connect to other computer or Ethernet devices. | Record 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 default 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 your collect and record this information here, or in some other secure place, in case you have to re-configure your ADSL connection in the future.

Once you have the above information, you are ready to setup and configure your DSL-G604T ADSL Router.

# Packing List

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

1. One DSL-G604T 802.11g Wireless ADSL Ethernet Router
2. One CD-ROM containing the User's Guide
3. One twisted-pair telephone cable used for ADSL connection
4. One straight-through Ethernet cable
5. One AC power adapter suitable for your electric service
6. One Quick Installation Guide

# Introduction

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

## Router Description and Operation

The DSL-G604T Router is designed to provide a simple and cost-effective ADSL Internet connection for a private Ethernet or 802.11g/802.11b wireless network. The Router combines high-speed ADSL Internet connection, IP routing for the LAN and wireless connectivity in one package.

The Router is easy to install and use. The DSL-G604T connects to an Ethernet LAN or computers via standard Ethernet ports. The ADSL connection is made using ordinary telephone line with standard connectors. Multiple workstations can be networked and connected to the Internet using a single Wide Area Network (WAN) interface and single global IP address. The advanced security enhancements, packet filtering and port redirection, can help protect your network from potentially devastating intrusions by malicious agents from outside your network.

### ADSL

Asymmetric Digital Subscriber Line (ADSL) is a broadband network technology that utilizes standard twisted-pair copper wire telephone lines to enable broadband high-speed digital data transmission and bandwidth hungry applications for business and residential customers.

ADSL routers and modems provide faster downloads and more reliable connectivity to the user without loss of quality or disruption of voice/fax telephone capabilities.

ADSL service operates at speeds of up to 8 Mbps downstream and up to 640 Kbps upstream. A secure dedicated point-to-point connection is established between the user and the central office of the service provider.

### 802.11g Wireless

The embedded 802.11g wireless access point provides Internet access and connectivity to the Ethernet for 802.11g and 802.11b wireless workstations. IEEE 802.11g is fully compatible with IEEE 802.11b wireless devices. The 802.11g standard supports data transfer rates of up to 54 Mbps. The Router's wireless access point supports common security protocols used for wireless LAN including WEP encryption, 802.1x and WPA.

## Router Features

The DSL-G604T Wireless ADSL Router utilizes the latest ADSL enhancements to provide a reliable Internet portal suitable for most small to medium sized offices. DSL-G604T advantages include:

- **802.11g Wireless Access Point** – The built-in 802.11g wireless access point connects 802.11g and 802.11b wireless devices to the Internet and the Ethernet.
- **PPP (Point-to-Point Protocol) Security –** The DSL-G604T ADSL Router supports PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol) for PPP connections.
- **DHCP Support –** Dynamic Host Configuration Protocol automatically and dynamically assigns al LAN IP settings to each host on your network. This eliminates the need to reconfigure every host whenever changes in network topology occur.
- **Network Address Translation (NAT) –** For small office environments, the DSL-G604T allows multiple users on the LAN to access the Internet concurrently through a single Internet account. This provides Internet access to everyone in the office for the price of a single user.

  NAT improves network security in effect by hiding the private network behind one global and visible IP address. NAT address mapping can also be used to link two IP domains via a LAN-to-LAN connection.
- **TCP/IP (Transfer Control Protocol/Internet Protocol) –** The DSL-G604T supports TCP/IP protocol, the language used for the Internet. It is compatible with access servers manufactured by major vendors.
- **RIP-1/RIP-2 –** The DSL-G604T supports both RIP-1 and RIP-2 exchanges with other routers. Using both versions lets the Router to communicate with all RIP enabled devices.
- **Static Routing –** This allows you to select a data path to a particular network destination that will remain in the routing table and never "age out". If you wish to define a specific route that will always be used for data traffic from your LAN to a specific destination within your LAN (for example to another router or a server) or outside your network (to a ISP defined default gateway for instance).
- **Default Routing –** This allows you to choose a default path for incoming data packets for which the destination address is unknown. This is particularly useful when if the Router functions as the sole connection to the Internet.
- **ATM (Asynchronous Transfer Mode) –** The DSL-G604T supports Bridged Ethernet over ATM (RFC1483), IP over ATM (RFC1577) and PPP over ATM (RFC 2364).
- **Precise ATM Traffic Shaping –** Traffic shaping is a method of controlling the flow rate of ATM data cells. This function helps to establish the Quality of Service for ATM data transfer.
- **G.hs (Auto-handshake) –** This allows the Router to automatically choose either the G.lite or G.dmt ADSL connection standards.
- **High Performance –** Very high rates of data transfer are possible with the Router. Up to eight Mbps downstream bit rate using the G.dmt standard.
- **Full Network Management –** The DSL-G604T incorporates SNMP (Simple Network Management Protocol) support for web-based management and text-based network management via an RS-232 or Telnet connection.
- **Telnet Connection –** The Telnet enables a network manager to access the Router's management software remotely.
- **Easy Installation –** The DSL-G604T uses a web-based graphical user interface program for convenient management access and easy set up. Any common web browser software can be used to manage the Router.

# Standards Compatibility and Compliance

The DSL-G604T complies with or is compatible with the following standards as recognized by their respective agencies.

- ITU G.992.2 (G.lite) compliant
- ITU-T Rec. I.361 compliant
- RFC 791 Internet Protocol compliant
- RFC 792 UDP compliant
- RFC 826 Address Resolution Protocol compliant (ARP) compliant
- RFC 1058 Routing Information Protocol (RIP) compliant
- RFC 1213 MIB II for IP compliant
- RFC 1334 PPP Authentication Protocol compliant
- RFC 1389 Routing Information Protocol 2 (RIP2) compliant
- RFC 1483 IP over AAL5/ Bridged Ethernet over AAL5 compliant
- RFC 1557 Classical IP over ATM (IPoA) compliant
- RFC 1661 Point to Point Protocol (PPP) compliant
- RFC 1877 Automatic IP assignment compliant
- RFC 1994 Challenge Handshake Authentication Protocol compliant
- Supports RFC 2131 and RFC 2132 DHCP functions including: automatic assignment of IP address, use of subnet mask and default gateway and provision of DNS server address for all hosts
- RFC 2364 PPP over ATM compliant (PPPoA) compliant
- RFC 2516 PPP over Ethernet compliant (PPPoE) compliant
- RFC 2684 Bridged/Routed Ethernet over ATM compliant
- IEEE 802.3 compliant
- IEEE 802.3u compliant
- IEEE 802.1d compliant
- IEEE 802.11g compliant
- IEEE 802.3x compliant
- Embedded web server support
- Supports Dynamic Learning
- Supports Static Routing
- Supports NAPT for up to 4096 connections
- Supports DHCP for up to 253 hot connections
- Supports IGMP
- Supports ATM Forum UNI 3.1/4.0
- Supports ATM VCC (Virtual Channel Circuit) for up to eight sessions
- Supports TELNET and TFTP
- Supports back pressure for half-duplex

# Front Panel Display

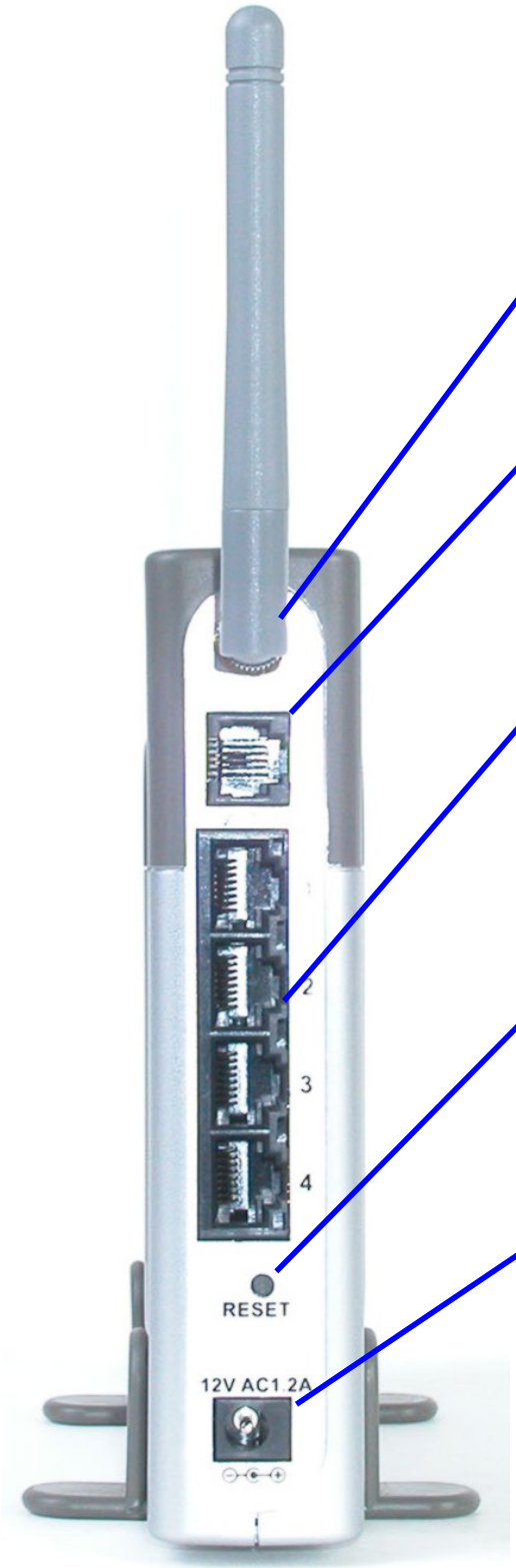
Place the Router in a location that permits an easy view of the LED indicators on the front panel.

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

| | |
|---|---|
| **Power** | 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 Connections

All cable connections to the Router are made at the rear panel. Connect the power adapter here to power on the Router. Use the Reset button to restore the settings to the factory default values in the next chapter for instructions on using the reset button).




**Antenna**

For wireless operation, mount the antenna on the threaded antenna post

**ADSL Port**

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

**Ethernet ports**

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

**Reset button**

To manually reset, depress button with the power on for at least seven seconds

**Power Insert**

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

**Note**

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

# *Wireless LAN Basics*

Some basic understanding of 802.11b/g 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 he 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.

2

# Hardware Installation

The DSL-G604T maintains three separate interfaces, an Ethernet LAN, a wireless LAN and an ADSL (WAN) interface. Place the Router in a location where it can be connected to the various devices as well as to a power source. The Router should not be located where it will be exposed to moisture or excessive heat. Make sure the cables and power cord are placed safely out of the way so they do not create a tripping hazard. As with any electrical appliance, observe common sense safety procedures.

The Router 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.

## *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 meters indoors and up to 300 meters outdoors, Wireless LAN lets you access your network from anywhere you want. However, the number of walls, ceilings, or other objects that the wireless signals must pass through can limit 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 minimized.

2. **Consider the direct line between access points and workstations:** A wall that is 0.5 meters thick, at a 45-degree angle appears to be almost 1 meter thick. At a 2-degree angle, it is over 14 meters thick. Be careful to position access points and client adapters so the signal can travel straight through (90º angle) a wall or ceiling for better reception.

3. **Building Materials make a difference:** Buildings constructed using metal framing or doors can reduce effective range of the device. If possible, position wireless devices so that their signal can pass through drywall or open doorways, avoid positioning them so that their signal must pass through metallic materials. Poured concrete walls are reinforced with steel while cinderblock walls generally have little or no structural steel.

4. **Position the antennas for best reception.** Play around with the antenna position to see if signal strength improves. Some adapters or access points allow the user to judge the strength of the signal.

5. **Keep your product away (at least 1-2 meters) from electrical devices:**
   Position wireless devices away from electrical devices that generate RF noise such as microwave ovens, monitors, electric motors, etc.

# Power on Router

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

To power on the Router:

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

# Factory Reset Button

The Router may be reset to the original factory default settings by depressing the reset button for a few seconds while the device is powered on. Use a ballpoint or paperclip to gently push down the reset button. Remember that this will wipe out any settings stored in flash memory including user account information and LAN IP settings. The device settings will be restored to the factory default IP address 10.1.1.1 and the subnet mask is 255.0.0.0, the default management Username is **admin** and the default Password is **admin**.

# Wired Network Connections

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

## Connect ADSL Line

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

## Connect Router to Ethernet

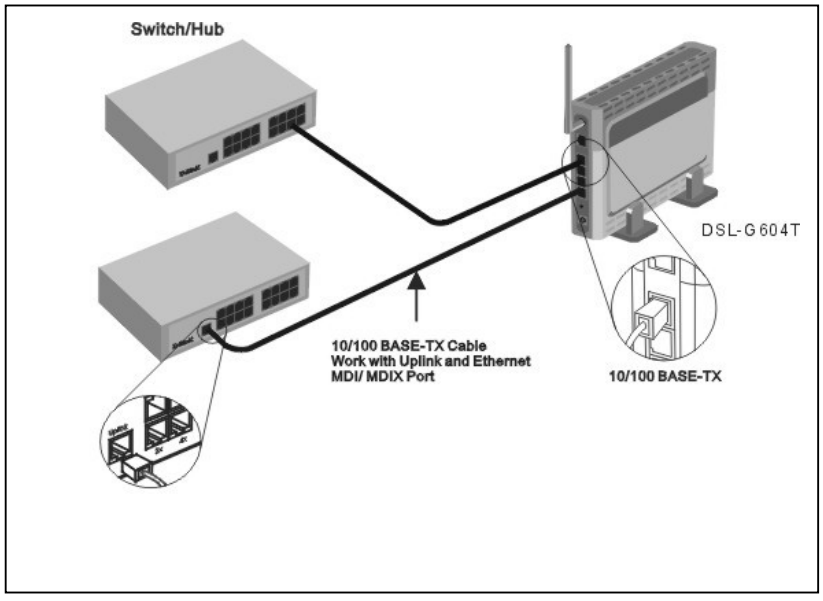
The Router may be connected to a single computer or Ethernet device through the 10/100 BASE-TX Ethernet port on the rear panel. Any connection to an Ethernet concentrating device such as a switch or hub must operate at a speed of 10/100 Mbps only. When connecting the Router to any Ethernet device that is capable of operating at speeds between 0~100Mbps, be sure that the device has auto-negotiation (NWay) enabled for the connecting port.

Use standard twisted-pair cable with RJ-45 connectors. The RJ-45 port on the Router is a crossed port (MDI-X). Follow standard Ethernet guidelines when deciding what type of cable to use to make this connection. When connecting the Router directly to a PC or server use a normal straight-through cable. You should use a crossed cable when connecting the Router to a normal (MDI-X) port on a switch or hub. Use a normal straight-through cable when connecting it to an uplink (MDI-II) port on a hub or switch.

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

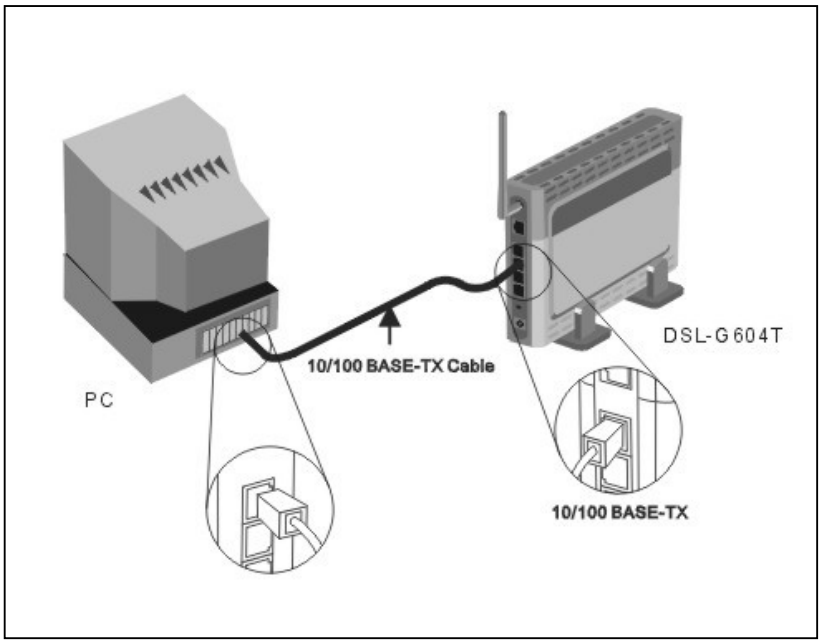
## Hub or Switch to Router Connection

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



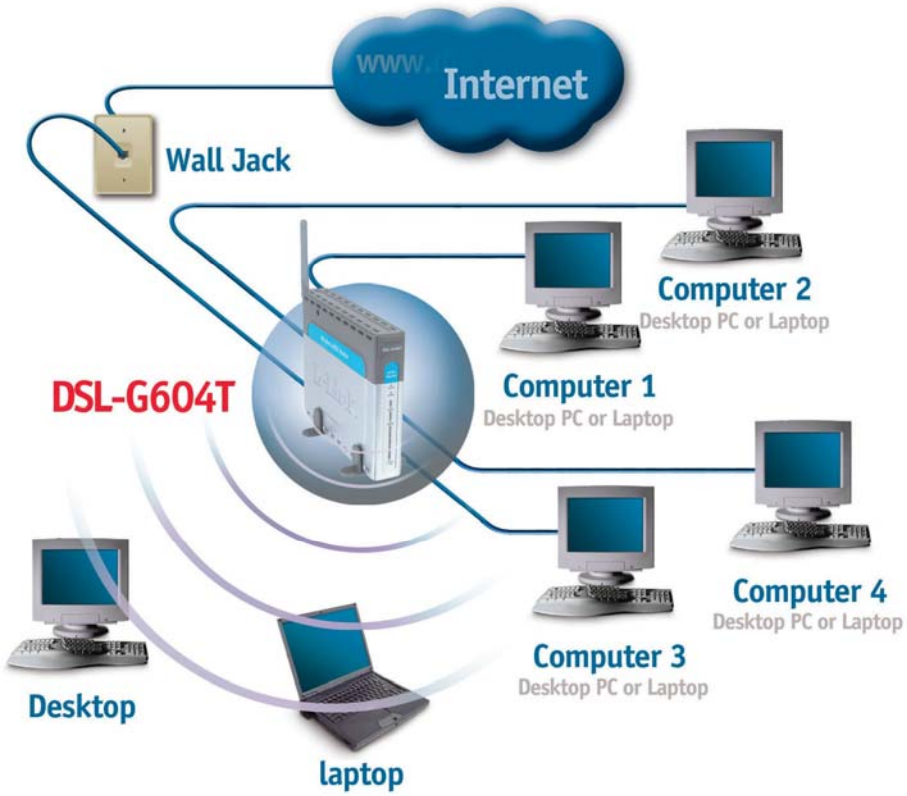

If you wish to reserve the uplink port on the switch or hub for another device, connect to any on the other MDI-X ports (1x, 2x, etc.) with a crossed cable.

## Computer to Router Connection




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

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



3

# Basic Router Configuration

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

### Wan Configuration Summary

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

## Configuring IP Settings on Your Computer

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

For computers running non-Windows operating systems, follow the instructions for your OS that configure the system to receive an IP address from the Router, that is, configure the system to be a DHCP client.

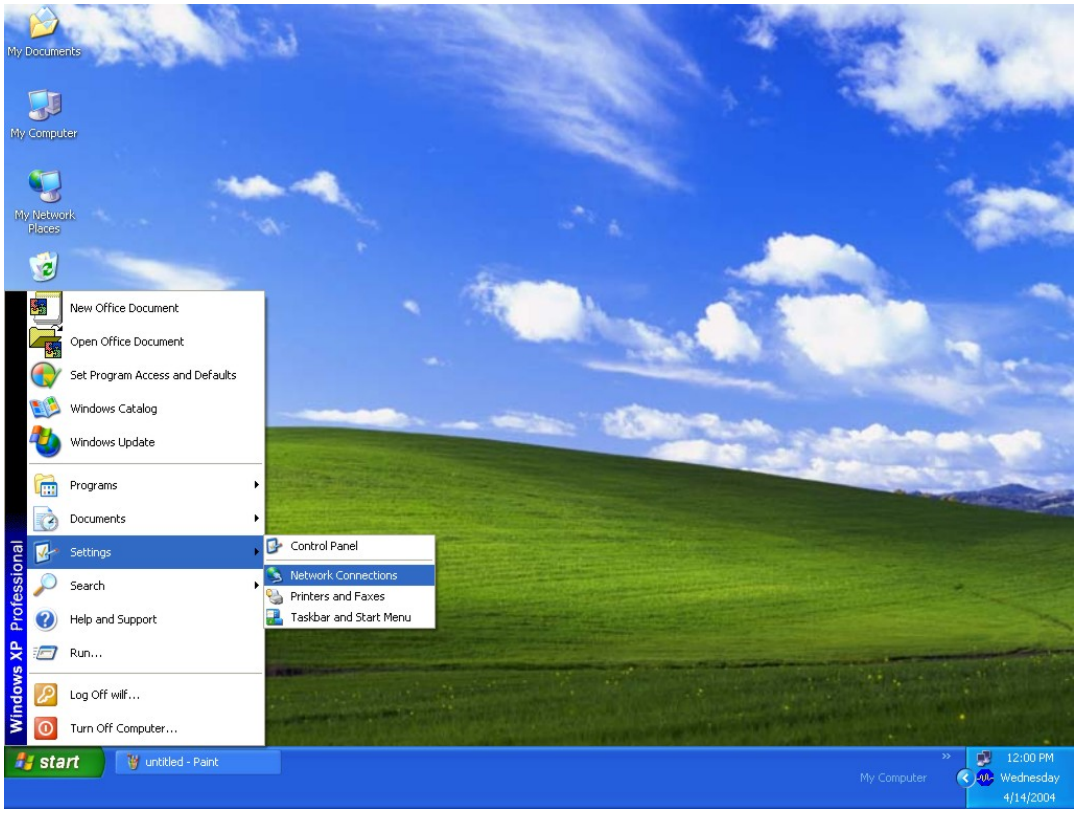
**Note**

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

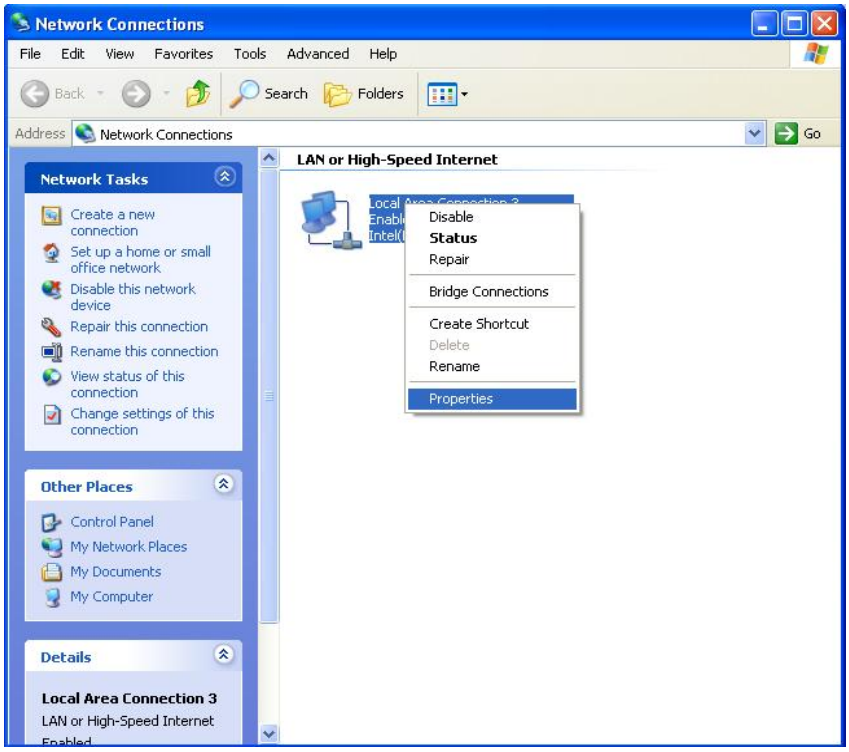
## Configure Windows XP for DHCP

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

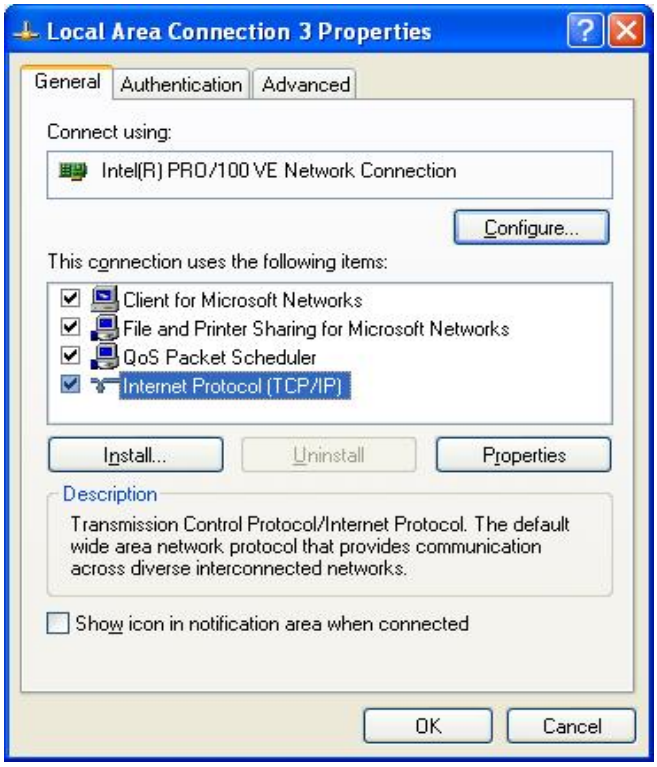
1. From the **Start** menu on your desktop, go to **Settings**, then click on **Network Connections**.



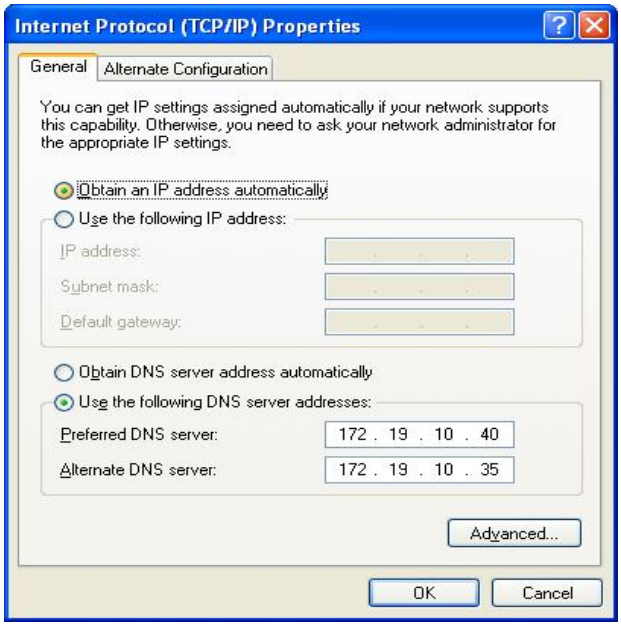
2. In the **Network Connections** window, right-click on **LAN** (Local Area Connection), then click **Properties**.




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




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




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

## Windows 2000

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

1. In the **Windows** task bar, click the **Start** button, point to **Settings**, and then click **Control Panel**.
2. Double-click the **Network and Dial-up Connections** icon.

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

## Configure Windows 2000 for DHCP

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

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

## Windows ME

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

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

## Configure Windows ME for DHCP

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

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

## Windows 95 and Windows 98

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

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

## Configure Windows 95 and Windows 98 for DHCP

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

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

## Windows NT 4.0 Workstations

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

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

## Configure Windows NT 4.0 for DHCP

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

# Access the Configuration Manager

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

Note

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

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

*Alternatively, you can access this **Internet Options** menu using the **Tools** pull-down menu in Internet Explorer.*

## Login to Home Page

To use the web-based management software, launch a suitable web browser and direct it to the IP address of the Router. Type in **http://** followed by the default IP address, **10.1.1.1** in the address bar of the browser. The URL in the address bar should read: **http://10.1.1.1**.

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

**Figure 3-1. Enter Password**

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

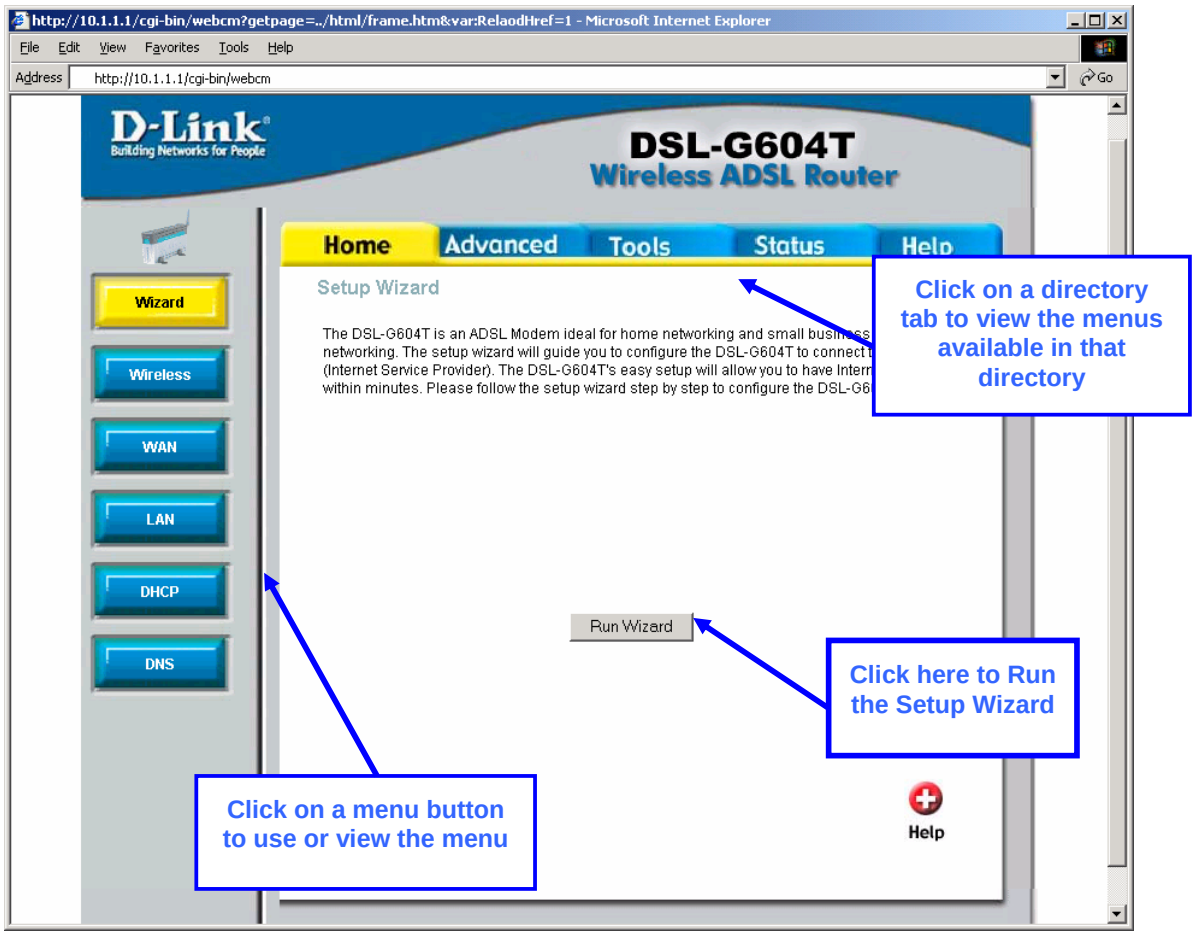
Note

*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 Internet.*

# Configure the Router

When you successfully connect to the web manager, the **Home** directory tab will display the **Setup Wizard** menu. You can launch the Setup Wizard from this page or use the menu buttons located in the left panel of the web page to view other menus used for basic configuration. You may use the Setup Wizard if your Internet connection is a PPPoE connection. If you are using a PPPoE and connection and want to use the Setup Wizard, follow the instructions below. If your Internet connection is a Bridge or Static IP type connection, you should follow the instructions below in the section **Configure WAN Connection**.

When you successfully connect to the web manager, the **Home** directory tab will display the **Setup Wizard** menu. You can launch the Setup Wizard from this page or use the menu buttons located in the left panel of the web page to view other menus used for basic configuration. You may use the Setup Wizard if your Internet connection is a PPPoE connection. If you are using a PPPoE and connection and want to use the Setup Wizard, follow the instructions below. If your Internet connection is a PPPoA, Bridge, Static IP, or Dynamic IP type connection, you should follow the instructions below in the section **Configure WAN Connection**.




**Web Manager – First Time Log On**

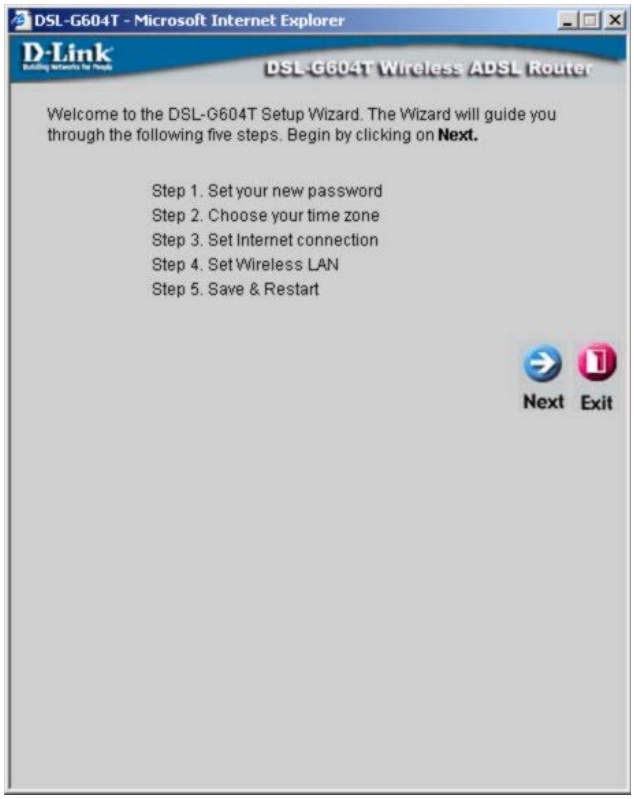
All configuration and management of the Router is done using the web-based management interface pictured in the above example. The various menus accessed by clicking on one of the directory tabs, Home, Advanced, Tools, Status and Help. Each tab displays menu buttons located in the left hand panel of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

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

# Using the Setup Wizard

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

The first window summarizes the setup process. Click the **Next** button to proceed. You may stop using the Setup Wizard at any time by clicking the **Exit** button. If you exit the wizard you will return to the first page without saving any of the settings changed during the process.




The first window of the Setup Wizard lists the basic steps in the process. These steps are as follows:

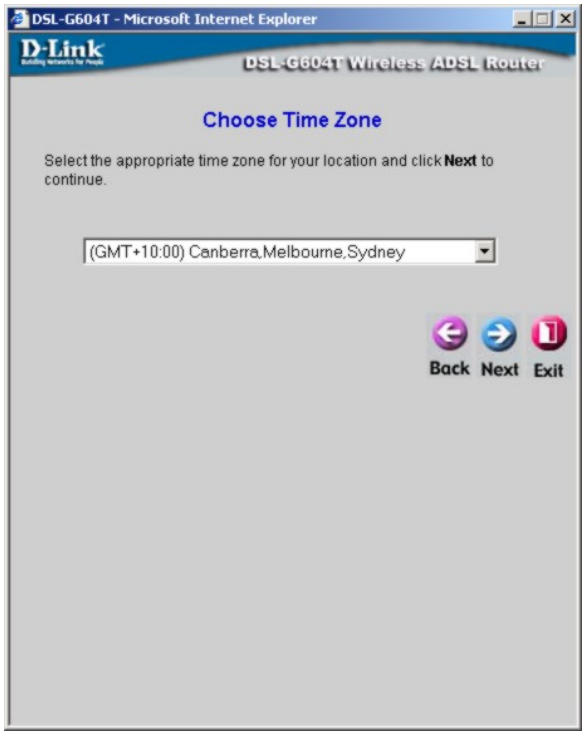
1. Set your new system password.
2. Set the system time.
3. Configure the connection to the Internet.
4. Configure Wireless LAN settings.
5. Save the new configuration settings and reboot the system.

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

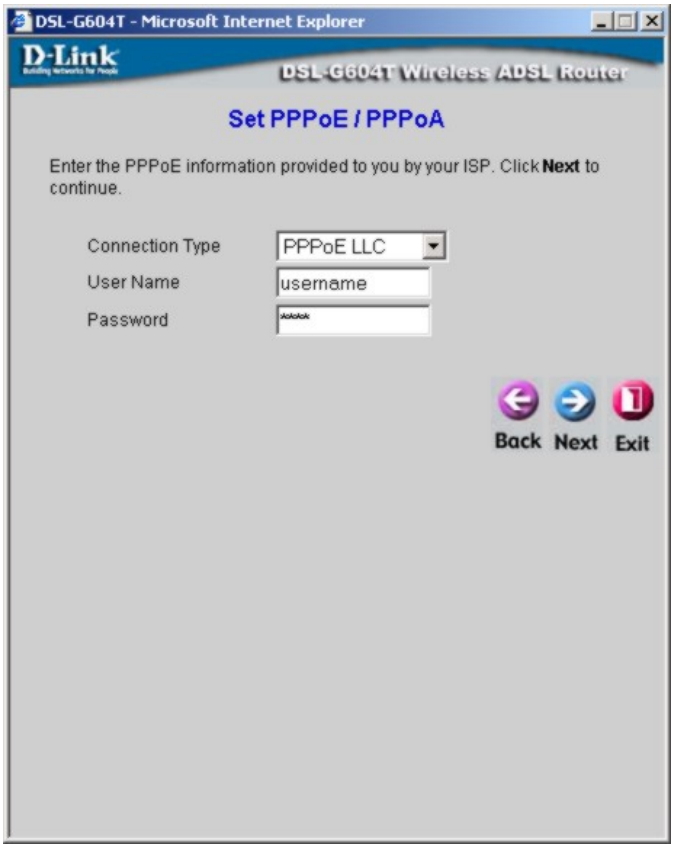
**Note**

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

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



Now select the Connection Type for the Internet and enter your account User Name and Password. Your ISP has given this information to you. The connection types available in the Setup Wizard menu are PPPoE LLC, PPPoA LLC and PPPoA VC-MUX. For Bridge Mode and Static IP connections, use the WAN menu in the Home directory to configure the connection (see instruction in the next section).

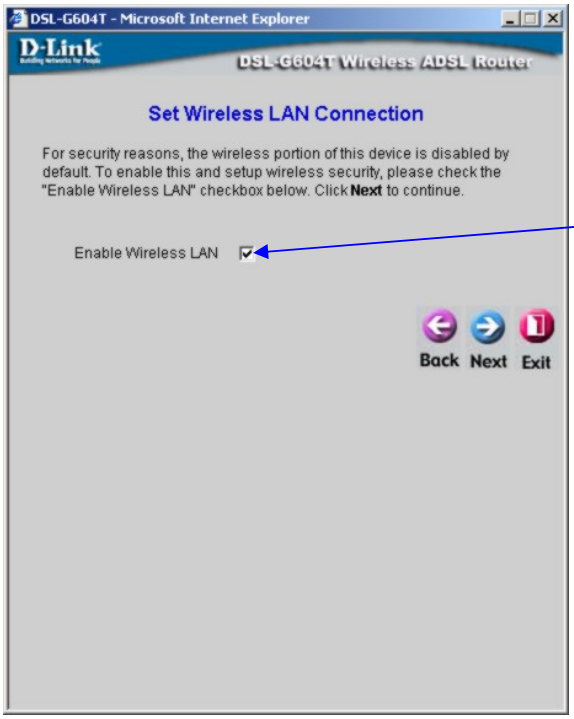



1. Select the **Connection Type** specific to your service.
2. Type in the **Username** and **Password** used to identify and verify your account to the ISP.
3. Click **Next** to proceed to the wireless settings menu.

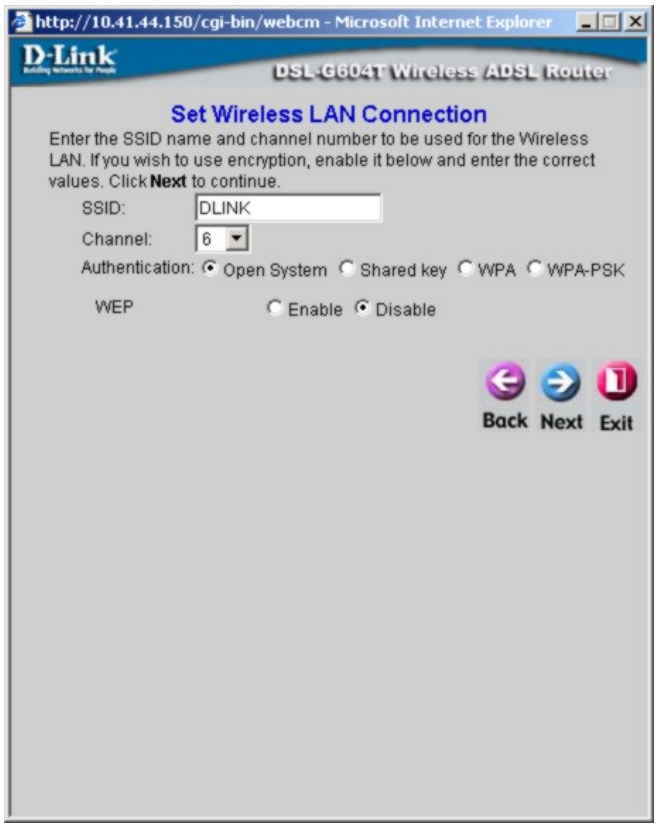
**Note**

*If your service provider has instructed you to change the VPI or VCI value for your ADSL connection, use the WAN menu to change these.*

Wireless LAN operation must be enabled before any settings can be configured. To enable Wireless LAN function, click the **Enable Wireless LAN** option box to select it. If you do not want to enable the Wireless LAN connection now, leave the box empty and click **Next to** continue to the final step of the Setup Wizard. If you enable Wireless LAN now, configure the wireless settings in the next step. Click **Next** to continue.




Check this box to enable wireless access to the Router.



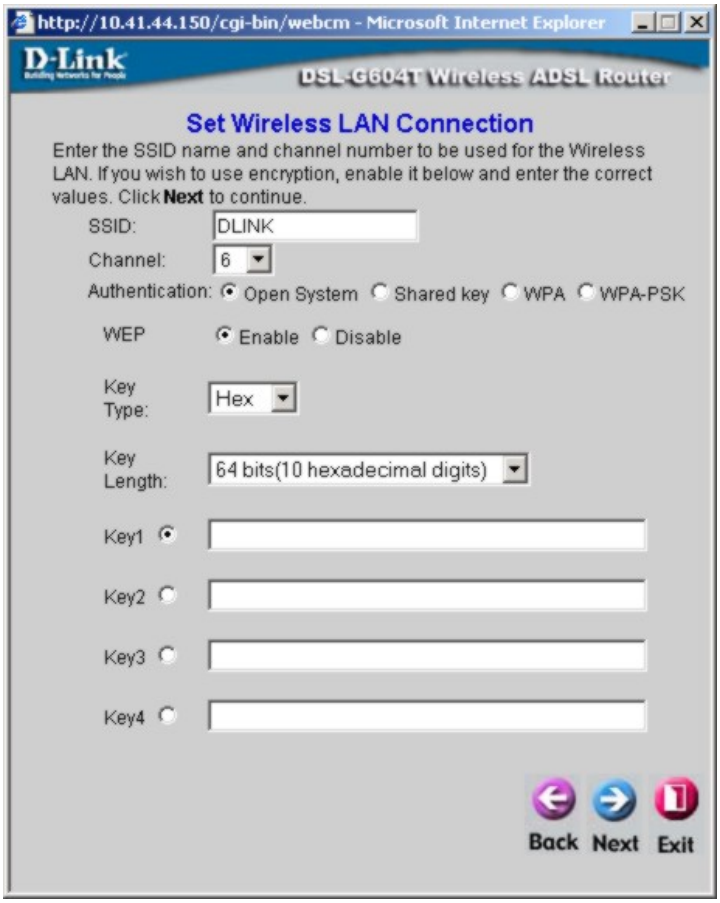

Configure the **SSID** and **Channel** according to the requirements of your network. The default settings use an **Open System** for wireless **Authentication** and WEP is disabled. Open System Authentication to allow any wireless station to associate with the access point. You can accept the default settings and click **Next** to proceed to the final step. Wireless LAN security can be configured at any time using the Wireless menu in the Home directory.

If you choose to change the Authentication to Shared key, WPA or WPA-PSK; or if you enable WEP using the Setup Wizard, the dialog box will present a menu for configuring these options.

Select **Shared key** to only allow stations using a shared key encryption to associate with it. The shared key is configured the same way WEP keys are configured. See below for a description.

## WEP Settings in the Setup Wizard

WEP is disabled by default. To enable **WEP**, click the **Enable** radio button. The menu will change to present additional settings to configure the WEP keys.




**Note**

*The SSID can be a continuous character string (i.e. no spaces) of up to 16 characters in length.*

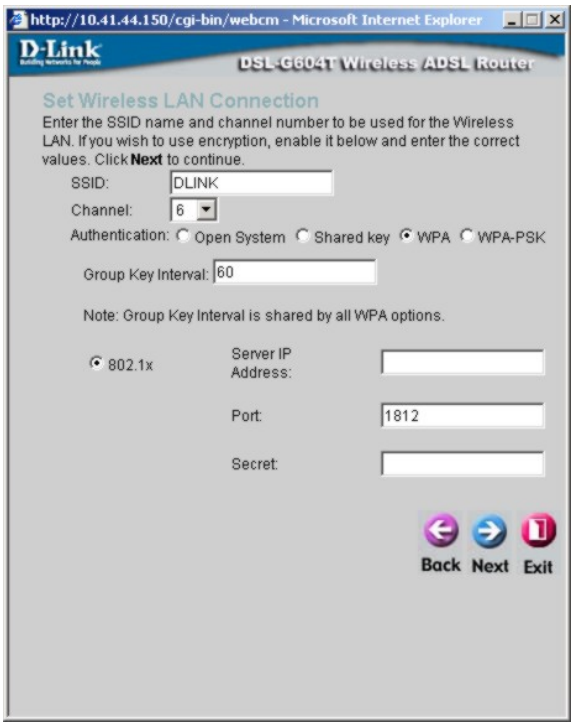
To configure the WEP keys (or shared keys for authentication), select the **Key Type** (Hex or ASCII) the **Key Length** (64, 128 or 256 bits) and type the keys of the appropriate length in the 4 spaces provided. Click one of the radio buttons (**Key 1 – Key 4**) to select the active key.

Click the **Next** button to proceed to the final step.

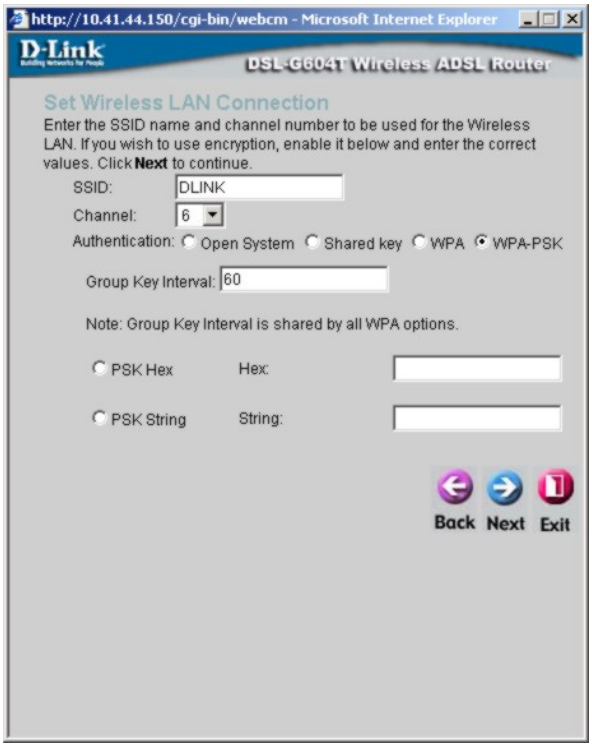
For a more complete description of Keys read the discussion of wireless LAN security in the next chapter.

## WPA and WPA-PSK Authentication Settings in the Setup Wizard

WPA authentication can be used on networks that employ 802.1x authentication.

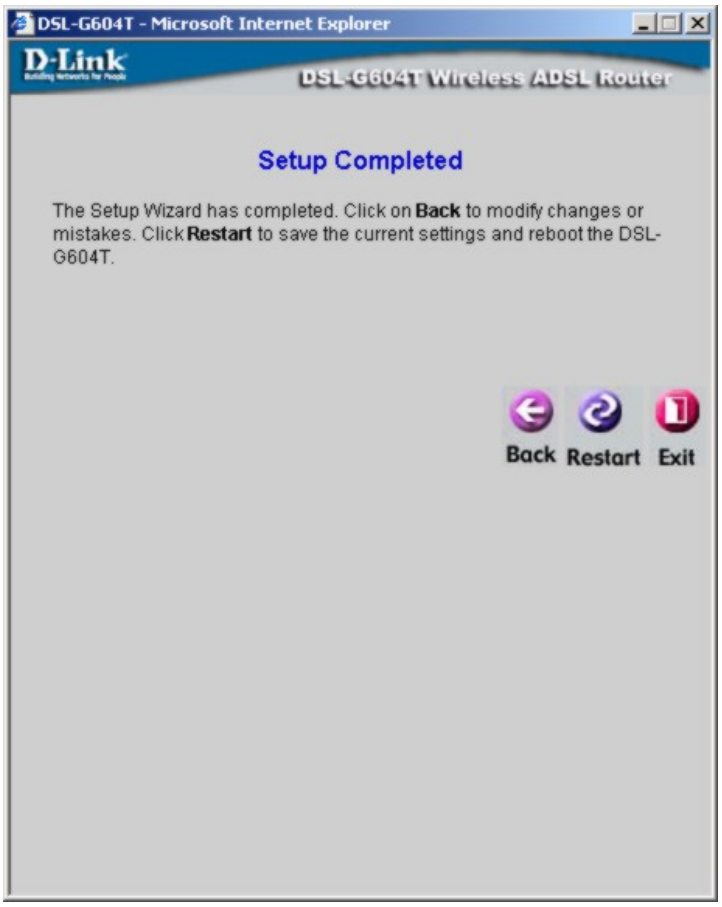



To configure WPA Authentication, type in the **Group Key Interval**, RADIUS **Server IP Address** and **Secret** in the spaces provided. If you are using a different port number for WPA, type that in as well. Click the **Next** button to continue to the final step.



For WPA-PSK, select **PSK Hex** or **PSK String** and type in the desired value in the space provided. Click the **Next** button to continue to the final step.

Finally you can confirm that the setup process is completed. If you are satisfied that you have entered all the necessary information correctly, click the **Restart** button to save the new configuration settings and restart the Router. If you need to change settings from a previous menu, click the **Back** button.

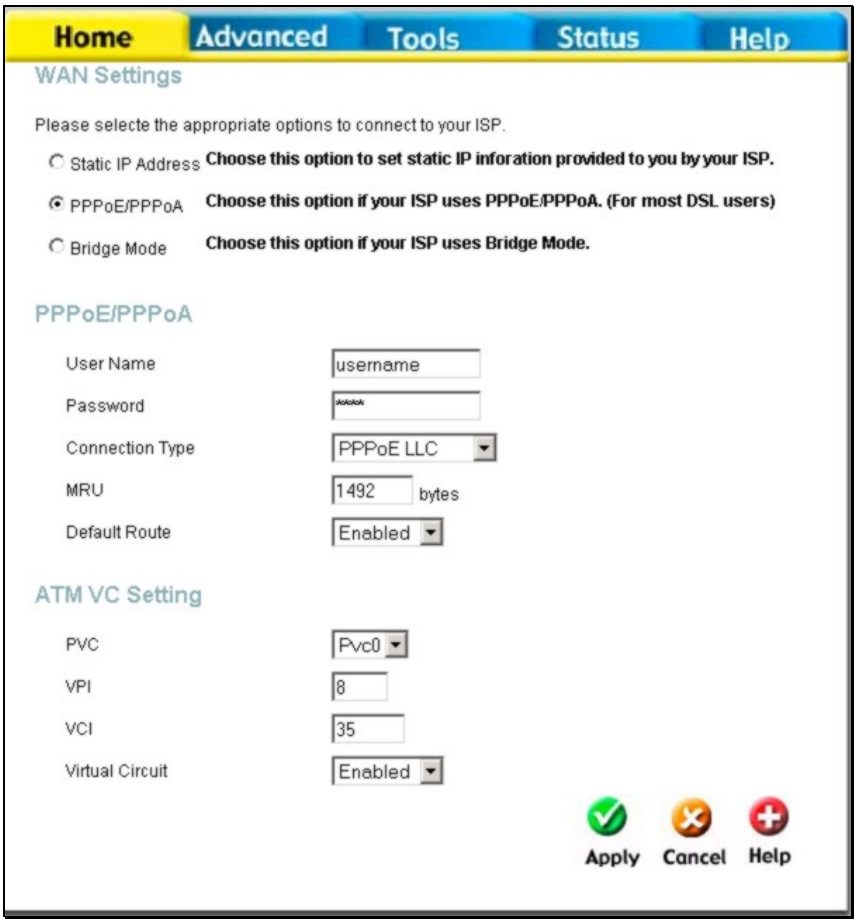



Do not turn the Router off while it is restarting. When it is finished rebooting, click **Close** to close the box and continue to configure the Router as desired.

# Configure WAN Connection

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

The WAN Settings menu is also used to configure the Router for multiple virtual connections (Multiple PVCs). The next chapter contains a section describing how to set up multiple PVCs on the Router.




**WAN Settings Menu – PPPoE / PPPoA**

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

# PPPoE and PPPoA Connection for WAN

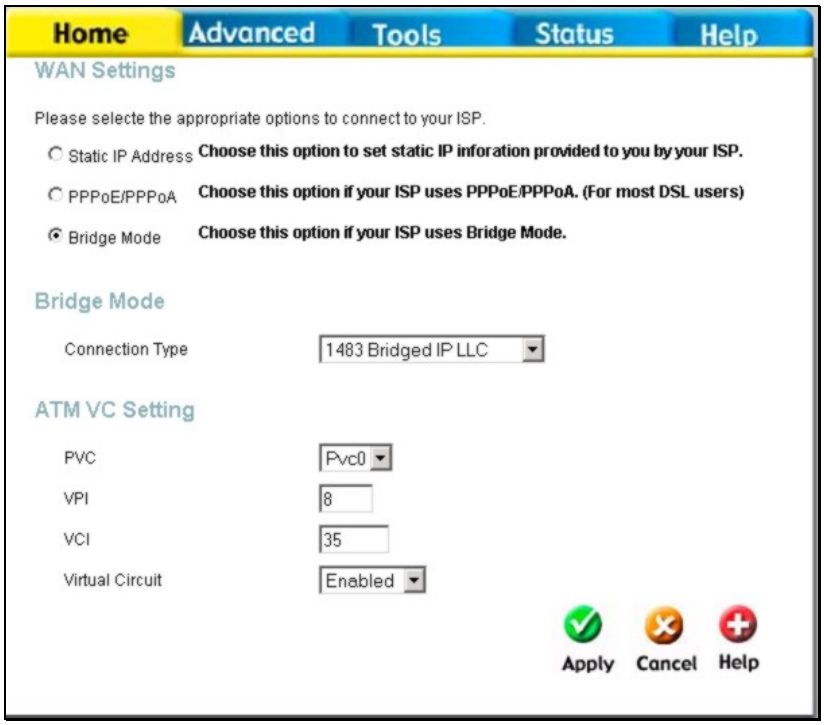
Follow the instructions below to configure the Router to use a PPPoE or PPPoA for the Internet connection. Make sure you have all the necessary information before you configure the WAN connection.

1. Click to select the **PPPoE/PPPoA** radio button in the **WAN Settings** options list. This is selected by default if you are configuring the Router for the first time. If it is not selected, click the **PPPoE/PPPoA** radio button located under the **WAN Settings** heading.
2. The **ATM VC Settings** at the top of the menu should not be changed unless you have been instructed to change them. However, if you are instructed to change the **VPI** or **VCI** values, type in the values assigned for your account. Leave the **PVC** and **Virtual Circuit** settings at their default (*Pcv0* and *Enabled*) values for now. These can be used later if you are configuring multiple virtual circuits for your ADSL service.
3. Under the **PPPoE/PPPoA** heading, type the **User Name** and **Password** used for your ADSL account. A typical User Name will be in the form user@isp.com.au, the Password may be assigned to you by your ISP or you may have selected it when you set up the account with your ISP.
4. Choose the **Connection Type** from the pull-down menu located under the User Name and Password entry fields. This defines both the connection protocol and encapsulation method used for your ADSL service. The available options are *PPPoA VC-MUX*, *PPPoA LLC* and *PPPoE LLC.* If have not been provided specific information for the Connection Type setting, leave the default setting.
5. Leave the **MRU** value at the default setting (default = 1492) unless you have been instructed to change this.
6. If you are instructed to use enable **Default Route**, this setting specifies that the Router be used to define the default route to the Internet for your LAN. Whenever a computer on the LAN attempts to access the Internet, the Router becomes the Internet gateway to the computer.
7. Set **NAT** to *Enabled* unless you have been told to NAT must be *Disabled* for your account.
8. If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **VCI** in Kbps.
9. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
10. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Admin** menu button. In the Administrator Settings menu, click the **Reboot** button under **Force the DSL-G604T to system restart**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish a connection to the Internet.

# Bridged Connection for WAN

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

Follow the instructions below to configure a Bridged connection for the WAN interface.

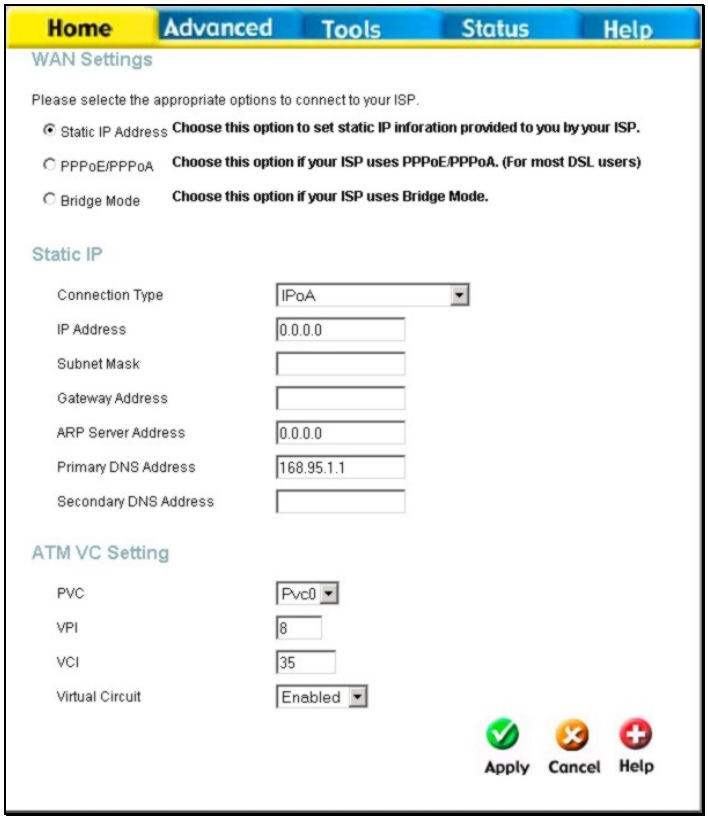



**WAN Settings Menu – Bridge Mode**

1. Click to select the **Bridge Mode** radio button in the **WAN Settings** options list. The menu will change to offer a different set of configuration options.
2. Under the **ATM VC Setting** heading, do not change the **PVC** (*Pvc0*) index for the initial connection.
3. Also under the **ATM VC Setting**, you see two numbers, the **VCI** and **VPI** values. Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.
4. Set the **Virtual Circuit** setting to *Enabled* in the pull-down menu if it is not already enabled.
5. Under **Bridge Mode**, choose the **Connection Type** from the pull-down menu. For bride mode connections the available encapsulation methods are *1483 Bridged IP LLC* and *1483 Bridged IP VC-Mux*.
6. If you have not been instructed to change the ATM settings at the bottom of the menu, leave these at the default settings. If you have been given new settings to configure, select the **Service Category** and type in the values for **PCR** and **SCR** in Kbps.
7. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
8. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Admin** menu button. In the Administrator Settings menu, click the **Reboot** button under **Force the DSL-G604T to system restar**t. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

# Static IP Address for WAN

When the Router is configured to use Static IP Address assignment for the WAN connection, you must manually assign a global IP Address, Subnet Mask and Gateway IP Address used for the WAN connection. Most users will also to configure DNS server IP settings in the DNS Settings configuration menu (see below). Follow the instruction below to configure the Router to use Static IP Address assignment for the WAN connection.



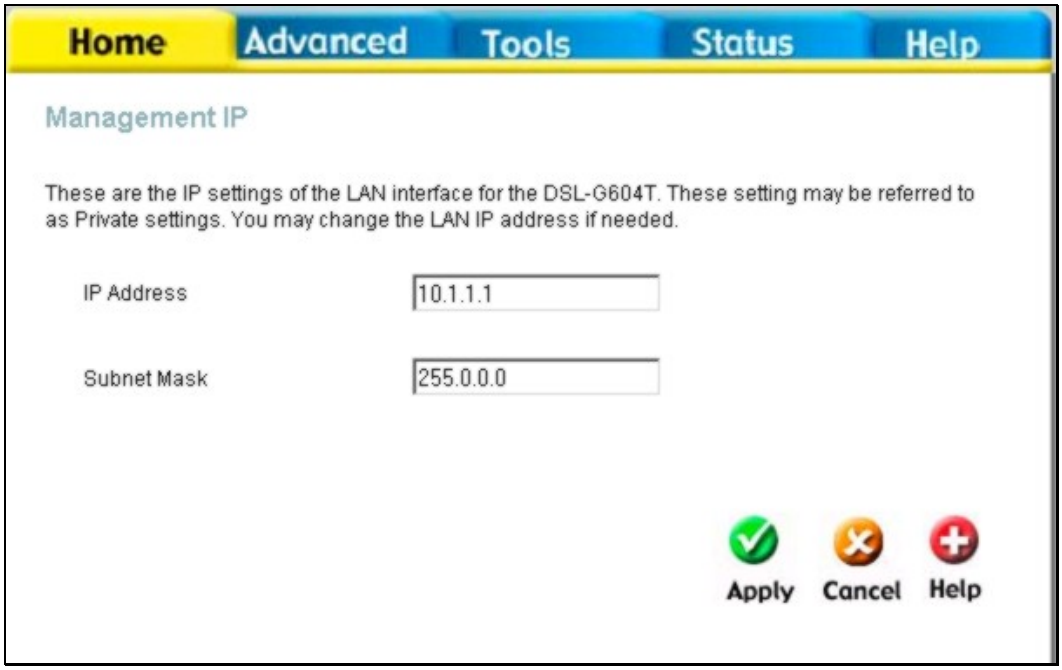

**WAN Settings - Static IP**

1. Click to select the Static **IP Address** radio button listed in the **WAN Settings** options list. The menu will change to offer a different set of configuration options.
2. Under the **ATM VC Setting** heading, do not change the **PVC** (*Pvc0*) index for the initial connection.
3. Also under the **ATM VC Setting**, you see two numbers, the **VCI** and **VPI** values. Do not change the **VPI** or **VCI** value unless you have been told to do so. These numbers are used to define a unique path for your connection. If you have been given specific settings for this to configure, type in the correct values assigned by your ISP.
4. Set the **Virtual Circuit** setting to *Enabled* in the pull-down menu if it is not already enabled.
5. Select the **Connection Type** from the pull-down menu under the **Static IP** heading. Your ISP should provide this information to you. The available options are *IPOA, 1483 Bridged VC-Mux, 1483 Bridged LLC*, and *1483 Routed VC-Mux*. If have not been provided specific information for the Connection Type setting, leave the default setting.
6. Change the **IP Address**, **Subnet Mask**, **Gateway Address** and (if available) **Secondary DNS** Server IP address as instructed by your ISP. Your ISP should have provided these IP settings to you.
7. Set **NAT** to *Enabled* unless you have been told to NAT must be *Disabled* for your account
8. When you are satisfied that all the WAN settings are configured correctly, click on the **Apply** button.
9. The new settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Admin** menu button. In the Administrator Settings menu, click the **Reboot** button under **Force the DSL-G604T to system restart**. The Router will save the new settings and restart. Upon restarting the Router will automatically establish the WAN connection.

# LAN IP Settings

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

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



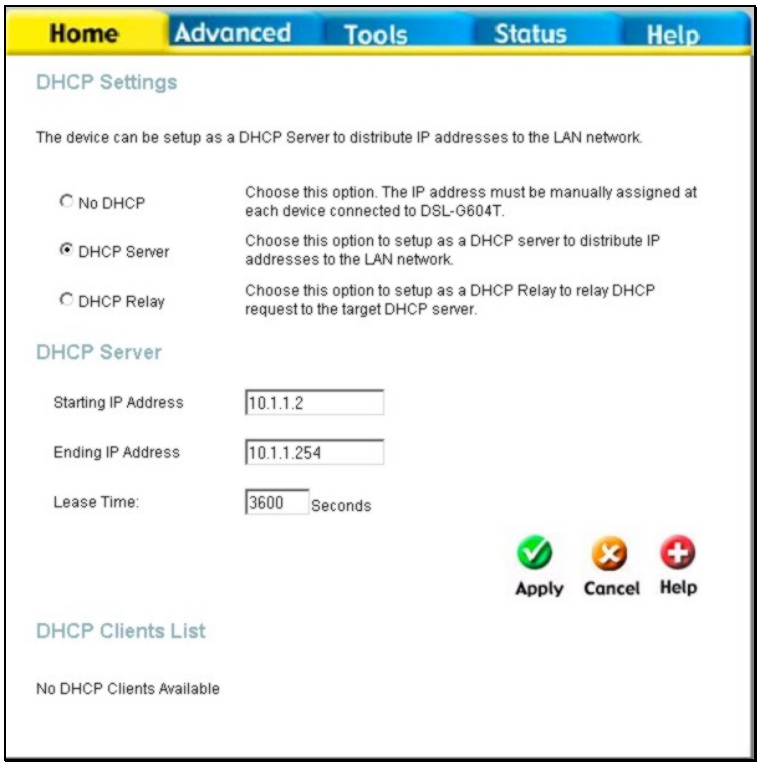

**Configure LAN IP settings**

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

# DHCP Server Settings for the LAN

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

To display the **DHCP Server** menu, click the **DHCP** button in the **Home** directory. Active DHCP Clients appear listed in the **DHCP Client List** below the configuration menu. Information about DHCP clients includes the IP address, MAC address, host name and lease time are displayed in the list.




**Configure DHCP server settings for the LAN**

The three options for DHCP service are as follows:

- You may use the Router as a DHCP server for your LAN.
- You can disable DHCP service and manually configure IP settings for workstations.
- You use DHCP service provided by your ISP.

Follow the instructions below according to which of the above DHCP options you want to use. When you have configured the DHCP Settings as you want them, click the **Apply** button to commit the new settings. The new DHCP settings must be saved and the Router must be restarted for the settings to go into effect. To **Save & Reboot** the Router, click on the **Tools** directory tab and then click the **Admin** menu button. In the Administrator Settings menu, click he **Save & Reboot** button.

## Use the Router for DHCP

To use the built-in DHCP server, click to select the **DHCP Server** option if it is not already selected. The IP Address Pool settings can be adjusted. The **Starting IP Address** is the lowest available IP address (default = 10.1.1.2). If you change the IP address of the Router this will change automatically to be 1 more that the IP address of the Router. The **Ending IP Address** is the highest IP address number in the pool. Type in the **Lease Time** in the entry field provided. This is the amount of time in seconds that a workstation is allowed to reserve an IP address in the pool if the workstation is disconnected from the network or powered off.

## Disable the DHCP Server

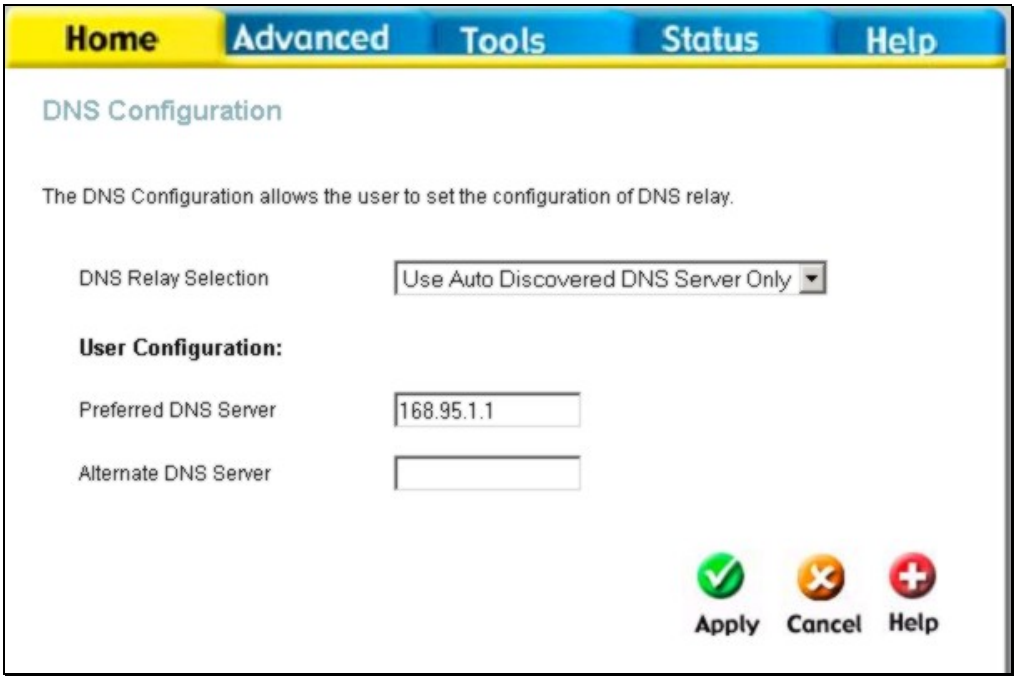
To disable DHCP, click to select the **No DHCP** option and click on the **Apply** button.

## DHCP Relay

To use DHCP service from your ISP, select the **DHCP Relay** option and type the **DHCP Relay IP** address in the space provided. Click **Apply** to begin DHCP relay from the ISP.

# DNS Server Settings

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




**Configure DNS Settings**

In the DNS Relay Selection pull-down menu, choose to *Use Auto Discovery*, *Use User Configured* or *Disable* DNS relay.

If you have not been given specific DNS server IP addresses or if the Router is not pre-configured with DNS server information, select the Auto Discover option for DNS relay. Auto discovery DNS instructs the Router to automatically obtain the DNS IP address from the ISP through DHCP. If your WAN connection uses a Static IP address, auto discovery for DNS cannot be used.

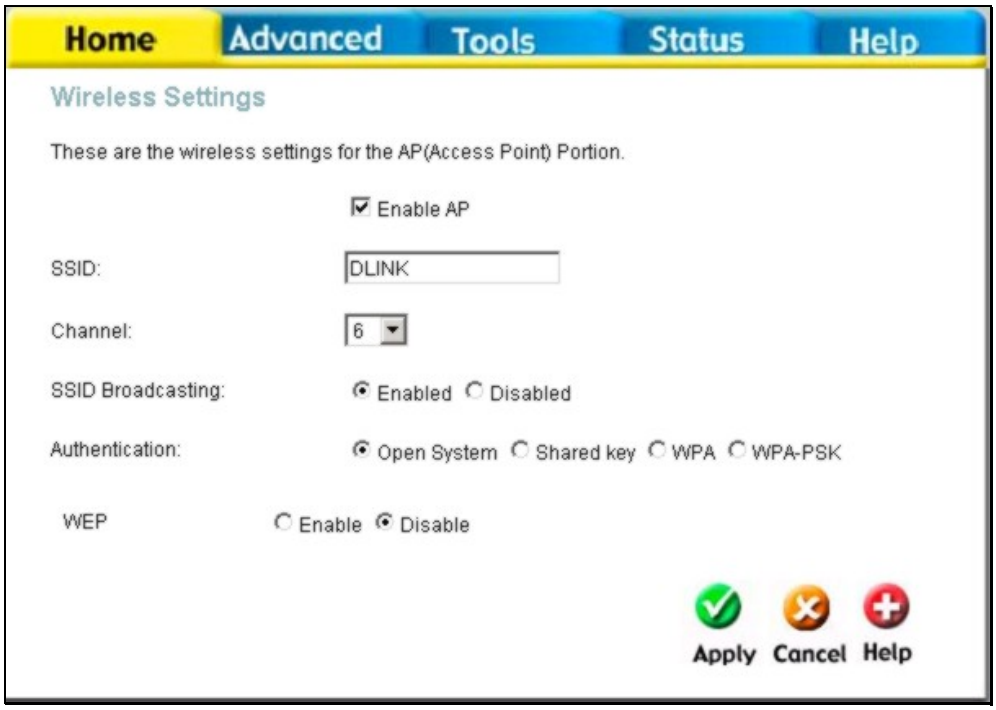
If you have DNS IP addresses provided by your ISP, enter these IP addresses in the available entry fields for the **Preferred DNS Server** and the **Alternative DNS Server**.

If you choose to disable DNS relay, it will be necessary to configure DNS settings for hosts on the LAN since they will not be depending on the Router to forward the DNS requests.

When you have configured the DNS settings as desired, click the **Apply** button.

# Basic Wireless LAN Setup

The two essential settings for wireless LAN operation are the SSID and Channel Number. The SSID (Service Set Identifier) is used to identify a group of wireless LAN components. To enable or disable the wireless interface, configure a new SSID or change the broadcast channel, click on the **Wireless Setup** link to view the menu displayed below. For instructions on setting up wireless security, please read the next chapter.




**Configure Basic Wireless LAN settings**

## 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.

# Advanced Router Management

This chapter introduces and describes the management features that have not been presented in the previous chapter. These include the more advanced features used for network management and security as well as administrative tools to manage the Router, view statistics and other information used to examine performance and for troubleshooting.

Use your mouse to click the directory tabs and menu buttons in order to display the various configuration and read-only menus discussed below. The table below summarizes again the directories and menus available in the management web interface. In this chapter you will find descriptions for the menus located in the Advanced, Tools and Status directories.

| Directory | Configuration and Read-only Menus |
|---|---|
| **Home** | Click the Home tab to access the Setup Wizard, Wireless LAN Configuration, WAN Configuration, LAN IP Configuration, DHCP for the LAN Setup and DNS IP Configuration menus. These menus are discussed in the previous Chapter on Basic Router Configuration. |
| **Advanced** | Click the Advanced tab to access the UPnP, Virtual Server, IP Filters, IP Routing, DMZ, Firewall, RIP, PPP, ADSL, ATM VCC, Wireless Performance and Wireless Management menus. |
| **Tools** | Click the Tools tab to access the Administrator Settings, System Time Configuration, System Settings (load and save configuration files), Firmware Upgrade and Diagnostic Test menus. |
| **Status** | Click the Status tab to view the Device Information, Event Log, Traffic Statistics and ADSL Status information windows. |
| **Help** | The Help menu presents links to pages that explain various functions and services provided by the Router. |

# Port Forwarding

Use the Port Forwarding menu to create Virtual Server functions through the Router. A Virtual Server can allow remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DSL-G604T will accept remote requests for these services at your Global IP Address, using the specified TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the Private IP address you specify. Remember that the Private IP Address must be within the range specified for your LAN.

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

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

The table below describes the configuration settings presented in the Virtual Server menu.

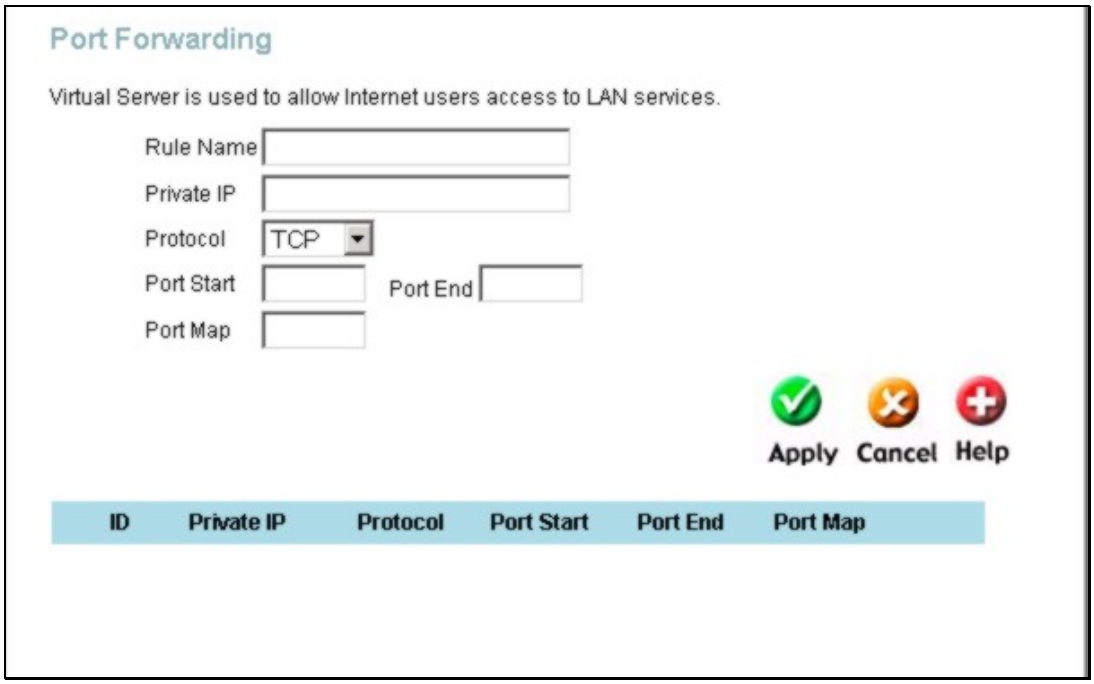



**Figure 4- 1. Virtual Server Menu and List**

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

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

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

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

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

**Note**

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

# Filters

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

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

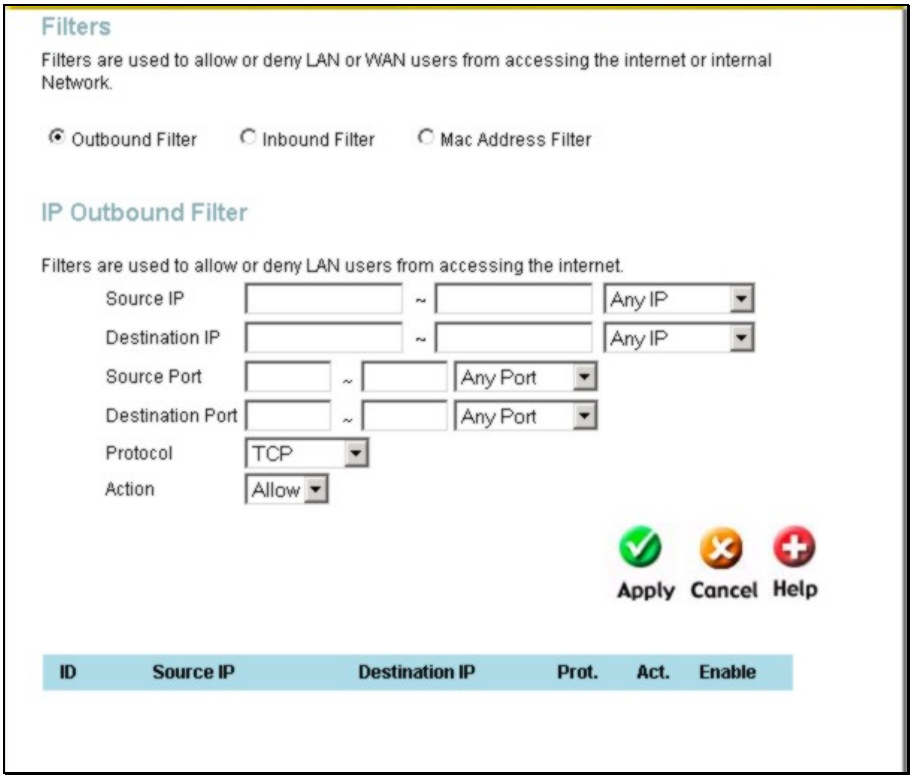



**Figure 4- 2. Filters Configuration Menu**

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

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

The parameters described below are used to set up filter rules.

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

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

# DMZ

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

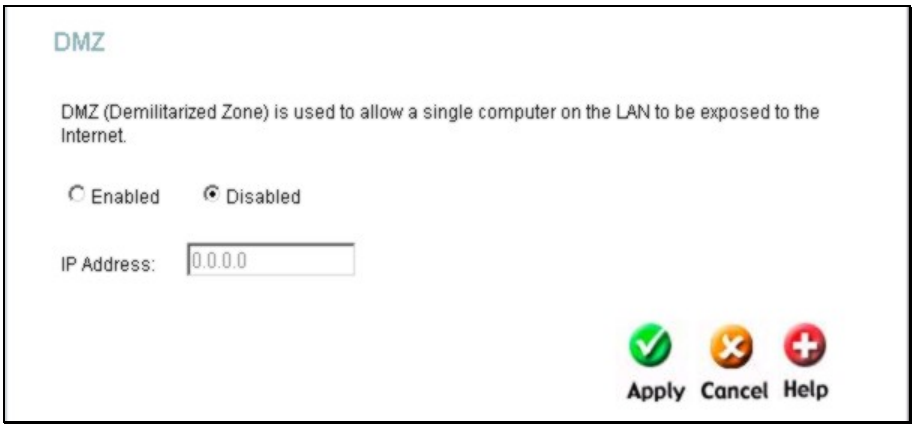



**Figure 4- 3. DMZ IP address configuration**

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

# Firewall

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

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

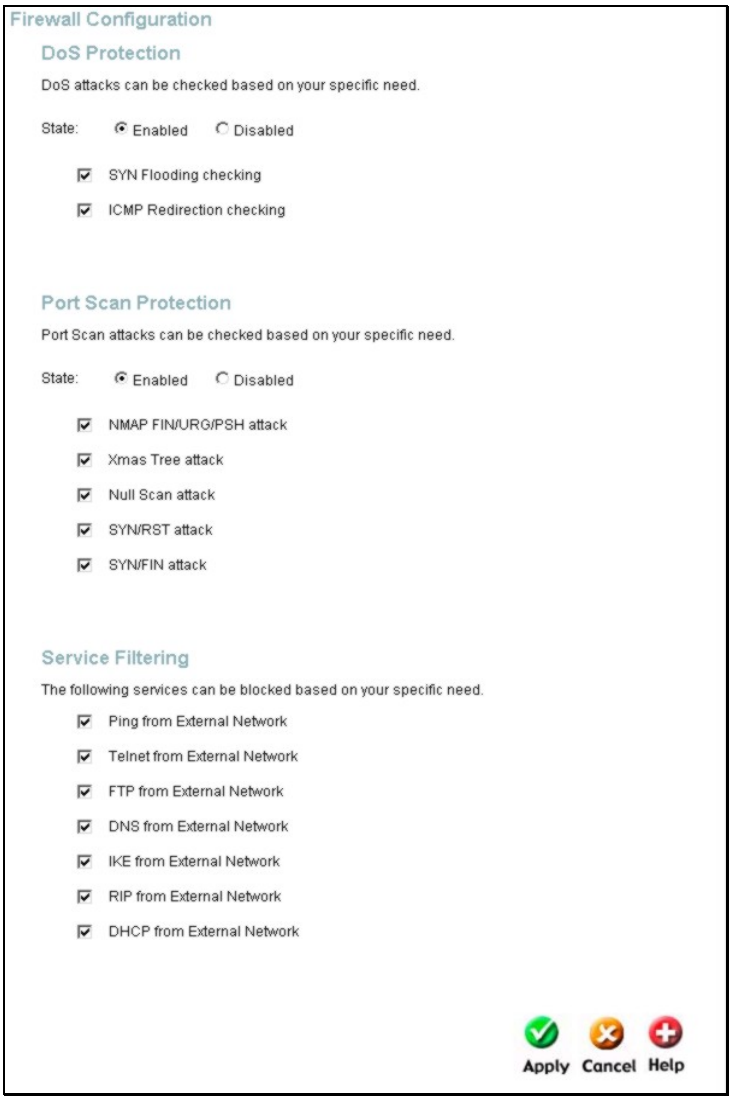



**Figure 4- 4. Firewall Configuration Menu**

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

| Dos Protection | Port Scan Protection | Service Filtering |
|---|---|---|
| SYN Flood check | Nmap/FIN attack | Ping from WAN |
| ICMP Redirection check | URG/PSH attack | Telnet from WAN |
| | Xmas Tree Scan | FTP from WAN |
| | Null Scan attack | DNS from WAN |
| | SYN/RST attack | IKE from WAN |
| | SYN/FIN Scan | RIP from WAN |
| | | DHCP from WAN |

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

Port scan protection is designed to block attempts to discover vulnerable ports or services that might be exploited in an attack from the WAN.

The Service Filtering options allow you to block FTP, Telnet response, Pings, etc, from the external network. Check the category you want to block to enable filtering of that type of packet.

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

# Static Routing

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

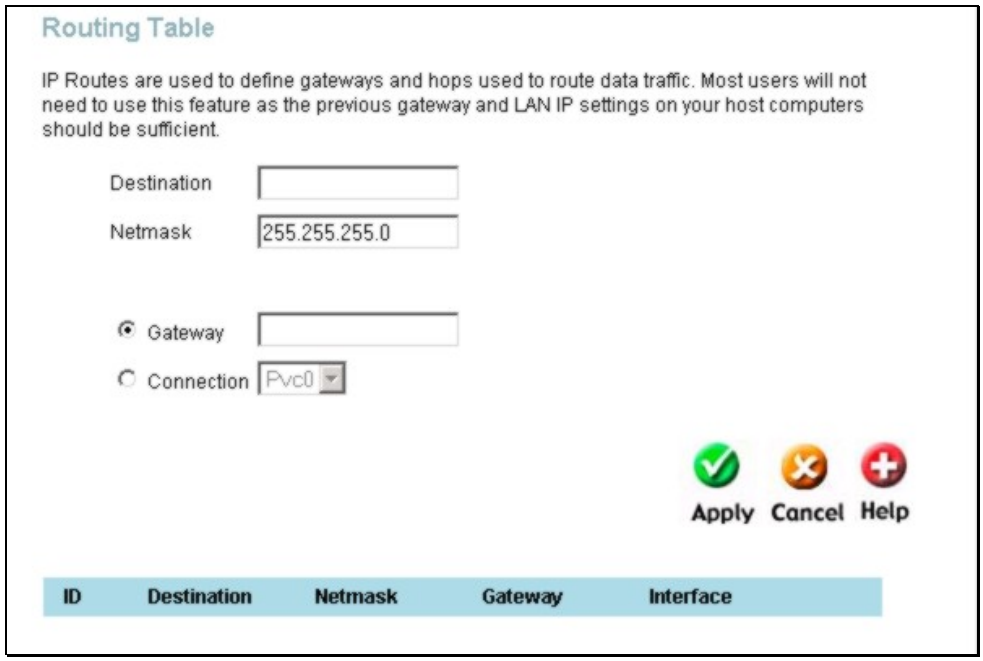



**Figure 4-5. Static Routing menu**

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

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

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

# Dynamic Routing (RIP)

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

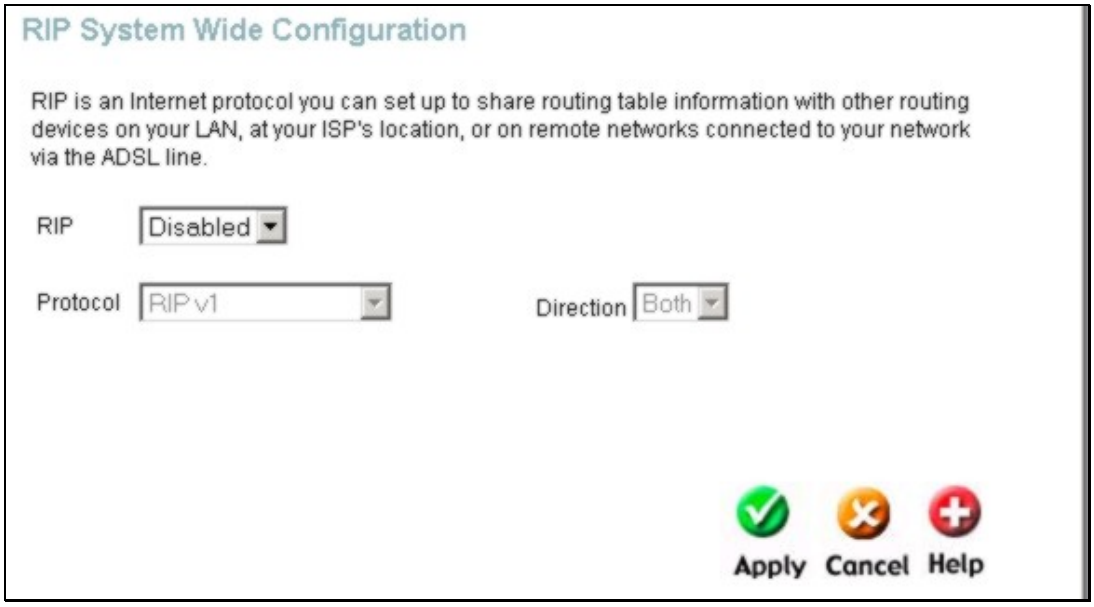



**Figure 4- 6. RIP menu**

To enable RIP, select *Enabled* from the **RIP** pull-down menu, select the **Protocol** (*RIPv1*, *RIPv2* and *RIPv1 Compatible*) and **Direction** (*In*, *Out*, or *Both*), and click **Apply**.

The RIPv1 Compatible option will respond to or send RIP requests compatible with both RIP v1 and RIP v2.

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

# ATM VC

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

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

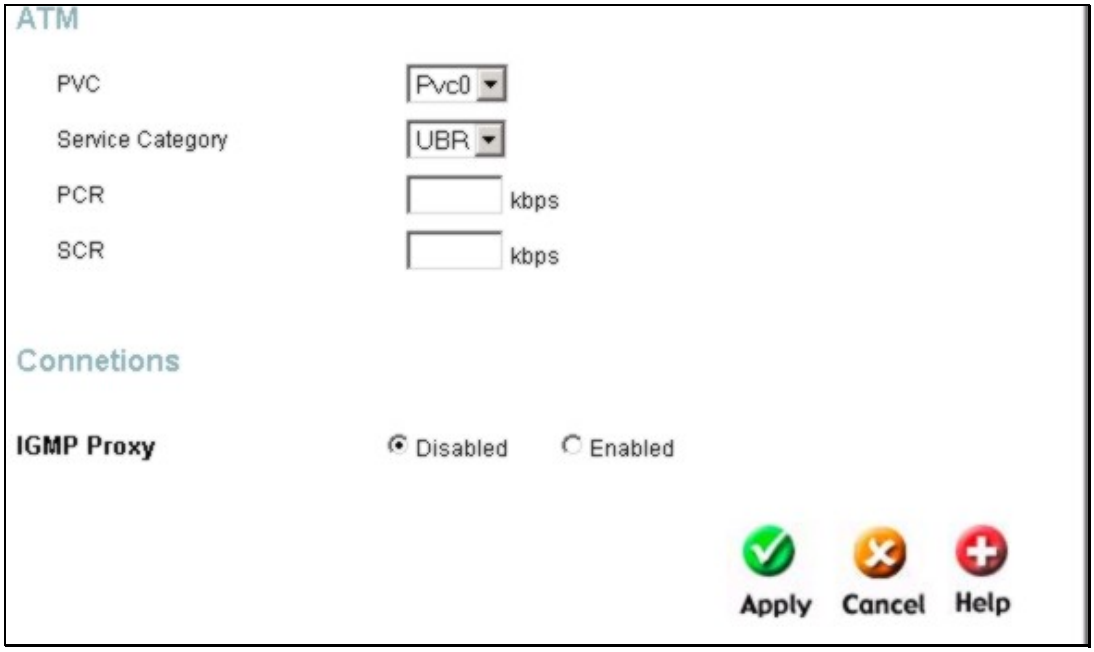



**Figure 4- 7. ATM Virtual Circuit configuration menu**

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

# Advanced Wireless LAN Configuration

The menus used to configure Wireless LAN settings available in the Advanced directory inclued the Wrieless Performance and Wireless Management menus. Wireless security settings are configured using the WirelessSettings menu located in the Home directory. The wireless performance, management and security features are described below.

## Wireless Performance

If you want to tweek 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 be benefit performance. Carefully consider and evaluate any changes to these wireless settings.*

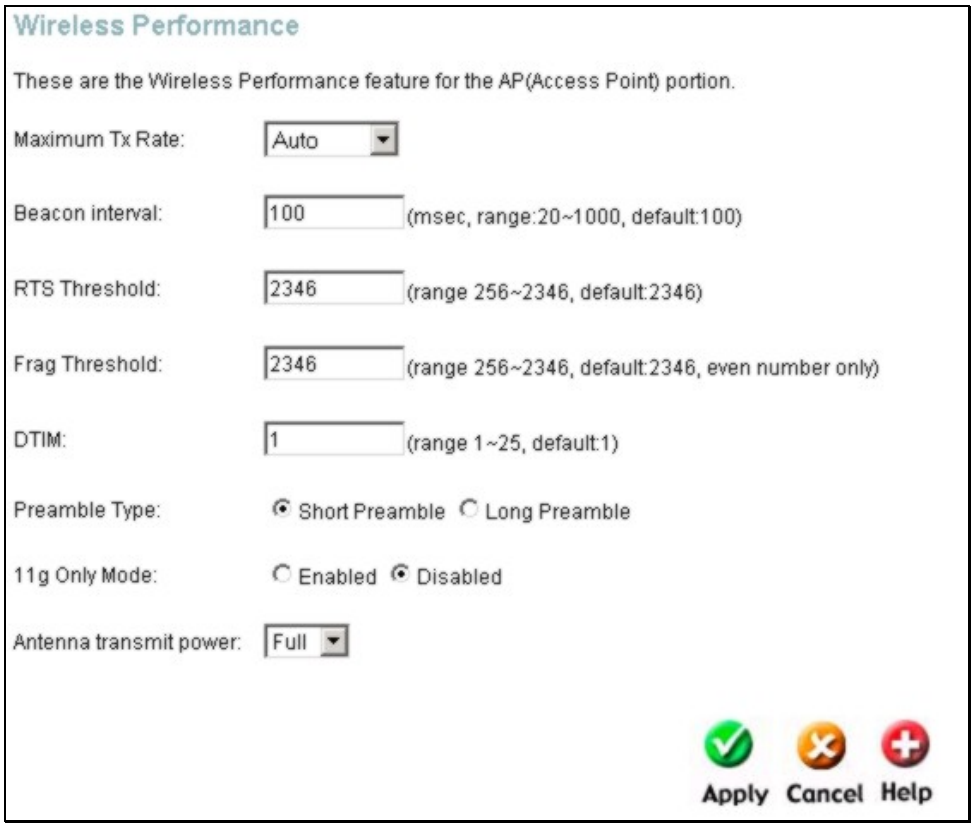



**Figure 4- 8. Wireless LAN Performance settings**

# Wireless Security

The wireless LAN interface of the DSL-G604T has various security features used to limit access to the device or to encrypt data and shared information. The available standardized security for wireless LAN includes WEP, 802.1x, WPA and WPA-PSK Wireless security is configured with the **Wireless Settings** menu located in the **Home** directory.

The wireless access point is not enabled by default. It may be enabled using the Setup Wizard as previously described, or use the Wireless Settings menu. To enable the wireless access point, click the **Enable AP** option so that a check mark appears in the box. Click the **Apply** button to begin wireless operation. To disable the access point, deselect the Enable AP option and click the Apply button.

Note

*Before enabling any security function for wireless operation, it is recommended to be sure the access point is working effectively. If possible, test the wireless interface to be sure stations are able to associate with the DSL-G604T before changing security settings.*

## Configure Security Protocols

In the Wireless Settings menu, select the type of security you want to configure. The menu will change to present the settings specific to the method being configured.

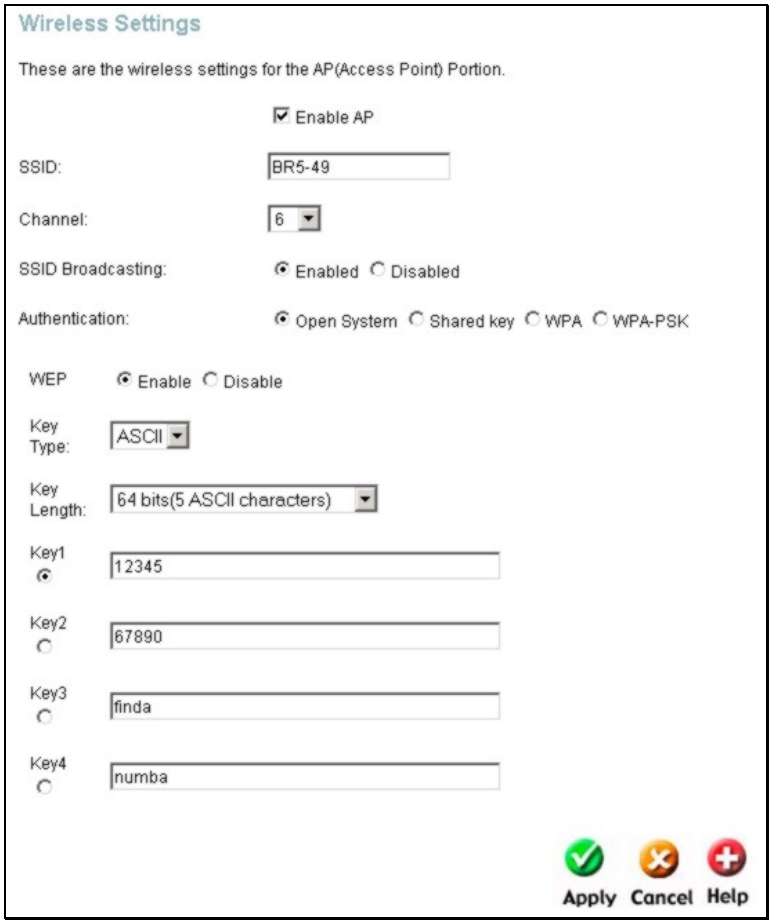



**Figure 4- 9. Configure WEP Wireless Security**

# SSID and Channel

The SSID used for your wireless network can be any character string up to 16 characters in length. Type the desired **SSID** in the space provided, select the channel you want to use from the drop-down **Channel** menu and click on the **Apply** button to begin operation with the new SSID and channel.

## Disable SSID Broadcast

By default the access point will broadcast the SSID that has been configured. This can be disabled by selecting the **Disabled** radio button listed to the right of **SSID Broadcasting** and clicking on the **Apply** button. This change goes into effect immediately. When SSID broadcasting is disabled, each wireless station or access point that associates with the DSL-G604T must have the SSID setting configured. Wireless nodes will not be able to discover the SSID.

If SSID has been disabled, it can be enabled in the same Wireless Settings menu. The change is effective as soon as it is applied.

# WEP Encryption

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.

WEP can use different methods of Authentication. Use the **Authentication Type:** drop-down menu to choose **Open** or **Shared**.

- Select **Open** to allow any wireless station to associate with the access point.
- Select **Shared** to only allow stations using a shared key encryption to associate with it. Shared key requires additional configuration of the keys to be used. Follow the instructions below to configure the Shared Keys.

WEP is disabled by default. To enable **WEP**, select the **Enable** option. Configure the Encryption Keys as desired and click the **Apply** button. The encryption key setup is described below.

## Setup Encryption Keys

WEP Keys are available in two types (Hex and ASCII) and three levels of encryption. Select **Hex** or **ASCII** from the **Key Type** drop-down menu. Hex or Hexadecimal digits are defined as the numerical digits 0 – 9 and the letters A – F (upper and lower case are recognized as the same digit). ASCII characters include numbers and letters but no spaces. An upper case ASCII character is NOT recognized as the same lower case character, and therefore must be configured exactly as typed for all wireless nodes using the access point. The length of the key depends on the level of encryption used.

Select the **Key Length** from the drop-down menu. The available key lengths are 64, 128 or 256-bit encryption. In the spaces provided, type in **Key 1**, **Key 2**, **Key 3** and **Key 4**. The length of the character string used of the keys depends on the level (Key Length) of encryption selected. Only one key can be active. The active key is selected by clicking the radio button for the key you want to use.

Click the **Apply** button when you have configured WEP as desired to put the changes into effect.

## Configure WPA Settings

WPA 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.

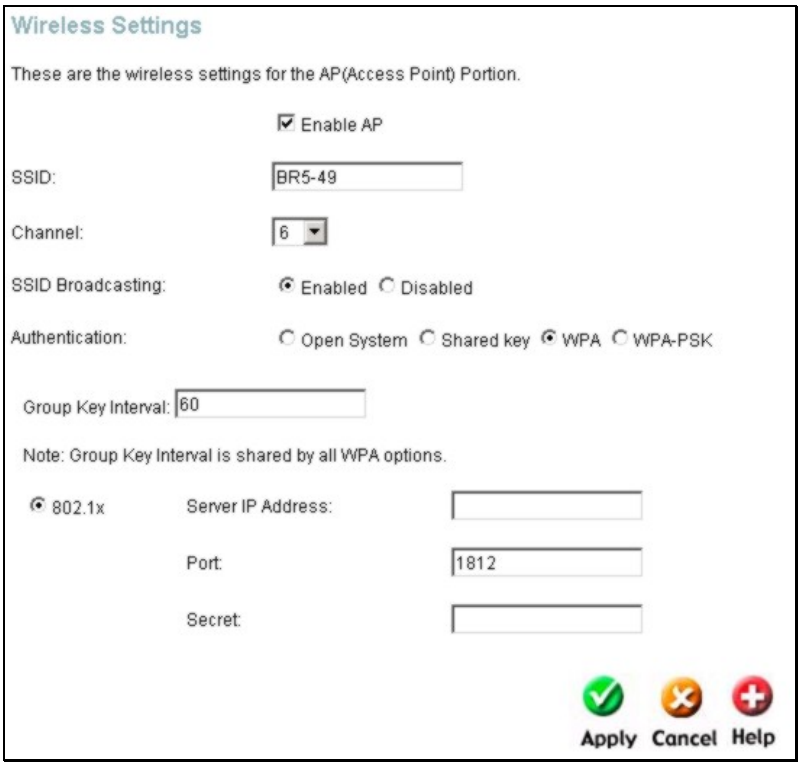



**Figure 4- 10. Configure WPA Security for WLAN**

To configure WPA settings, select the **WPA** option. The menu will change to offer the appropriate settings. Type in the IP address of the RADIUS server used in the **Server IP Address** field. Change the **Port:** if necessary, type in the password in the **Secret** field and change the **Group Key Interval** as desired. Click the **Apply** button to put the changes into effect.

## Configure WPA-PSK Settings

WPA-PSK requires a shared key and does not use a separate server for authentication. PSK keys can be ASCII or Hex type.

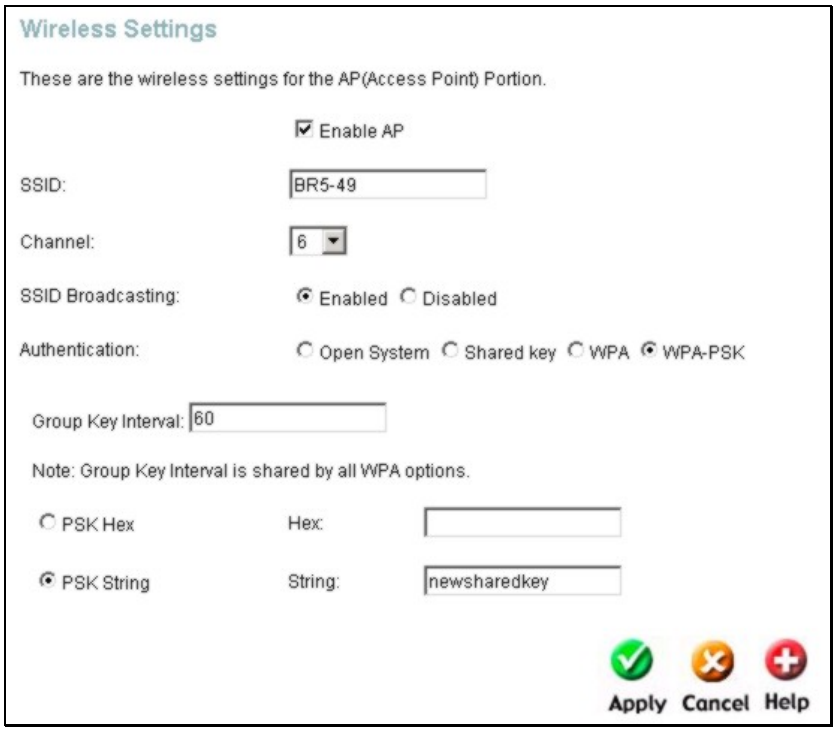



**Figure 4- 11. Configure WPA-PSK Security for WLAN**

To configure WPA settings, select the **WPA-PSK** option. The menu will change to offer the appropriate settings. Type in the IP address of the RADIUS server used in the **Server IP Address** field. Change the **Group Key Interval** as desired. Select either **PSK Hex** or **PSK String** key and type the key in the space provided. Click the **Apply** button to put the changes into effect.

# Tools and Utilities

Click the **Tools** tab to reveal the menu buttons for various functions located in this directory. The first menu that appears in the Tools directory is used to change the system password used to access the web manager, to save or load Router configuration settings, save current configuration settings, restore default settings, and to reboot the Router or just the wireless access point. The functions in this and the other Tools menus are described below.

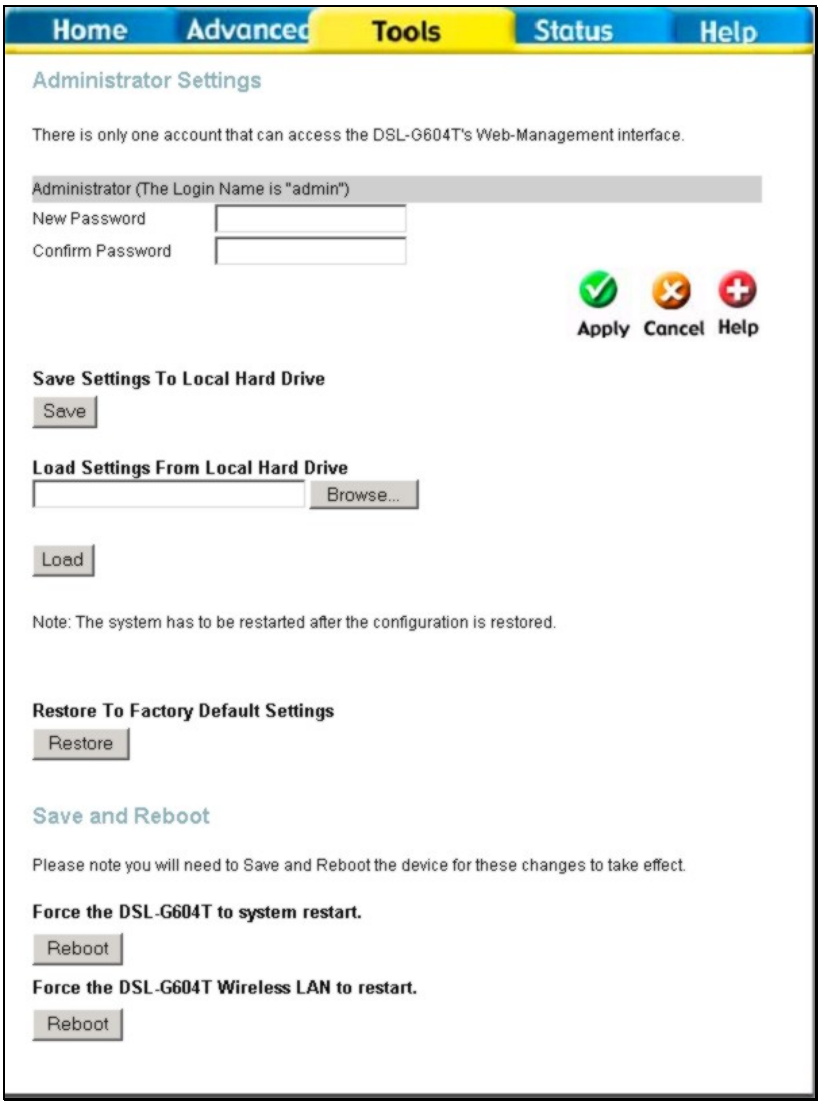



**Figure 4- 12. System Tools administrative functions**

# Change System Password

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

**Figure 4- 13. Administrator Settings change password menu**

# Save Router Configuration Settings

When you have completed configuration of the Router, make sure you save the current configuration settings to flash memory or risk losing the settings. To save the current configuration settings, click the **Admin** button in the **Tools** directory to display the Administrator Settings menu.

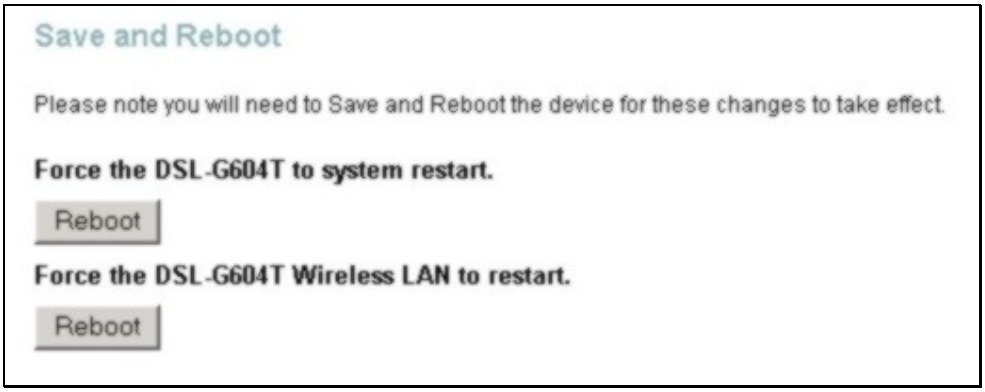



**Figure 4- 14. Save and Reboot menu**

Under **Save and Reboot**, click the **Reboot** button to **Force the DSL-G604T to system restart**. The current settings will be saved to NV-RAM and the system will restart. Do not turn off the Router during this process. It should take about two minutes to complete. After restarting, it is a good idea to backup the Router configuration file to your computer in the same Administrator Settings menu.

## Restart Access Point

To reboot the wireless access point, click the **Reboot** button that will **Force the DSL-G604T Wireless LAN to restart**.

# Save or Load Configuration File

Once you have configured the Router to your satisfaction, it is a good idea to back up the configuration file to your computer. To save the current configuration settings to your computer, click the **Admin** button in the **Tools** directory to display the Administrator Settings menu. Click the **Save** button to **Save Settings to Local Hard Drive**. You will be prompted to select a location on your computer to put the file. The file type is .xml (HTML) and may be named anything you wish.

To load a previously saved configuration file, click the **Browse** button and locate the file on your computer. Click the **Load** button to **Load Settings From Local Hard Drive**. Confirm that you want to load the file when prompted and the process is completed automatically. The Router will reboot and begin operating with the configuration settings that have just been loaded.

**Figure 4- 15. Save System Settings and Restore Defaults**

# Restore Factory Default Settings

To reset the Router to its factory default settings, click the **Restore** button in the Administrator Settings menu. You will be prompted to confirm your decision to reset the Router. The Router will reboot with the factory default settings including IP settings.

# Time & Date

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

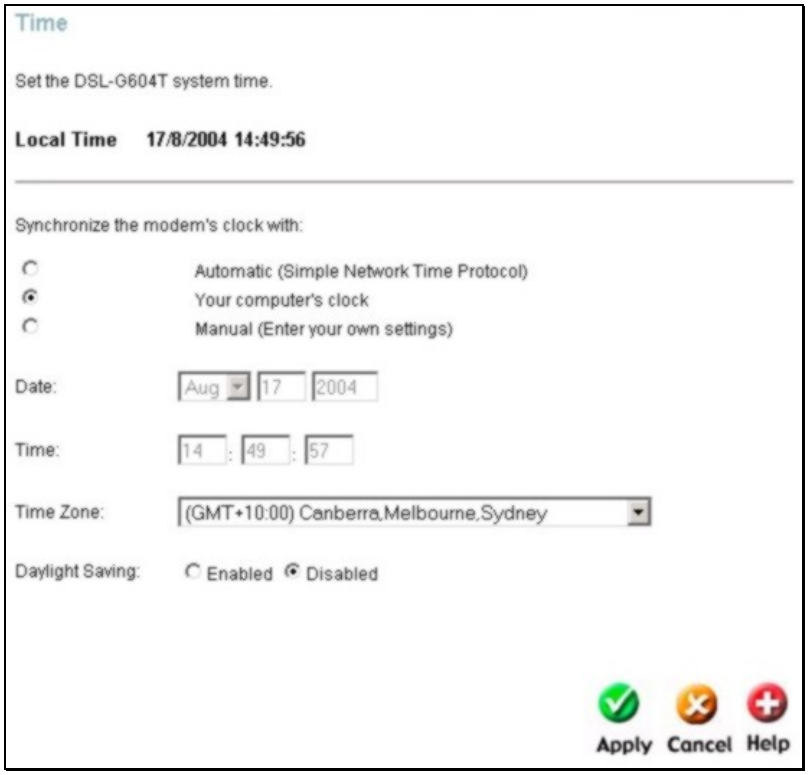



**Figure 4- 16. Time & Date Configuration**

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

# Firmware Upgrade

**Note**

*Performing a Firmware Upgrade can sometimes change the configuration settings. Be sure to back-up the Router's configuration settings before upgrading the firmware.*

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

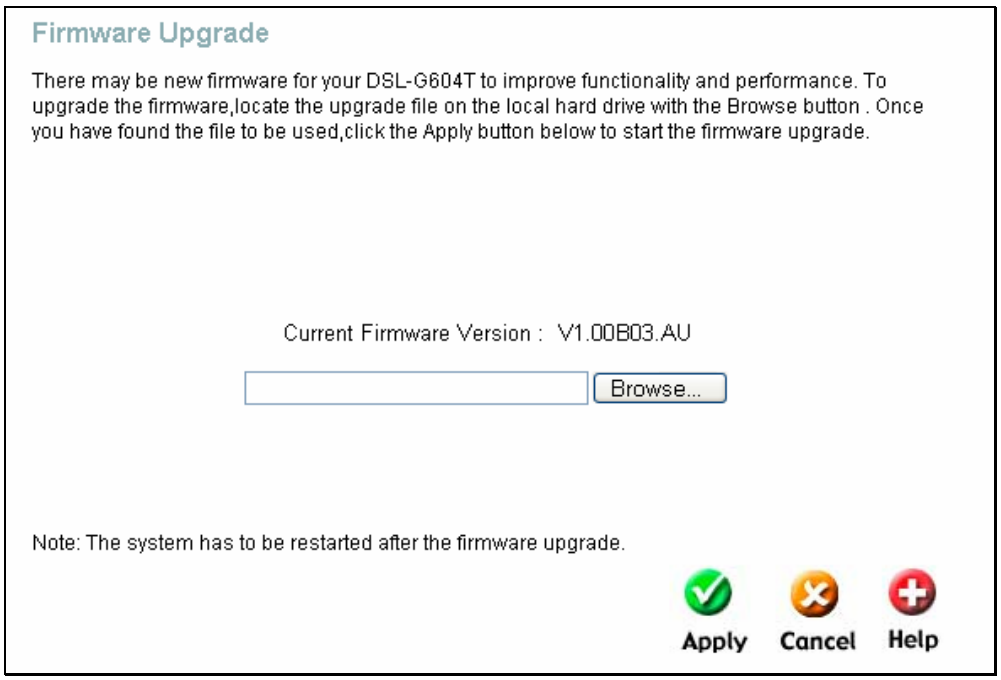



**Figure 4- 17. Firmware Upgrade**

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

# Router Status Information

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

## Device Information Display

Use the Device Information window to quickly view basic current information about the LAN, WAN and Wireless interfaces.

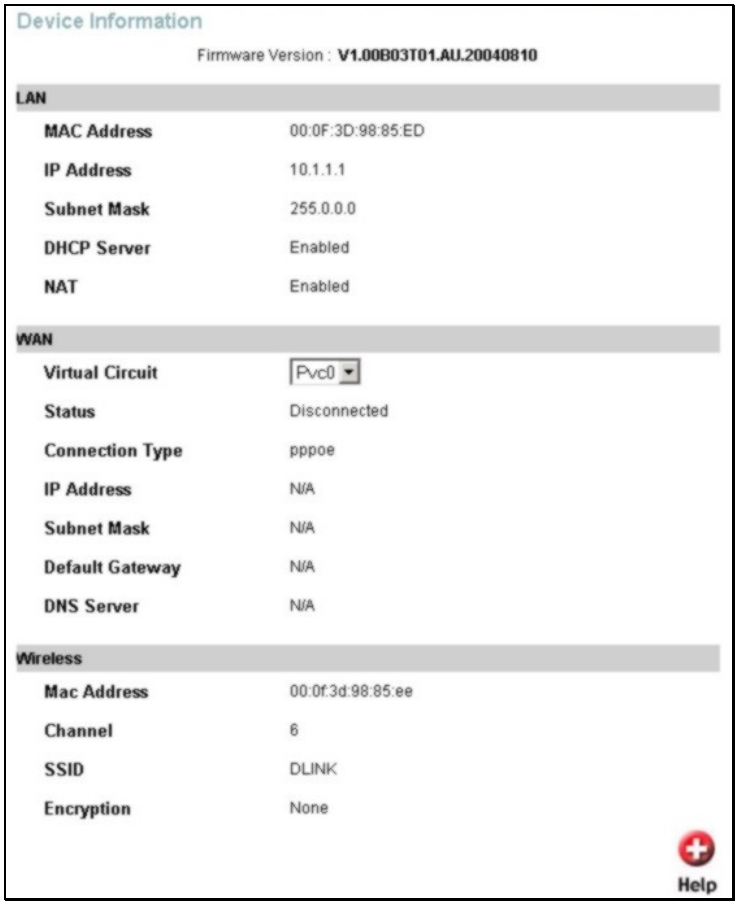



**Figure 4- 18. Device Information display**

# Multiple Virtual Connections

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

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

## Configure Multiple PVCs

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

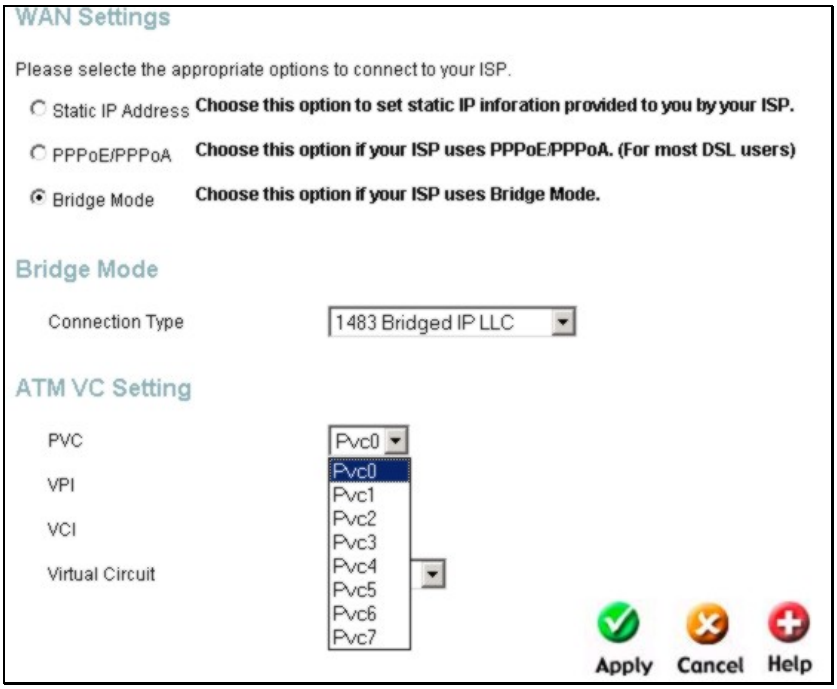



**Figure 4- 19. Select new PVC to configure in the WAN menu**

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

To add a new virtual connection:

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

In the example below, a new VC (Pvc1) has been added using the WAN Settings menu. The connection is setup as a bridged connection.

The new VC appears listed in the ATM VC Setting menu located in the Home > WAN directory. Any VC may be configured in the ATM VC menu by clicking the notepad icon for the PVC you want to configure. VCs configured with PPP connection types can be further configured in the PPP menu.

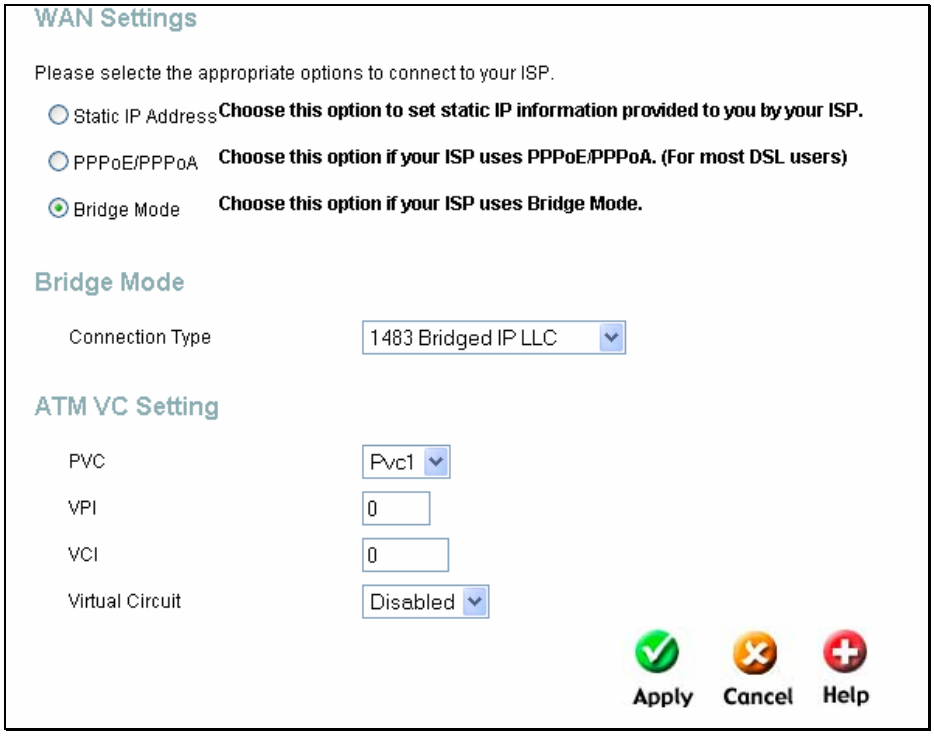



**Figure 4- 20. Configure new VC**

# Technical Specifications

| General | | |
|---|---|---|
| **Standards** | IEEE 802.11b/ 802.11g<br>IEEE 802.3/ 802.3u<br>IEEE 802.1d<br>RFC 791 (IP Routing)<br>RFC 792 (UDP)<br>RFC 826 (ARP)<br>RFC 1058 (RIP 1)<br>RFC 1389 (RIP 2)<br>RFC 1483 (Bridged Ethernet)<br>RFC 1577 (IP over ATM)<br>RFC 1661 (PPP)<br>RFC 1994 (CHAP) | RFC 1334 (PAP)<br>RFC 2364 (PPP over ATM)<br>RFC 1631 (NAT)<br>RFC 1877 (Automatic IP assignment)<br>RFC 2516 (PPP over Ethernet)<br>RFC 2131 (DHCP)<br>ANSI T1.413 issue 2<br>ITU G.992.1 (G.dmt)<br>ITU G.992.2 (G.lite)<br>ITU G.994.1 (G.Hs)<br>ITU-T Rec. I.361<br>Supports ATM Forum UNI V3.1/4.0 PVC |
| **Wireless** | | |
| **Modulation** | IEEE 802.11b: DQPSK, DBPSK, DSSS, and CCK<br>IEEE 802.11g: BPSK, QPSK, 16QAM, 64QAM, OFDM | |
| **Frequency** | 2400 ~ 2484.5MHz ISM band | |
| **Channels** | 11 channels for United States<br>13 channels for European Countries<br>13 channels for Japan | |
| **Wireless Data Rates** | IEEE 802.11b: 11, 5.5, 2, and 1Mbps<br>IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps | |
| **Media Access Protocol** | CSMA/CA with ACK | |
| **WEP** | 64/128/256 bits | |
| **Wireless Certification** | Wi-Fi WPA | |
| **ADSL Data Rates** | G.dmt full rate: Downstream up to 8 Mbps<br>Upstream up to 640 Kbps<br>G.lite: Downstream up to 1.5 Mbps<br>Upstream up to 512 Kbps | |
| **Media Interface** | RJ-11 port ADSL telephone line connection<br>4 x RJ-45 ports for 10/100BASET Ethernet connection | |

| Physical and Environmental | |
|---|---|
| **DC Inputs:**<br>**Power Adapter** | Input: 230V AC 50 ~ 60Hz (per region)<br>Output: 12V AC, 1.2A |
| **Power Consumption** | 12 Watts (max) |
| **Operating Temperature** | 5° to 40° C (41° - 104° F) |
| **Humidity** | 5 to 95% (non-condensing) |
| **Dimensions** | 198 x 155 x 34 mm |
| **Weight** | 450 g |
| **EMI** | FCC Class B, CE EN301489 SMA |
| **Safety:** | CSA International |

# 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 preexisting IP network and are setting one up now, using the factory default IP address settings can greatly ease the setup process. If you already have a preexisting IP network, you can adjust the IP settings for the Router to fit within your existing scheme.

## Using the Default IP Address

The Router is shipped with a preset default IP address setting of 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.

| 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 |

**IP Setup - Example #1**

Please note that when using the default IP address as in the above example, the first number in the IP address must always be the same with only the second, third and fourth number changing. The first number defines the network IP address (all machines must belong to the same IP network), while the last three numbers denote 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 3 for information on how to use configure the Router for DHCP.

## Changing the IP Address of the Router

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

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

| Alternative IP Assignment | | | |
|---|---|---|---|
| **Host** | **IP Address** | **Subnet Mask** | **Gateway IP** |
| **Router** | 10.0.0.1 | 255.0.0.0 | |
| **Computer #1** | 10.0.0.2 | 255.0.0.0 | 10.0.0.1 |
| **Computer #2** | 10.0.0.3 | 255.0.0.0 | 10.0.0.1 |
| **Computer #3** | 10.0.0.4 | 255.0.0.0 | 10.0.0.1 |

**IP Setup - Example #2**

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

# IP Concepts

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

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

## IP Addresses

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

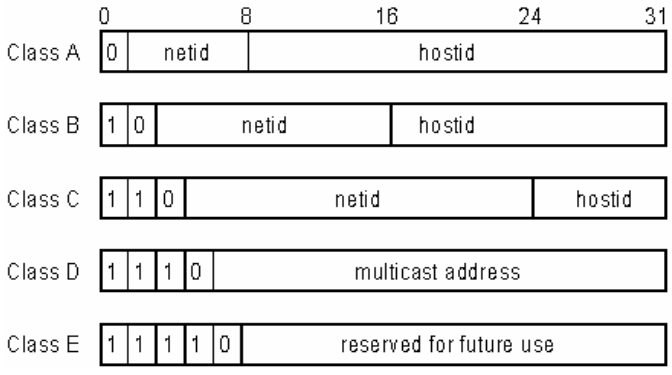
To make IP addresses easy to understand, the originators of IP adopted a system of representation called "dotted decimal" or "dotted quad" notation. Below are examples of IP addresses written in this format:

201.202.203.204 189.21.241.56 125.87.0.1

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

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

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




Networks attached to the Internet are assigned class types that determine the maximum number of possible hosts per network. The previous figure illustrates how the net and host portions of the IP address differ among the

three classes. Class A is assigned to networks that have more than 65,535 hosts; Class B is for networks that have 256 to 65534 hosts; Class C is for networks with less than 256 hosts.

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

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

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

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

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

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

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

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

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

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

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

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

## Subnet Mask

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

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

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

D

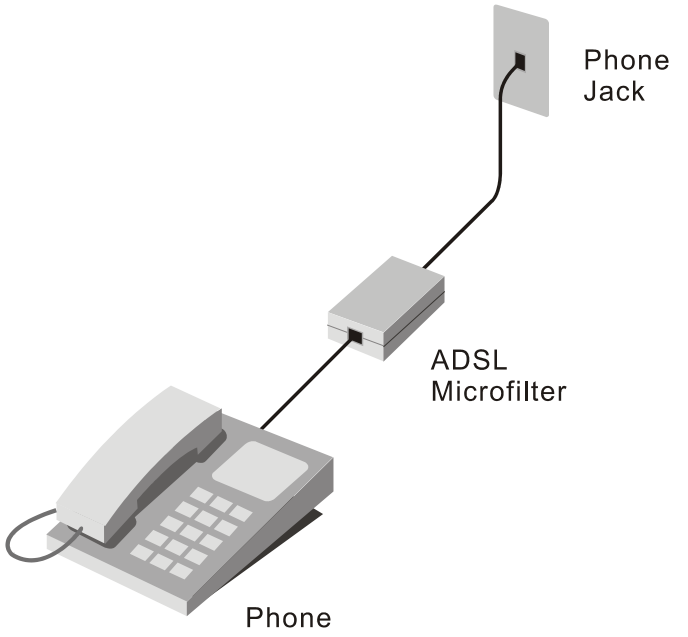
# Microfilters and Splitters

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




**Microfilter Installation**

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

## Line Splitter

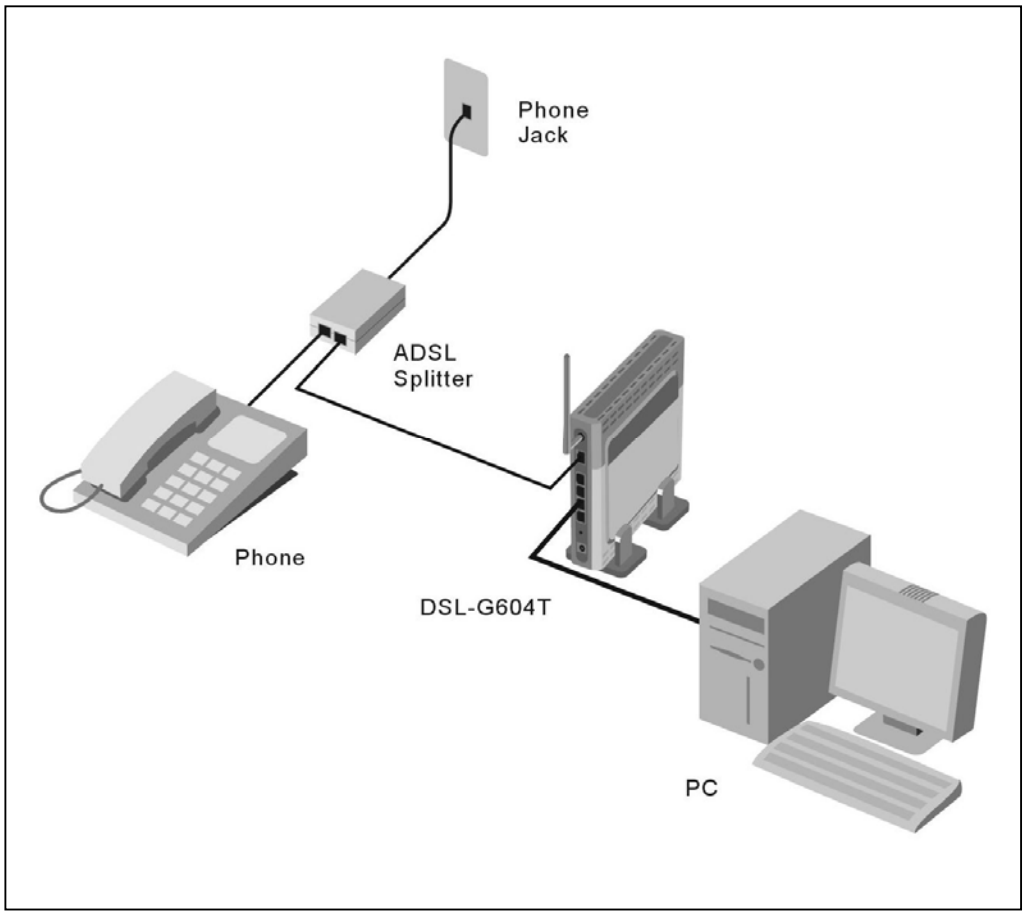
If you are instructed to use a "line splitter", you must install the device between the Router and the phone jack. Use standard telephone cable with standard RJ-11 connectors. The splitter has three RJ-11 ports used to connect to the wall jack, the Router and if desired, a telephone or telephone device.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

**Line -** This port connects to the wall jack.

**ADSL** – This port connects to the Router.

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

The diagram below illustrates the proper use of the splitter.




**Line Splitter Installation**