D-Link®
Building Networks for People

DI-724GU

Release I

Wireless 108G Gigabit QoS Router

User Manual

Business Class Networking

Table of Contents

Product Overview 4
Package Contents 4
System Requirements 4
Introduction 5
Features 6
Hardware Overview 7
Hardware Installation 9
Network Overview 10

Wireless Installation Considerations 11

Configuration 12
Home Page Screen 13
Setup Wizard 14
Dynamic IP Address 15
Static IP Address 16
PPPoE 17
PPTP 18
L2TP 19
Big Pond 20
Wireless Setup 21
Printer Wizard 23
Wireless 26
WAN 28
Dynamic IP Address 28
Static IP Address 30
PPPoE 32
PPTP 34
L2TP 36
Big Pond 38
LAN 40
DHCP 42
Advanced 44
Virtual Server 44
Applications 45
Port Forwarding 46
StreamEngine 47
Filters 49
Parental Control 52
Firewall 53
DMZ 54
Performance 55
Schedules 56
Tools 57
Administration 57
Time 58
System 60
DDNS 61
Miscellaneous 62
Print Server 64
Status 65
Device Info 65

Log 67
Statistics 68
Wireless Status 69
Active Sessions 70
Print Server 71
Help 72

Troubleshooting 73

Wireless Basics 75

Networking Basics 80
Check your IP Address 80
Statically Assign an IP Address 81

Technical Specifications 82

Contacting Technical Support 83

Warranty 84

Registration 89

Package Contents

- D-Link DI-724GU Wireless 108G Gigabit QoS Office Router
- CAT5 Ethernet Cable
- Power Adapter

Note: *Using a power supply with a different voltage than the one included with your product will cause damage and void the warranty for this product.*

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

System Requirements

- Ethernet-based Cable or DSL Modem
- Computers with Windows®, Macintosh®, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer 6.x and above, or Netscape® Navigator 7.0 and above

Introduction

The D-Link DI-724GU Wireless 108G Gigabit QoS Office Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places.

Unlike most routers, the DI-724GU provides data transfers at up to 108Mbps (compared to the standard 54Mbps) when used with other D-Link *Air*Plus *Xtreme G* products. The 802.11g standard is backwards compatible with 802.11b products. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 802.11g's speed when you mix 802.11b and 802.11g devices, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11b network. You may choose to slowly change your network by gradually replacing the 802.11b devices with 802.11g devices .

In addition to offering faster data transfer speeds when used with other 802.11g products, the DI-724GU has the newest, strongest, most advanced security features available today. When used with other 802.11g WPA (WiFi Protected Access) and 802.1x compatible products in a network with a RADIUS server, the security features include:

WPA: Wi-Fi Protected Access authorizes and identifies users based on a secret key that changes automatically at a regular interval. WPA uses TKIP (Temporal Key Integrity Protocol) to change the temporal key every 10,000 packets (a packet is a kind of message transmitted over a network.) This insures much greater security than the standard WEP security. (By contrast, the older WEP encryption required the keys to be changed manually.)

802.1x: Authentication is a first line of defense against intrusion. In the Authentication process the server verifies the identity of the client attempting to connect to the network. Unfamiliar clients would be denied access.

For home users that will not incorporate a RADIUS server in their network, the security for the DI-724GU, used in conjunction with other 802.11g products, will still be much stronger than ever before. Utilizing the Pre Shared Key mode of WPA, the DI-724GU will obtain a new security key every time it connects to the 802.11g network. You only need to input your encryption information once in the configuration menu. With the DI-724GU you will no longer have to manually input a new WEP key to ensure security. Instead, you will automatically receive a new key every time you connect, vastly increasing the safety of your communications.

Features

- Fully compatible with the 802.11g standard to provide a wireless data rate of up to 108Mbps*.
- Backwards compatible with the 802.11b standard to provide a wireless data rate of up to 11Mbps
- WPA (Wi Fi Protected Access) authorizes and identifies users based on a secret key that changes automatically at a regular interval, for example:

  TKIP (Temporal Key Integrity Protocol), in conjunction with a RADIUS server, changes the temporal key every 10,000 packets, ensuring greater security.

  Pre Shared Key mode means that the home user, without a RADIUS server, will obtain a new security key every time the he or she connects to the network, vastly improving the safety of communications on the network.
- 802.1x Authentication in conjunction with the RADIUS server verifies the identity of would be clients.
- Utilizes OFDM technology (Orthogonal Frequency Division Multiplexing).
- User-friendly configuration and diagnostic utilities.
- Operates in the 2.4GHz frequency range.
- Connects multiple computers to a Broadband (Cable or DSL) modem to share the Internet connection.
- Advanced Firewall features: Supports NAT with VPN pass-through, providing added security, MAC Filtering, URL Filtering, and Scheduling.
- DHCP server enables all networked computers to automatically receive IP addresses.
- Web-based interface for Managing and Configuring.
- Access Control to manage users on the network.
- Supports special applications that require multiple connections.
- Equipped with 4 Gigabit Ethernet ports, 1 WAN port, Auto MDI/MDIX.

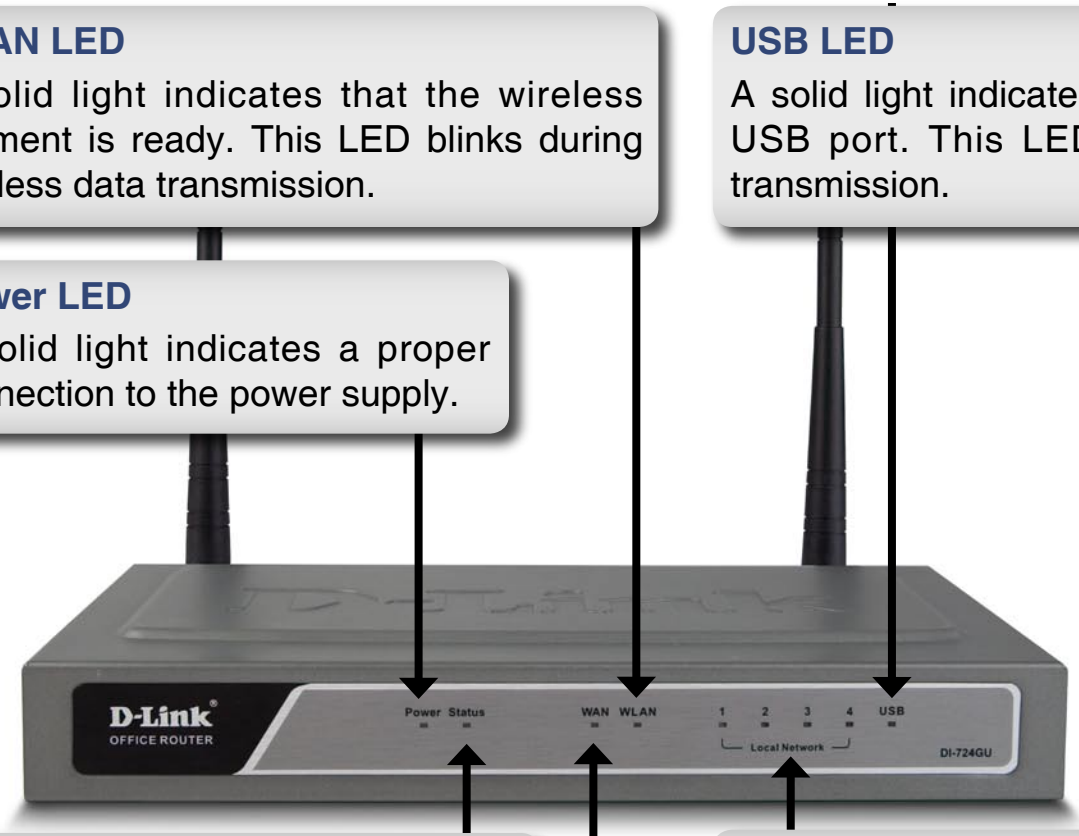
* Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate. D-Link 108G performance results are based on testing with other D-Link 108G enabled devices utilizing Packet Bursting, FastFrames, Turbo Mode and Compression techniques. Data already compressed may not benefit from the D-Link 108G compression techniques..

Hardware Overview

WLAN LED
A solid light indicates that the wireless segment is ready. This LED blinks during wireless data transmission.

USB LED
A solid light indicates a connection to the USB port. This LED blinks during data transmission.

Power LED
A solid light indicates a proper connection to the power supply.



Status LED
A blinking light indicates that the DI-724GU is functioning properly.

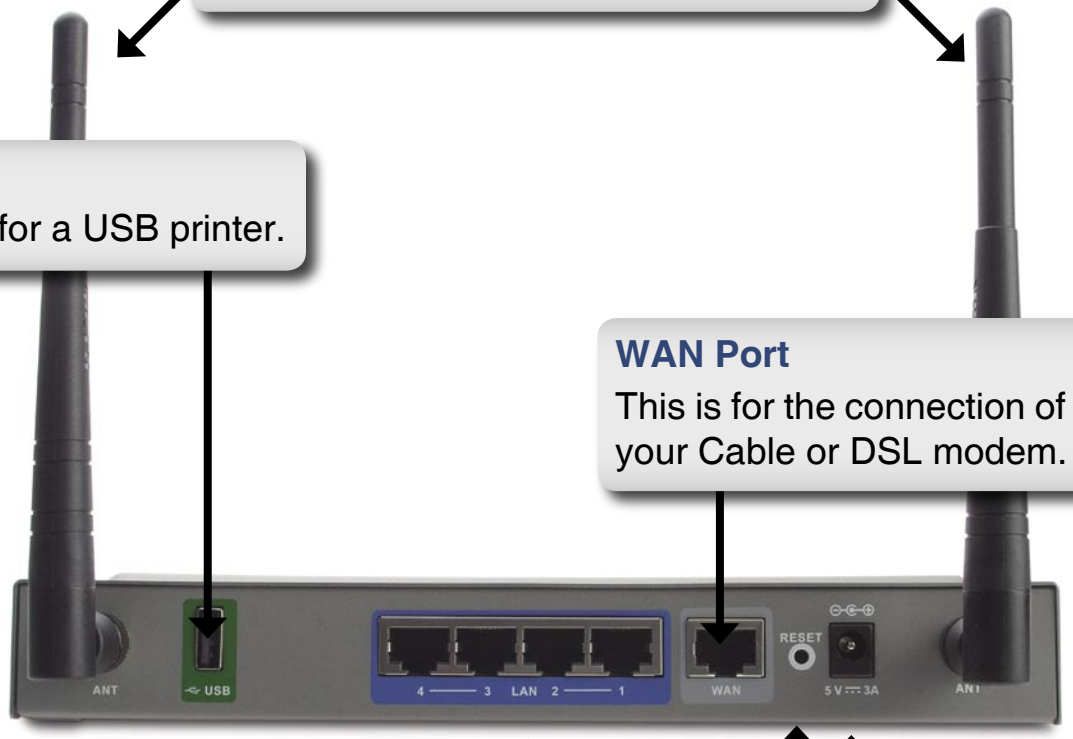
Local Network LEDs
A solid light on each port indicates a connection to an Ethernet enabled device. These LEDs blink during data transmission.

WAN LED
A solid light indicates a connection on the WAN port. This LED blinks during data transmission.

Antennas
Used to connect to 802.11g or 802.11b wireless adapters.

USB Port
Connection for a USB printer.

WAN Port
This is for the connection of an Ethernet cable to your Cable or DSL modem.



LAN Ports
These are the connections for Ethernet cables to Ethernet-enabled computers.

Power Receptor

Reset Button
Pressing this button restores the Router to its original factory default settings.

Hardware Installation

A. First, connect the power adapter to the receptor at the back panel of the DI-724GU and then plug the other end of the power adapter to a wall outlet or power strip. The Power LED will turn ON to indicate proper operation.

B. 1. Power off your Cable or DSL modem; some devices may not have a on/off switch and will require you to unplug the power adapter. Now, the DI-724GU should be powered on and the Cable/DSL modem should be turned off.

2. Cable/DSL modem (Power Off) – DI-724GU (Power On) Connect an Ethernet cable to the Ethernet jack located on the Cable/DSL modem. After the Ethernet cable is securely connected, power on the Cable/DSL modem by turning on the unit or plugging in the power adapter.

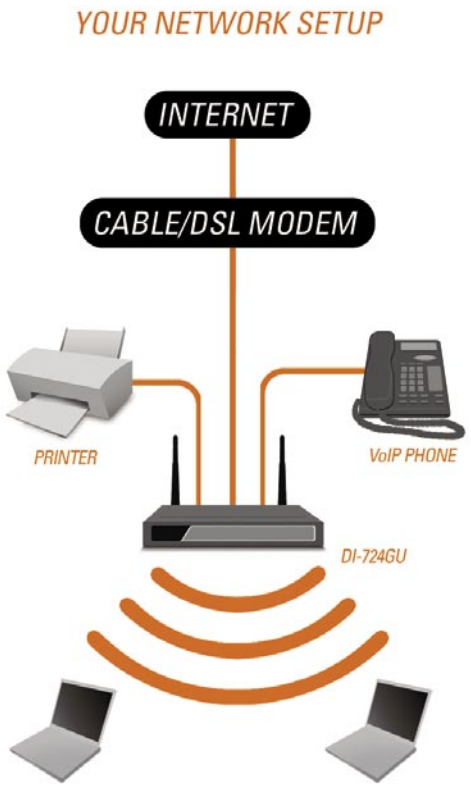
3. Cable/DSL modem (Power On) – DI-724GU (Power On) Insert the other end of the Ethernet cable to the WAN PORT on the back panel of the DI-724GU. The WAN LED light will illuminate to indicate proper connection. If the WAN LED is not illuminated, please go back to step B1 and repeat the instructions.

C. Insert an Ethernet cable to LAN port 1 on the back panel of the DI-724GU and an available Ethernet port on the network adapter in the computer you will use to configure the DI-724GU. The LED light for LAN Port 1 will illuminate to indicate proper connection.

Note: *The LAN Ports on the DI-724GU are Auto-MDI/MDIX. Meaning you can use a straight-through or crossover Ethernet cable to the LAN Ports*.

D. Computers equipped with 802.11g wireless adapters will be able to connect to the DI-724GU. The DWL-G650 *Air*Plus *Xtreme G* Wireless Cardbus Adapter and the DWL-G520 *Air*Plus *Xtreme G* Wireless PCI Adapter will be able to connect out of the box with the router using their default wireless settings.

Network Overview



Please remember that D-Link Wireless 108G devices are pre-configured to connect together, right out of the box, with their default settings.

Wireless Installation Considerations

The D-Link Wireless 108G Gigabit QoS Router lets you access your network using a wireless connection from virtually anywhere within the operating range of your wireless network. Keep in mind, however, that the number, thickness and location of walls, ceilings, or other objects that the wireless signals must pass through, may limit the range. Typical ranges vary depending on the types of materials and background RF (radio frequency) noise in your home or business. The key to maximizing wireless range is to follow these basic guidelines:

1. Keep the number of walls and ceilings between the D-Link adapter and other network devices to a minimum - each wall or ceiling can reduce your adapter's range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling (instead of at an angle) for better reception.

3. Building Materials make a difference. A solid metal door or aluminum studs may have a negative effect on range. Try to position access points, wireless routers, and computers so that the signal passes through drywall or open doorways. Materials and objects such as glass, steel, metal, walls with insulation, water (fish tanks), mirrors, file cabinets, brick, and concrete will degrade your wireless signal.

4. Keep your product away (at least 3-6 feet or 1-2 meters) from electrical devices or appliances that generate RF noise.

5. If you are using 2.4GHz cordless phones or X-10 (wireless products such as ceiling fans, lights, and home security systems), your wireless connection may degrade dramatically or drop completely. Make sure your 2.4GHz phone base is as far away from your wireless devices as possible. The base transmits a signal even if the phone in not in use.

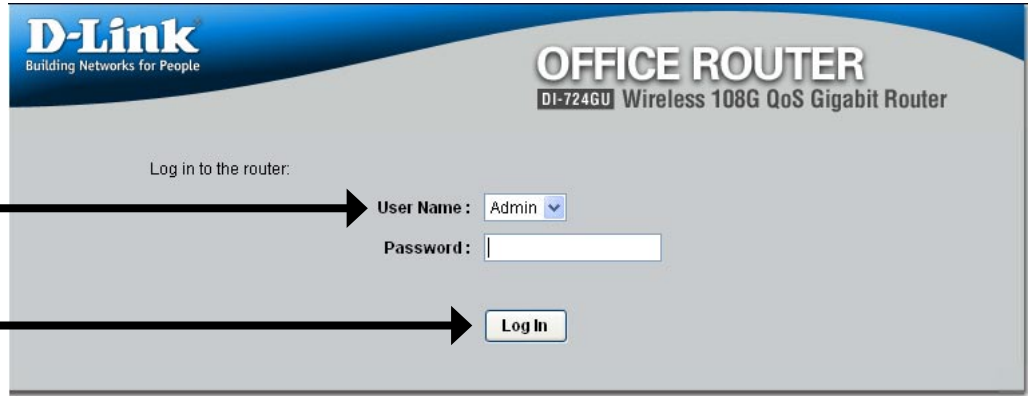
Configuration

This section will show you how to configure your new D-Link Wireless 108G Gigabit QoS Router using the D-Link Setup Wizard.

Open your Web browser and type **"http://192.168.0.1"** into the URL address box. Then press the **Enter** or **Return** key.

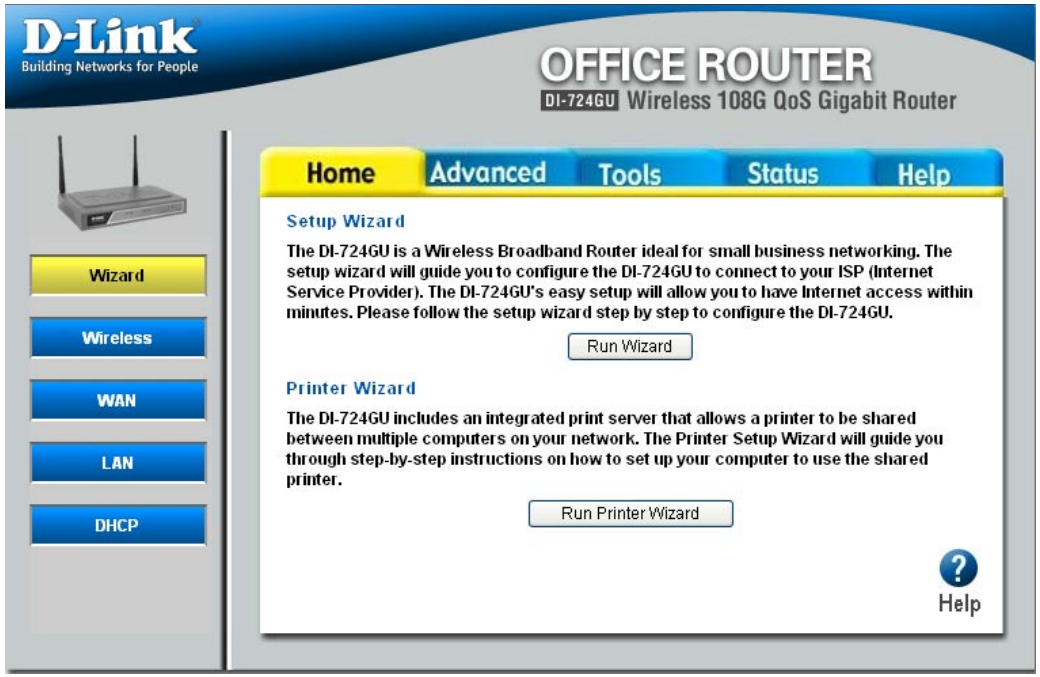
Select "**Admin**" from the User Name drop down menu and leave the password field blank.

Click **Login**



Home Page Screen

The image from the DI-724GU should be visible from the Home page on your computer monitor.



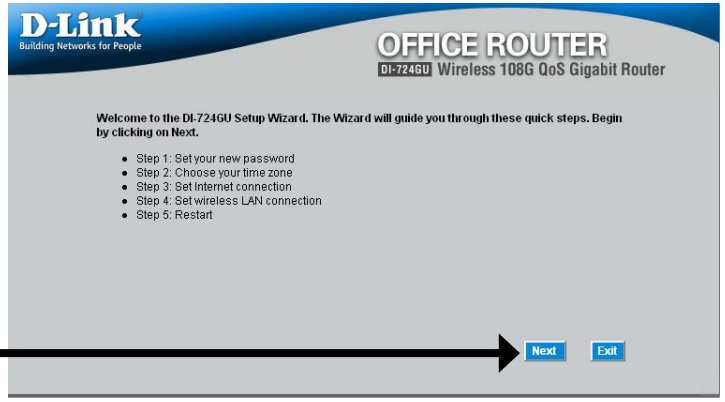
Run Wizard: This wizard guides you through the following basic router setup steps:

- Set your Password
- Select your Time Zone
- Configure your Internet Connection
- Configure the Wireless LAN Connection
- Restart

Continue to page 14 for instructions on running the Wizard.

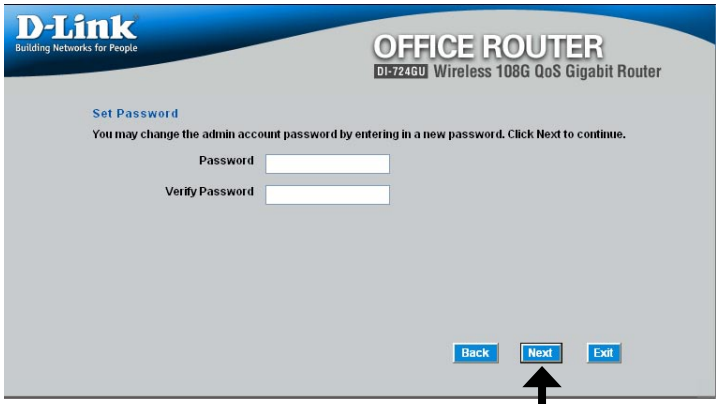
Run Print Wizard: Before you can use a printer that is plugged into the router's USB connector, you must configure your computer for that printer. If the operating system of your computer is Win32 compatible, all you need to do is click the **Printer Wizard** button, and the configuration is done by a Printer Wizard program. The Printer Wizard provides the necessary printer setup link between your PC and the router via the browser. The browser downloads the Printer Wizard program to your PC. You should already have a WAN connection, so that the browser can access the latest version of the program; however, the browser can always download some version of the program from the router itself. If the browser displays a pop-up window requesting permission to download the Printer Wizard program, answer Yes or OK. Continue to page 23 for instructions on running the Printer Wizard.

Setup Wizard



Click **Next**

You have the option to establish a password for the User Name “Admin”.



Click **Next**

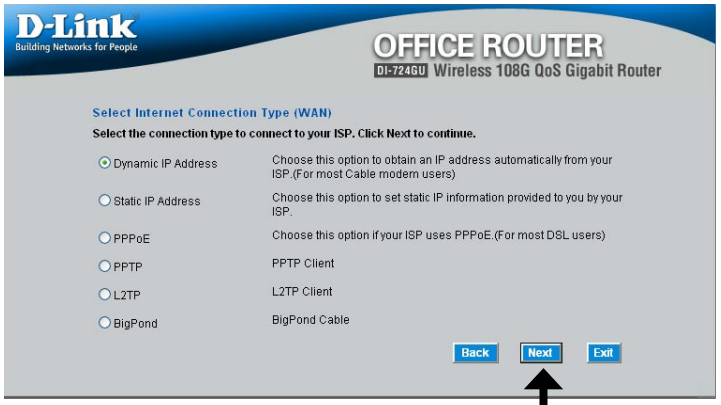
Choose your time zone from the drop down list.

Click **Next**

Dynamic IP Address

You will be prompted to select the type of Internet connection for your router. If you are unsure of which setting to select, please contact your Internet Service Provider.

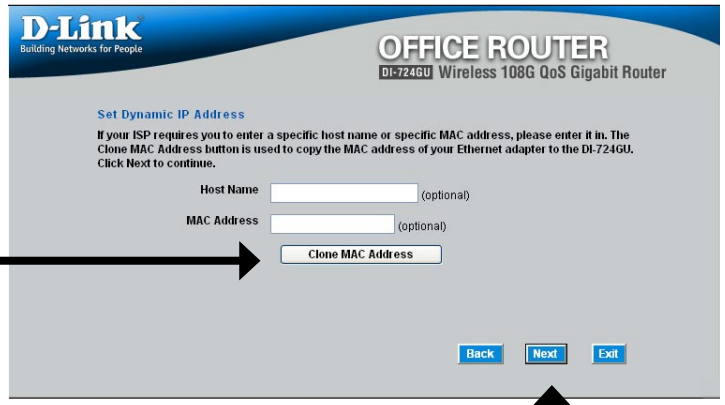
Static IP Address - page 16
PPPoE - page 17
PPTP - page 18
L2TP - page 19
Big Pond - page 20



Click **Next**

If you selected Dynamic IP Address, this screen will appear: (Used mainly for Cable Internet service).

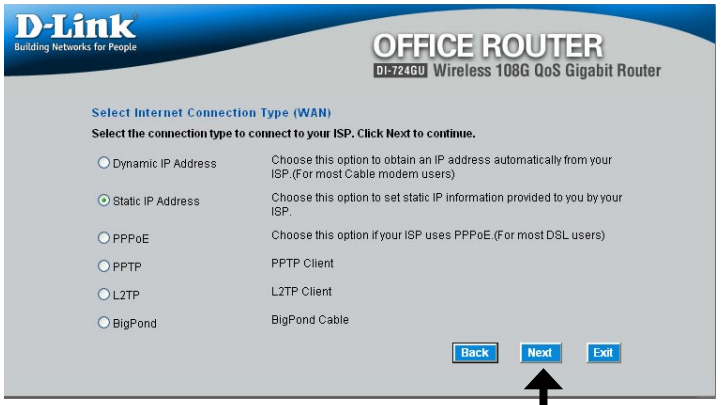
Click the **"Clone MAC Address"** button to automatically copy the MAC address of the network adapter in your computer. You can also manually type in the MAC address.



Click **Next**

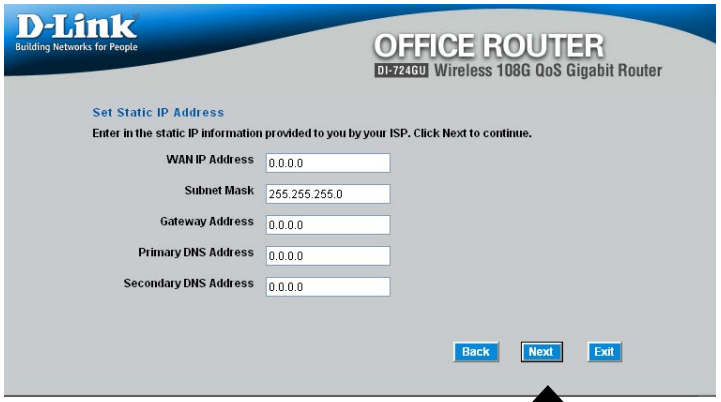
Static IP Address

If your ISP requires a Static IP Address, select the corresponding radio button.



Click **Next**

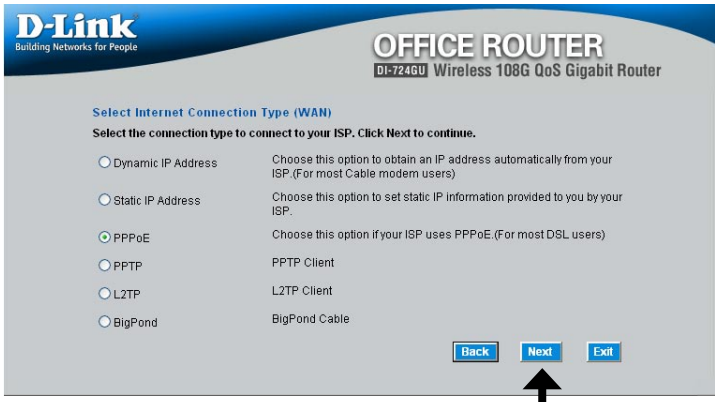
Enter the IP address that was originally provided to you by your ISP. You will need to complete all of the required fields.



Click **Next**

PPPoE

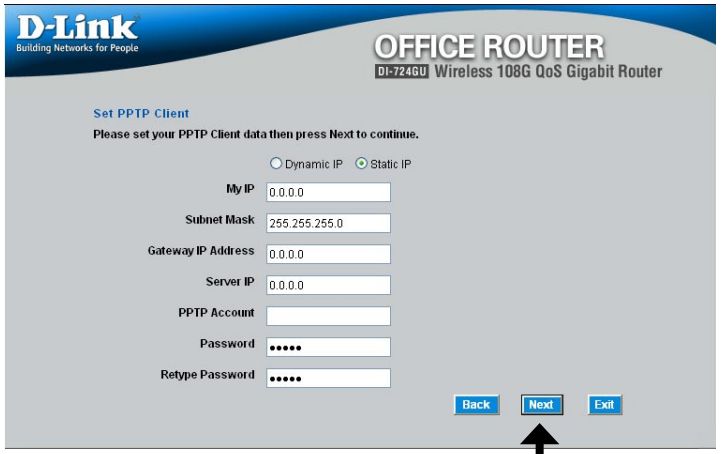
If your ISP uses PPPoE (Point-to-Point Protocol over Ethernet), select the corresponding radio button.



Click **Next**

If you have a Dynamic IP connection, enter the Server IP, PPPoE Account, and Password provided to you by your ISP.

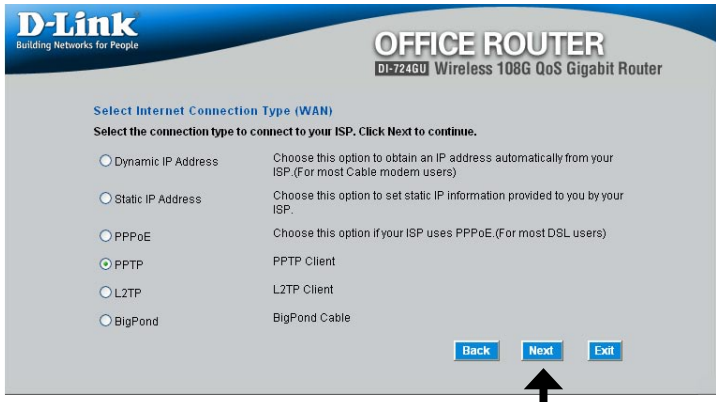
If you have a Static IP connection, enter the IP Address, Subnet Mask, Gateway IP Address, Server IP, PPTP Account, and Password provided to you by your ISP.



Click **Next**

PPTP

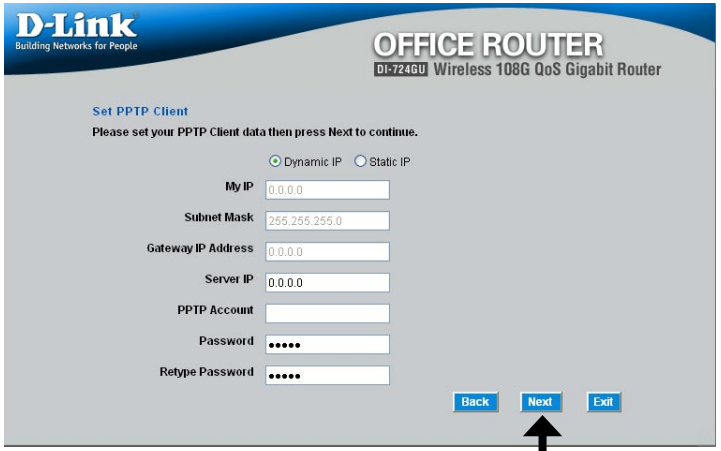
If your ISP uses PPTP (Point to Point Tunneling Protocol), select the corresponding radio button.



Click **Next**

If you have a Dynamic IP connection, enter the Server IP, PPTP Account, and Password provided to you by your ISP.

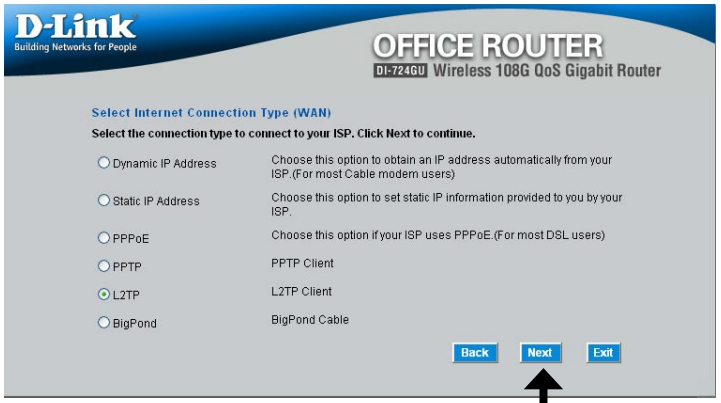
If you have a Static IP connection, enter the IP Address, Subnet Mask, Gateway IP Address, Server IP, PPTP Account, and Password provided to you by your ISP.



Click **Next**

L2TP

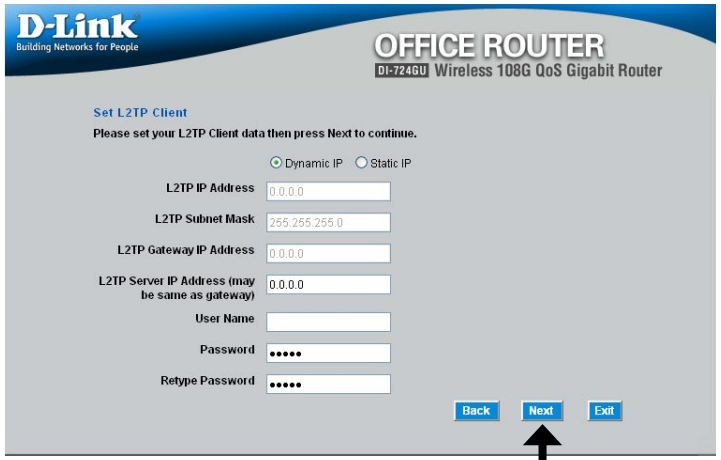
If your ISP uses L2TP (Layer Two Tunneling Protocol), select the corresponding radio button.



Click **Next**

If you have a Dynamic IP connection, enter the L2TP Server IP Address, User Name, and Password provided to you by your ISP.

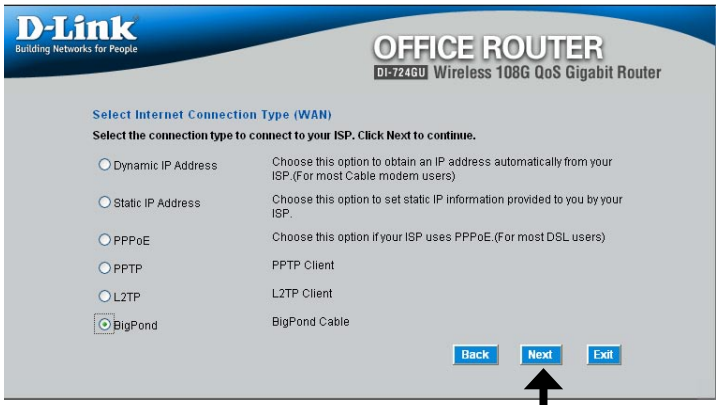
If you have a Static IP connection, enter the L2TP IP Address, Subnet Mask, Gateway IP Address, L2TP Server IP, User Name, and Password provided to you by your ISP.



Click **Next**

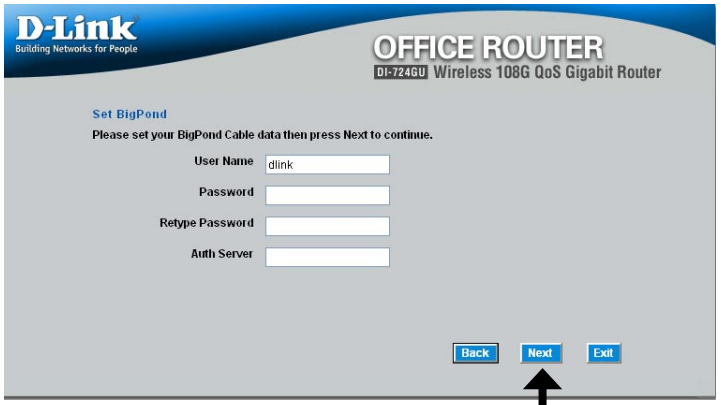
Big Pond

Select this option if you connect to the internet through Telstra BigPond Cable Broadband in Australia.



Click **Next**

Enter the User Name, and Password provided to you by your ISP.



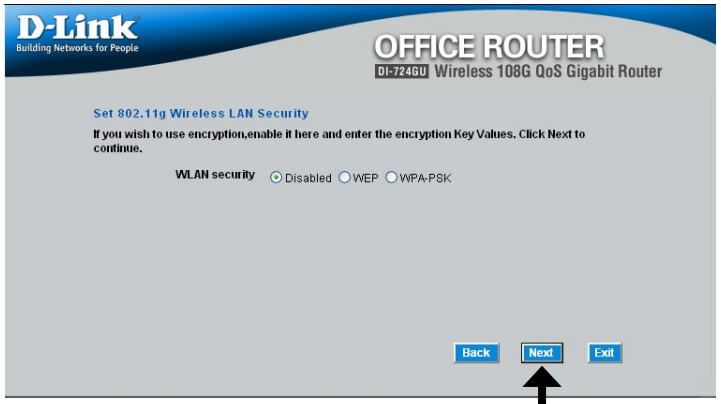
Click **Next**

Wireless Setup

The default wireless settings for your 802.11g wireless network are:
SSID = **dlink**
Channel = **6**
You can change these settings to match an existing wireless network.

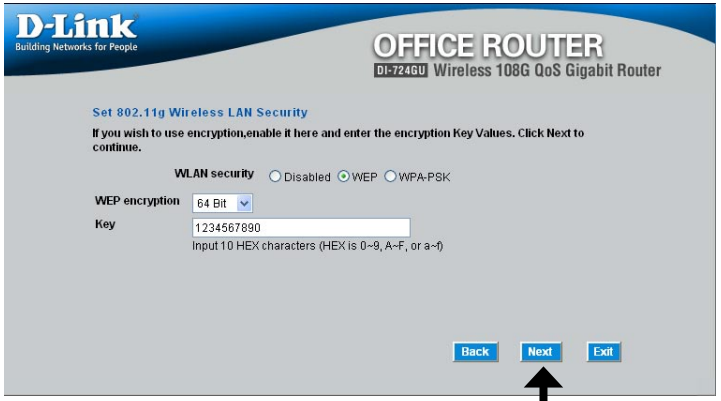
Click **Next**

If you wish to use encryption for your 802.11g network, the DI-724GU is capable of two types of wireless encryption WEP and WPA-PSK. By default the encryption is disabled. You can change the encryption settings for more secure wireless communication.



Click **Next**

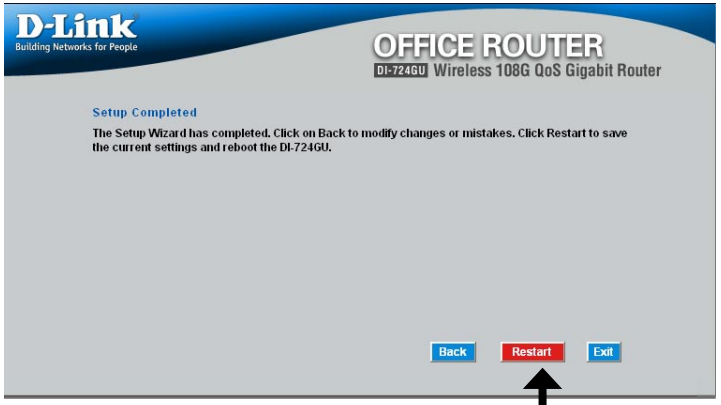
There are two levels of WEP encryption: 64-bit and 128-bit (using only Hexadecimal). You can change the encryption settings for more secure wireless communication.



Click **Next**

Enter a PassPhrase that is between 8 to 63 characters and is alphanumeric.

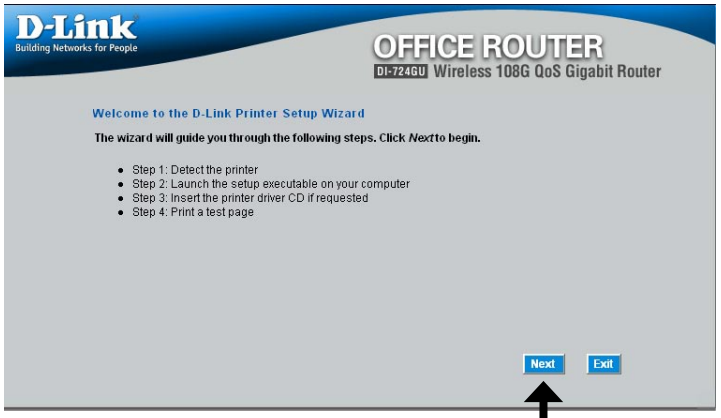
Click **Next**



Click **Restart**

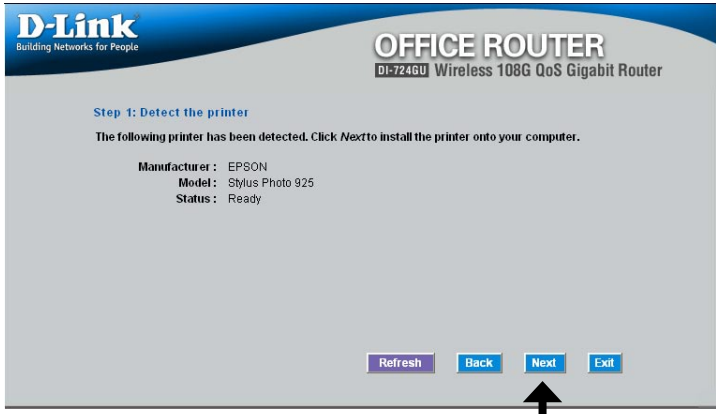
Printer Wizard

Before selecting to run the Print Wizard, make sure your printer is connected to the USB port on the router.



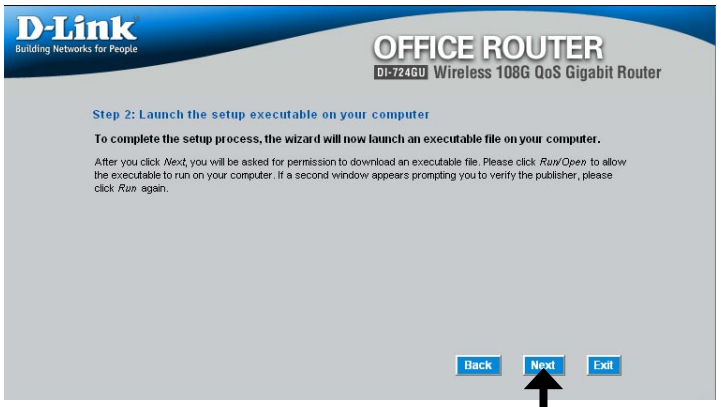
Click **Next**

The wizard will identify the make and model of your printer, as well as its status.



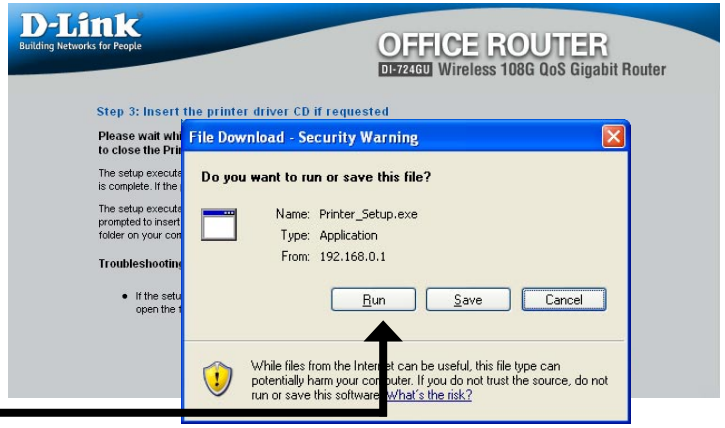
Click **Next**

Click **Next** to run the Printer Setup application.



Click **Next**

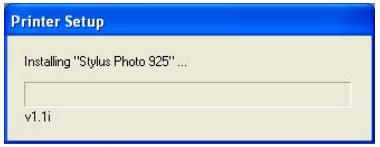
This application can only run when accessed from the router. Do not click **Save**.

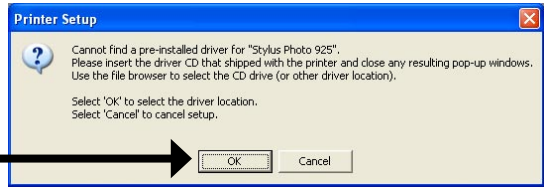


Click **Next**

Click **Next**

You may need to supply the drivers for your printer if they are not built into Windows®.



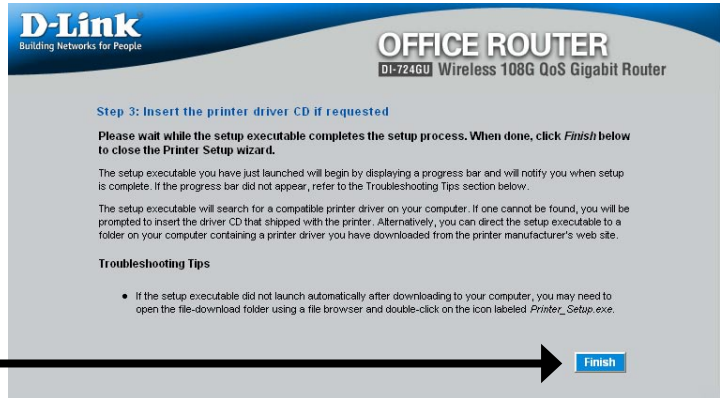


Click **OK**

Click **Browse** to locate the driver and then click **OK**.

Once the wizard has completed installing your printer, you will be prompted to print a test page to verify its functionality.

Click **OK**



Click **Finish**

Wireless

Wireless Radio: This gives you the option to turn off the wireless portion of the router. By default this feature is on.

SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is "dlink". The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Channel: 6 is the default channel. All devices on the network must share the same channel.

Note: *The wireless adapters will automatically scan and match the wireless setting.*

Super G™ Mode: The default Super G setting is Super G with Dynamic Turbo. Super G is a group of performance enhancement features that increase end user application throughput in an 802.11g network. Super G is backward compatible to standard 802.11g devices. For top performance, all wireless devices on the network should be Super G capable. Select either Disabled, Super G without Turbo, Super G with Dynamic Turbo, or Super G with Static Turbo.

Transmission Rate: This allows you to specify the rate at which wireless clients are allowed to connect to the router at. Default is set to Auto.

802.11g Only Mode: If all of the wireless devices you want to connect with this router can connect in 802.11g mode, you can improve performance slightly by enabling this mode. If you want to connect 802.11b devices to this router, leave this option disabled.

SSID Broadcast: Service Set Identifier (SSID) is the name that identifies a specific wireless local area network (WLAN). When a wireless device is browsing for available wireless networks, this is the name that will appear in the list. For security purposes, it is highly recommended to change from the preconfigured network name. You can change the SSID to match an existing wireless network or create a new name to establish a new wireless network.

Security Mode: To protect your privacy, use the wireless security mode to configure the wireless security features. This device supports three wireless security modes including: WEP, WPA-Personal, and WPA-Enterprise. WEP is the original wireless encryption standard. WPA provides a higher level of security. WPA-Personal does not require an authentication server. The WPA-Enterprise option does require a RADIUS authentication server.

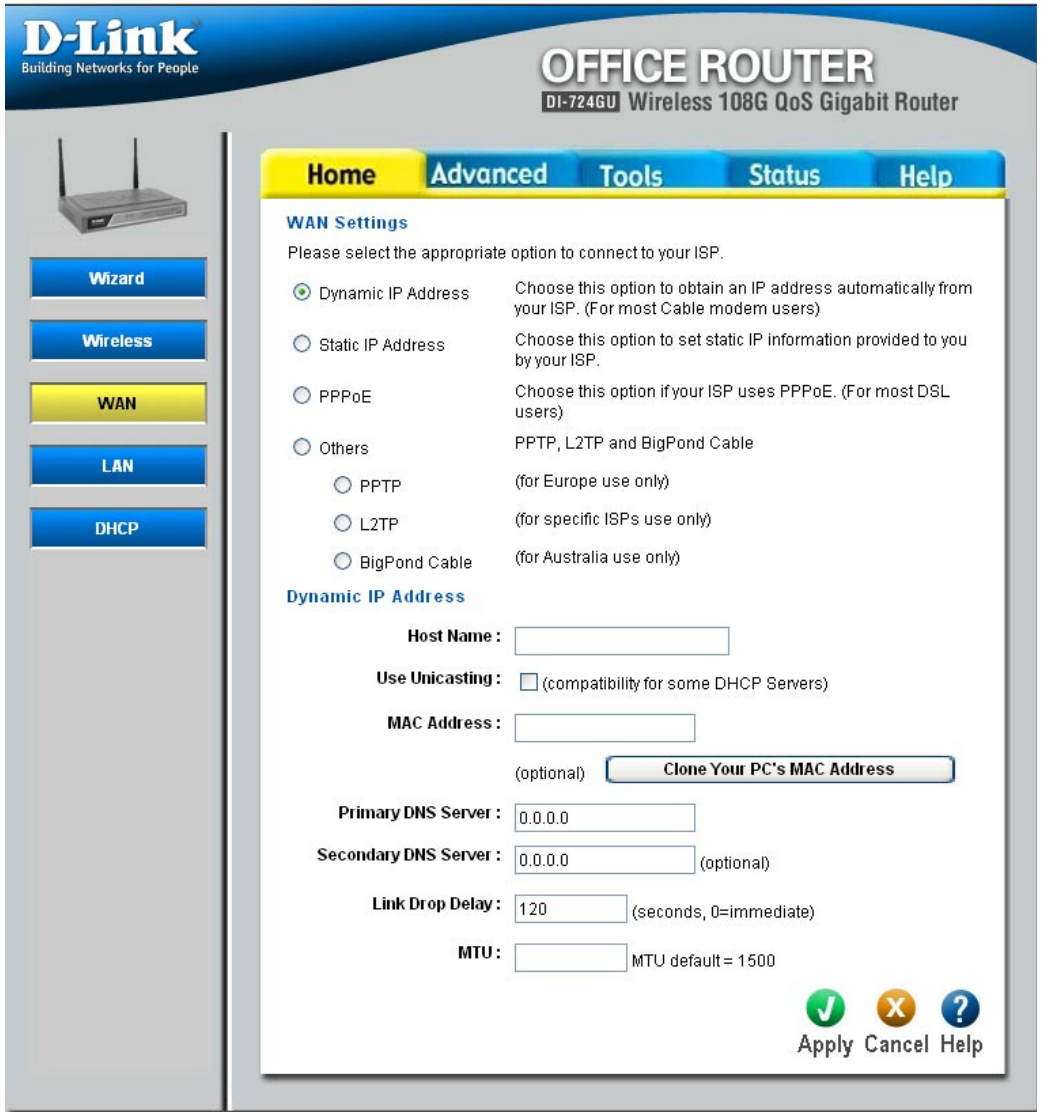
WAN

Dynamic IP Address

Dynamic IP Address: A method of connection where the your ISP assigns your IP address when your router requests one from the ISP's server. Some ISP's require you to make some settings on your side before your router can connect to the Internet.

Host Name: The Host Name is optional, but some ISPs may require it. The Host Name identifies your router to the ISP's server. This way they know your router is eligible to receive an IP address.

Use Unicasting: This option is normally turned off, and should remain off as long as the WAN-side DHCP server correctly provides an IP address to the router. However, if the router cannot obtain an IP address from the DHCP server, the DHCP server may be one that works better with unicast responses. In this case, turn the unicasting option on, and observe whether the router can obtain an IP address. In this mode, the router accepts unicast responses from the DHCP server instead of broadcast responses.



MAC Address: The MAC address is optional, but some ISPs may require it, in which case the MAC address of the router must equal the MAC address that is registered with your ISP account. Each networking device has its own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. Your new router has a different MAC address than the computer or router that initially connected to the ISP. The default MAC address of the router is set to the MAC address of the WAN interface in the device. You can either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the router using that computer and click the **Clone Your PC's MAC Address** button. The WAN port will then use the MAC address of the network adapter in your computer.

Primary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Secondary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Link Drop Delay: When the the router detects that the WAN cable has been disconnected, it waits for "Link Drop Delay" seconds before treating the WAN connection as broken. This delay allows you to temporarily remove the WAN cable without dropping the logical connection to the ISP. It also allows for temporary electrical "glitches" in the physical connection. Values can range from 0 to 65535 seconds. A value of zero causes immediate disconnection when the cable is pulled or when a glitch occurs. Having to increase Link Drop Delay because you are experiencing WAN disconnections for long periods would suggest a fault with the cable or with the modem (if any) to which it is connected.

MTU: If this box is left blank, the router selects the usual MTU settings for the type of WAN interface in use. The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

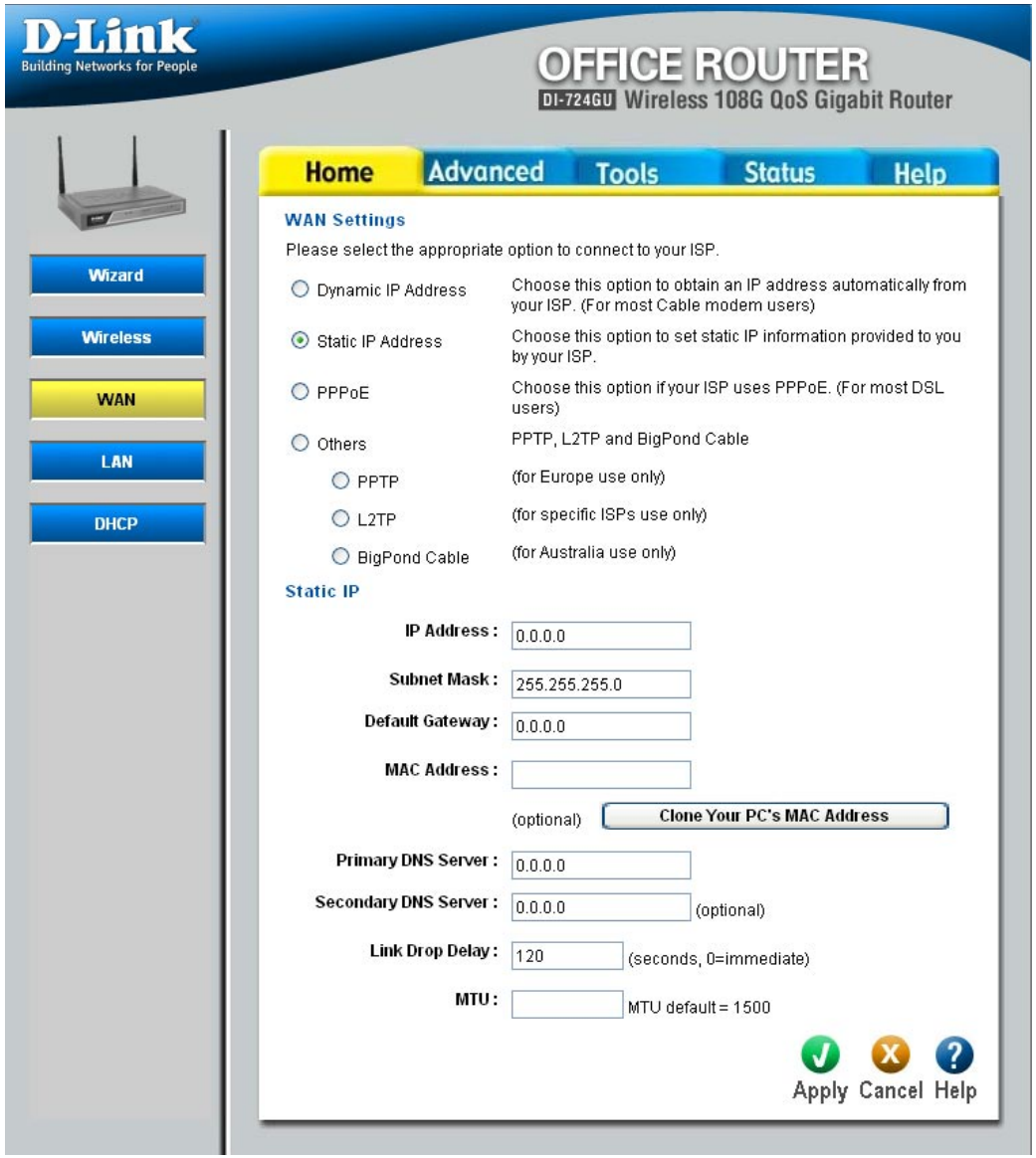
Static IP Address

Static IP Address: You must enter the **IP address, Subnet Mask, Gateway, Primary DNS Server,** and **Secondary DNS Server**. Your ISP provides you with all of this information.

Subnet Mask: Used when your ISP provides you an IP address that does not change. The IP information is manually entered in your IP configuration settings.

Default Gateway: When required, this value is provided by the ISP.

MAC Address: The MAC address is optional, but some ISPs may require it, in which case the MAC address of the router must equal the MAC address that is registered with your ISP account. Each networking device has its own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. Your new router has a different MAC address than the computer or router that initially connected to the ISP. The default MAC address of the router is set to the MAC address of the WAN interface in the device.



MAC Address (continued): You can either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the router using that computer and click the **Clone Your PC's MAC Address** button. The WAN port will then use the MAC address of the network adapter in your computer.

Primary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Secondary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Link Drop Delay: When the the router detects that the WAN cable has been disconnected, it waits for "Link Drop Delay" seconds before treating the WAN connection as broken. This delay allows you to temporarily remove the WAN cable without dropping the logical connection to the ISP. It also allows for temporary electrical "glitches" in the physical connection. Values can range from 0 to 65535 seconds. A value of zero causes immediate disconnection when the cable is pulled or when a glitch occurs. Having to increase Link Drop Delay because you are experiencing WAN disconnections for long periods would suggest a fault with the cable or with the modem (if any) to which it is connected.

MTU: If this box is left blank, the router selects the usual MTU settings for the type of WAN interface in use. The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

PPPoE

PPPoE: Select this option if your ISP requires you to use a PPPoE (Point to Point Protocol over Ethernet) connection. DSL providers typically use this option. This method of connection requires you to enter a **Username** and **Password** (provided by your Internet Service Provider) to gain access to the Internet.

Note: *When using the PPPoE option, you will need to ensure that any PPPoE client software on your computers is removed or disabled.*

Dynamic IP/Static IP: If your ISP has assigned a fixed IP address, select Static IP and enter the fixed IP address in the following field. For PPTP and L2TP, the subnet mask and the default gateway IP address must also be entered. If the ISP's servers assign these values upon establishing a connection, select Dynamic IP.

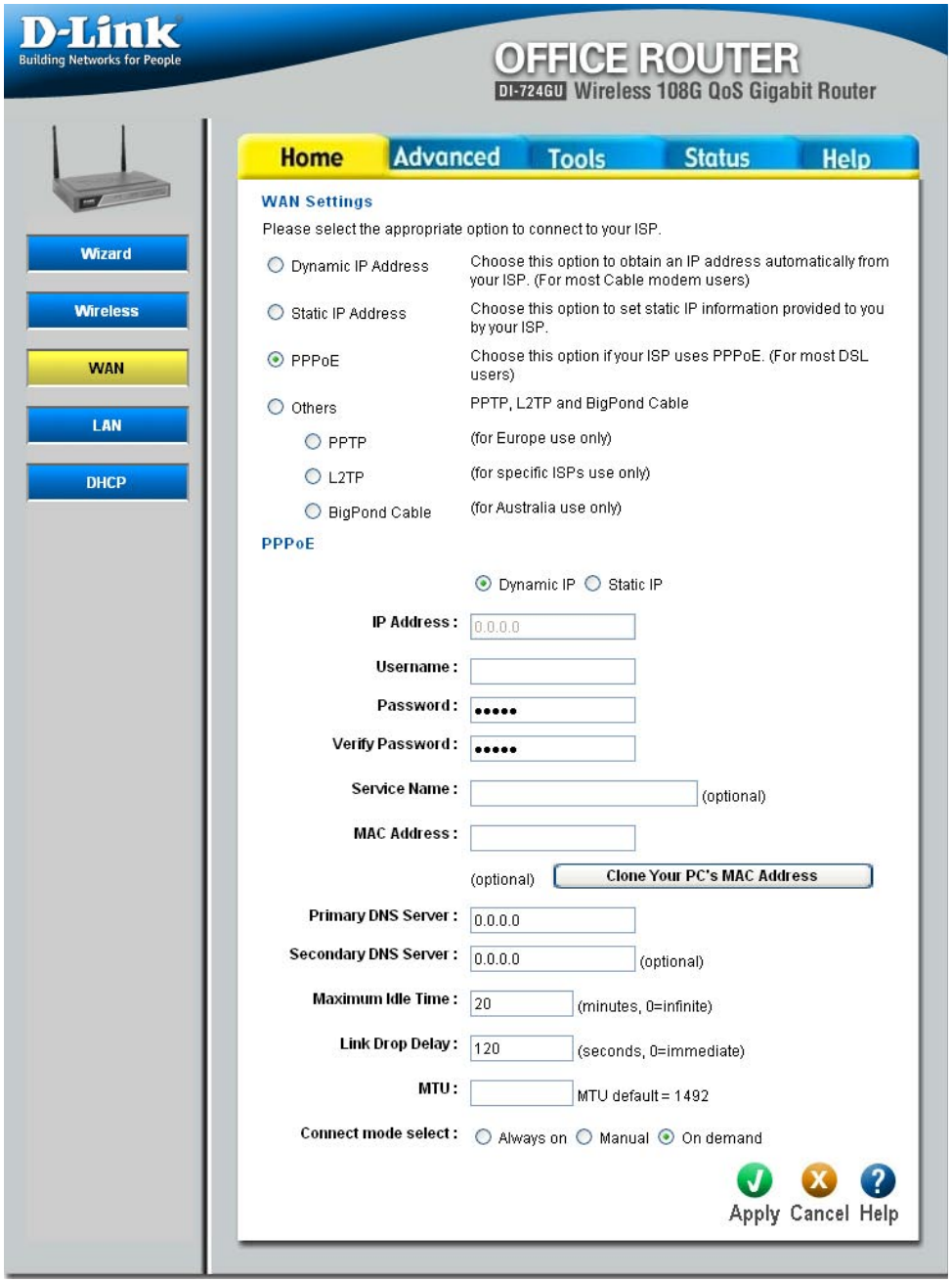
IP Address: When required, this value is provided by the ISP.

Username: This value is provided by agreement between you and the ISP.

Password: This value is provided by agreement between you and the ISP.

Verify Password: Re-enter the password.

Service Name: Service Name is optional, but may be required by some ISPs. If your ISP provides a Service Name, enter the provided value here.



MAC Address: The MAC address is optional, but some ISPs may require it, in which case the MAC address of the router must equal the MAC address that is registered with your ISP account. Each networking device has its own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. Your new router has a different MAC address than the computer or router that initially connected to the ISP. The default MAC address of the router is set to the MAC address of the WAN interface in the device. You can either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the router using that computer and click the **Clone Your PC's MAC Address** button. The WAN port will then use the MAC address of the network adapter in your computer.

Primary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Secondary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Maximum Idle Time: The Maximum Idle Time value is used for the "Connect on demand" and "Manual" connect modes. It specifies how many minutes the WAN connection can be idle before the connection is dropped. A value of zero means the connection will not be dropped due to idle time.

Link Drop Delay: When the the router detects that the WAN cable has been disconnected, it waits for "Link Drop Delay" seconds before treating the WAN connection as broken. This delay allows you to temporarily remove the WAN cable without dropping the logical connection to the ISP. It also allows for temporary electrical "glitches" in the physical connection. Values can range from 0 to 65535 seconds. A value of zero causes immediate disconnection when the cable is pulled or when a glitch occurs. Having to increase Link Drop Delay because you are experiencing WAN disconnections for long periods would suggest a fault with the cable or with the modem (if any) to which it is connected.

MTU: If this box is left blank, the router selects the usual MTU settings for the type of WAN interface in use. The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router's MTU is set too high, packets will be fragmented downstream. If the router's MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

Connect mode select: Typically, connections such as PPPoE, PPTP, and L2TP are not always on. The router allows you to set the connection mode. Choose **Always on**, **Connect on demand**, or **Manual.**

PPTP

PPTP: PPTP (Point to Point Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection is primarily used in Europe. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet. The ISP provides the values for **PPTP IP Address, PPTP Subnet Mask , PPTP Gateway IP Address**, and **PPTP Server IP Address** (may be the same as the gateway).

Dynamic IP/Static IP: If your ISP has assigned a fixed IP address, select Static IP and enter the fixed IP address in the following field. For PPTP and L2TP, the subnet mask and the default gateway IP address must also be entered. If the ISP's servers assign these values upon establishing a connection, select Dynamic IP.

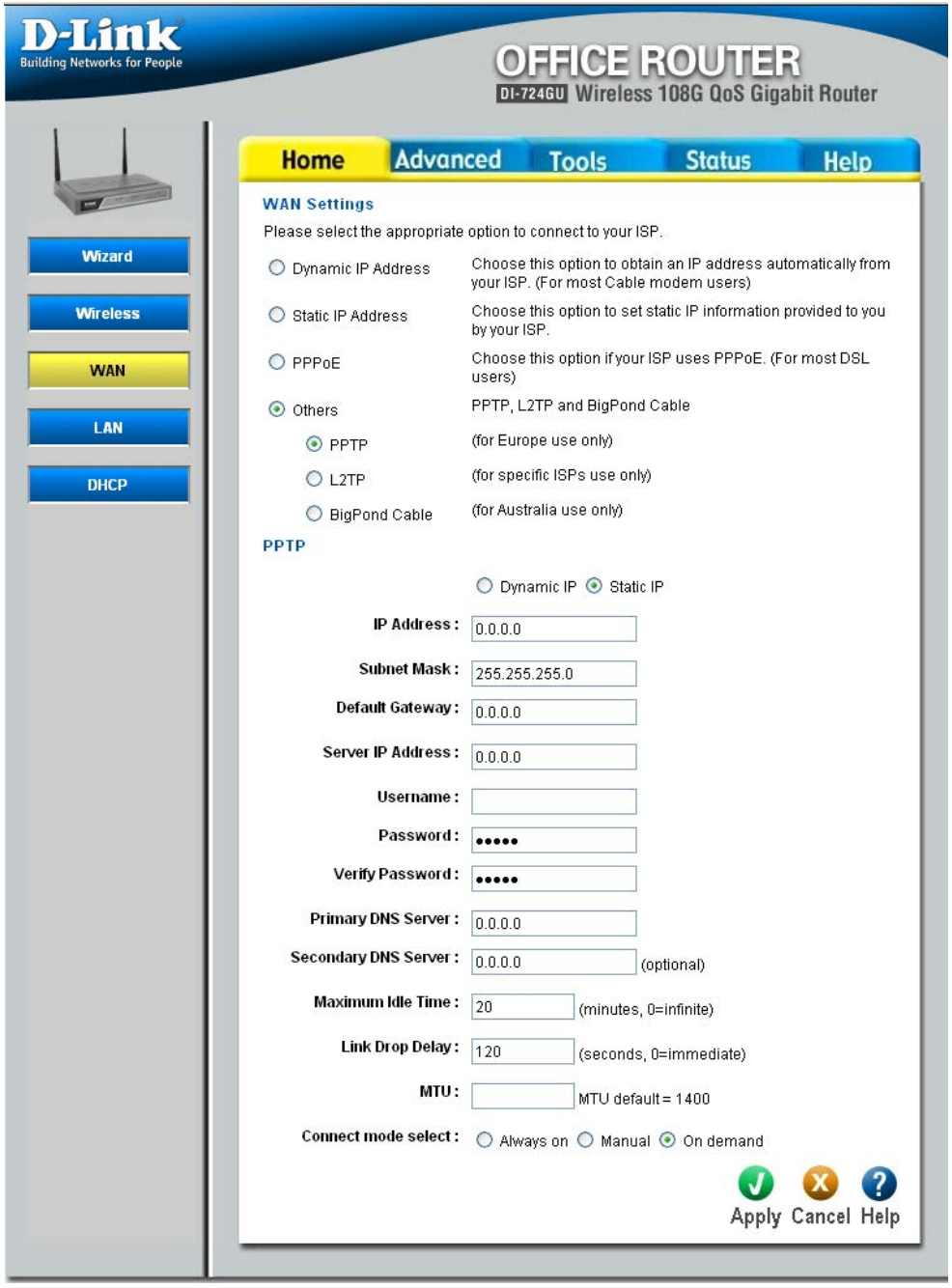
IP Address: When required, this value is provided by the ISP.

Subnet Mask: When required, this value is provided by the ISP.

Default Gateway: When required, this value is provided by the ISP.

Server IP Address: When required, this value is provided by the ISP.

Username: This value is provided by agreement between you and the ISP.



Password: This value is provided by agreement between you and the ISP.

Verify Password: Re-enter the password.

Primary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Secondary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Maximum Idle Time: The Maximum Idle Time value is used for the “Connect on demand” and “Manual” connect modes. It specifies how many minutes the WAN connection can be idle before the connection is dropped. A value of zero means the connection will not be dropped due to idle time.

Link Drop Delay: When the the router detects that the WAN cable has been disconnected, it waits for “Link Drop Delay” seconds before treating the WAN connection as broken. This delay allows you to temporarily remove the WAN cable without dropping the logical connection to the ISP. It also allows for temporary electrical “glitches” in the physical connection. Values can range from 0 to 65535 seconds. A value of zero causes immediate disconnection when the cable is pulled or when a glitch occurs. Having to increase Link Drop Delay because you are experiencing WAN disconnections for long periods would suggest a fault with the cable or with the modem (if any) to which it is connected.

MTU: If this box is left blank, the router selects the usual MTU settings for the type of WAN interface in use. The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router’s MTU is set too high, packets will be fragmented downstream. If the router’s MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

Connect mode select: Typically, connections such as PPPoE, PPTP, and L2TP are not always on. The router allows you to set the connection mode. Choose **Always on**, **Connect on demand**, or **Manual.**

L2TP

L2TP: L2TP (Layer Two Tunneling Protocol) uses a virtual private network to connect to your ISP. This method of connection requires you to enter a Username and Password (provided by your Internet Service Provider) to gain access to the Internet. The ISP provides the values for **L2TP IP Address, L2TP Subnet Mask , L2TP Gateway IP Address**, and **L2TP Server IP Address** (may be the same as the gateway).

Dynamic IP/Static IP: If your ISP has assigned a fixed IP address, select Static IP and enter the fixed IP address in the following field. For PPTP and L2TP, the subnet mask and the default gateway IP address must also be entered. If the ISP's servers assign these values upon establishing a connection, select Dynamic IP.

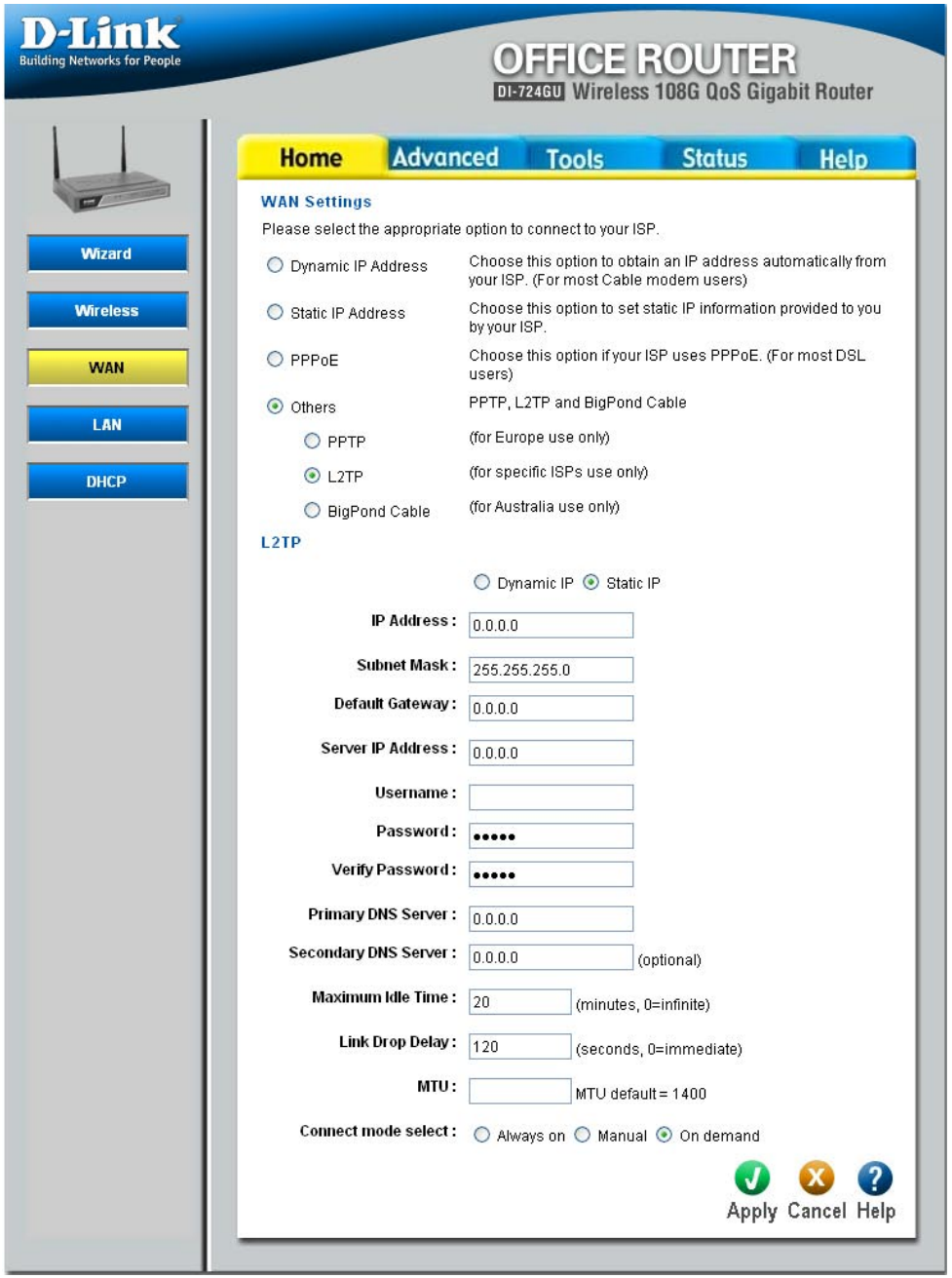
IP Address: When required, this value is provided by the ISP.

Subnet Mask: When required, this value is provided by the ISP.

Default Gateway: When required, this value is provided by the ISP.

Server IP Address: When required, this value is provided by the ISP.

Username: This value is provided by agreement between you and the ISP.



Password: This value is provided by agreement between you and the ISP.

Verify Password: Re-enter the password.

Primary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Secondary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Maximum Idle Time: The Maximum Idle Time value is used for the “Connect on demand” and “Manual” connect modes. It specifies how many minutes the WAN connection can be idle before the connection is dropped. A value of zero means the connection will not be dropped due to idle time.

Link Drop Delay: When the the router detects that the WAN cable has been disconnected, it waits for “Link Drop Delay” seconds before treating the WAN connection as broken. This delay allows you to temporarily remove the WAN cable without dropping the logical connection to the ISP. It also allows for temporary electrical “glitches” in the physical connection. Values can range from 0 to 65535 seconds. A value of zero causes immediate disconnection when the cable is pulled or when a glitch occurs. Having to increase Link Drop Delay because you are experiencing WAN disconnections for long periods would suggest a fault with the cable or with the modem (if any) to which it is connected.

MTU: If this box is left blank, the router selects the usual MTU settings for the type of WAN interface in use. The Maximum Transmission Unit (MTU) is a parameter that determines the largest packet size (in bytes) that the router will send to the WAN. If LAN devices send larger packets, the router will break them into smaller packets. Ideally, you should set this to match the MTU of the connection to your ISP. Typical values are 1500 bytes for an Ethernet connection and 1492 bytes for a PPPoE connection. If the router’s MTU is set too high, packets will be fragmented downstream. If the router’s MTU is set too low, the router will fragment packets unnecessarily and in extreme cases may be unable to establish some connections. In either case, network performance can suffer.

Connect mode select: Typically, connections such as PPPoE, PPTP, and L2TP are not always on. The router allows you to set the connection mode. Choose **Always on**, **Connect on demand**, or **Manual.**

Big Pond

BigPond Cable: Connect to the internet through Telstra BigPond Cable Broadband in Australia. Telstra BigPond provides the values for **BigPond Server, BigPond User Id**, and **BigPond Password**.

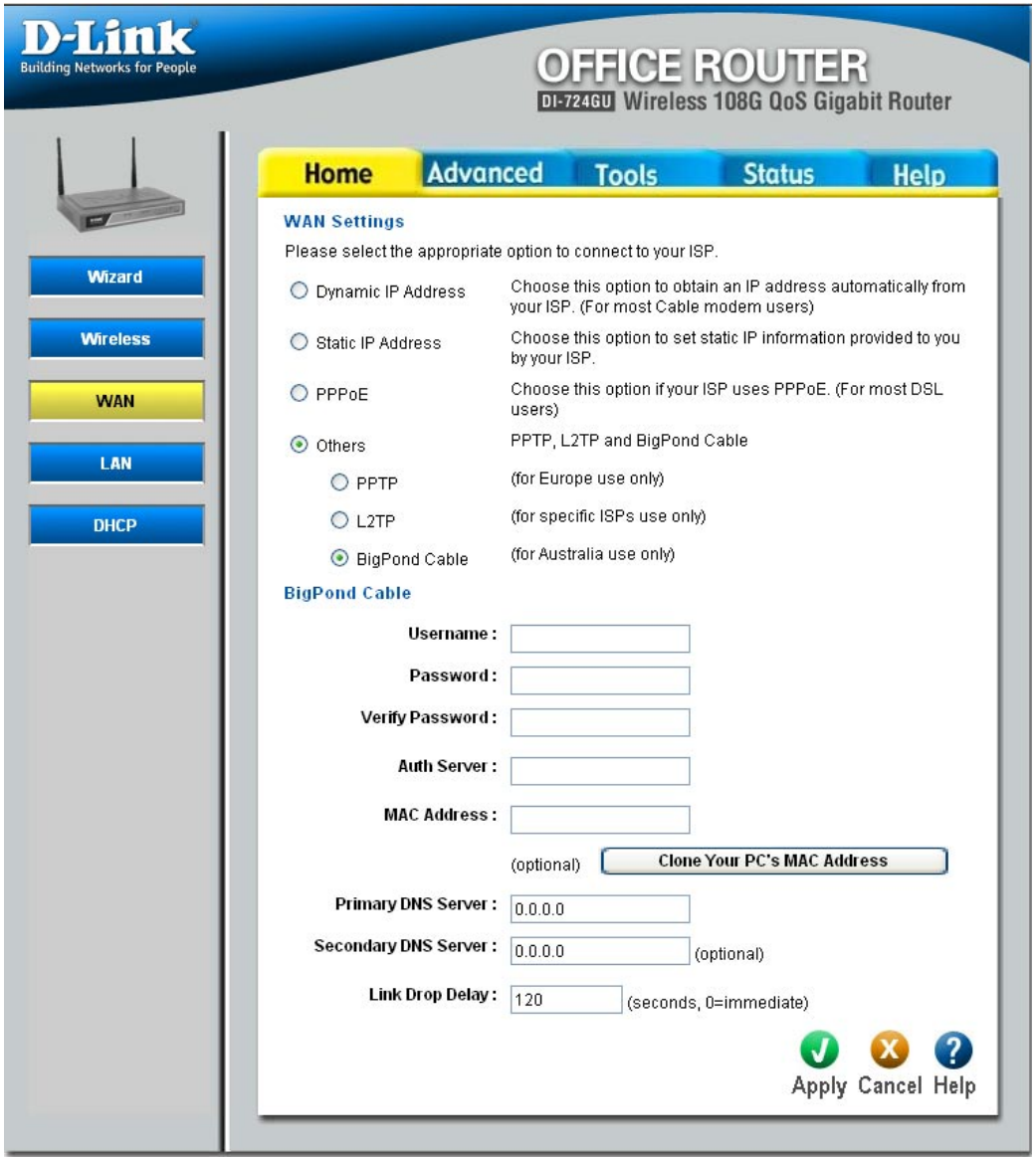
Username: This value is provided by agreement between you and the ISP.

Password: This value is provided by agreement between you and the ISP.

Verify Password: Re-enter the password.

Auth Server: When required, this value is provided by the ISP.

MAC Address: The MAC address is optional, but some ISPs may require it, in which case the MAC address of the router must equal the MAC address that is registered with your ISP account. Each networking device has its own unique MAC address defined by the hardware manufacturer. Some ISP's record the MAC address of the network adapter in the computer or router used to initially connect to their service. The ISP will then only grant Internet access to requests from a computer or router with this particular MAC address. Your new router has a different MAC address than the computer or router that initially connected to the ISP. The default



MAC address of the router is set to the MAC address of the WAN interface in the device. You can either type in an alternate MAC address (for example, the MAC address of the router initially connected to the ISP) or copy the MAC address of a PC. To copy the MAC address of the computer that initially connected to the ISP, connect to the router using that computer and click the **Clone Your PC's MAC Address** button. The WAN port will then use the MAC address of the network adapter in your computer.

Primary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Secondary DNS Address: The IP address of the Domain Name Server. Your ISP will provide this information if it is required; otherwise, leave this box set to 0.0.0.0.

Link Drop Delay: When the the router detects that the WAN cable has been disconnected, it waits for "Link Drop Delay" seconds before treating the WAN connection as broken. This delay allows you to temporarily remove the WAN cable without dropping the logical connection to the ISP. It also allows for temporary electrical "glitches" in the physical connection. Values can range from 0 to 65535 seconds. A value of zero causes immediate disconnection when the cable is pulled or when a glitch occurs. Having to increase Link Drop Delay because you are experiencing WAN disconnections for long periods would suggest a fault with the cable or with the modem (if any) to which it is connected.

LAN

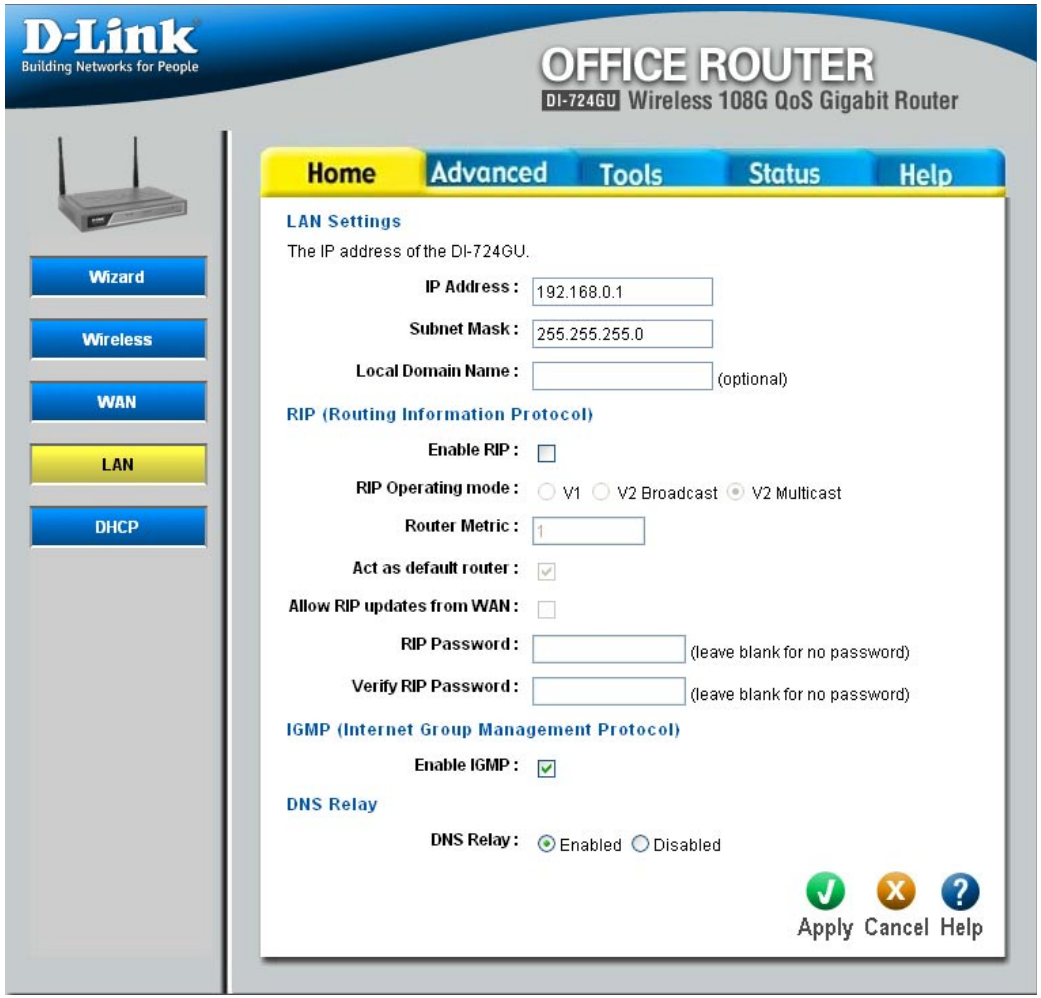
IP Address: The IP address of your router on the local area network. Your local area network settings are based on the address assigned here. For example, 192.168.0.1.

Subnet Mask: The subnet mask of your router on the local area network.

Local Domain Name: This entry is optional. Enter a domain name for the local network. The DHCP server will give this domain name to the computers on the LAN. So, for example, if you enter mynetwork.net here, and you have a PC with a name of chris, that PC will be known as chris.mynetwork.net. Note, however, if the router's WAN settings specify Dynamic IP Address, and the ISP's DHCP server assigns a domain name to the router, that domain name will override any name you enter here.

Enable RIP: Enable RIP if required by the ISP, if the LAN has multiple routers, or if the LAN has auto-IP devices.

RIP Operating mode: This router supports both version 2 and version 1 of the RIP specification.



V1. Use if none of the routers supports Version 2.

V2 Broadcast. Use if some routers are capable of Version 2, but some are only capable of Version 1.

V2 Multicast. Use if this is the only rounter on the LAN or if all the routers support Version 2.

Router Metric: The additional cost of the routing a packet through this router. The normal value for a simple network is 1. This metric is added to routes learned from other routers; it is not added to static or system routes.

Act as default router: Make this router the preferred destination for packets that are not otherwise destined.

Allow RIP updates from WAN: For security, disable this option unless required by the ISP.

RIP Password: RIP Version 2 supports the use of a password to limit access to routers through the RIP protocol. If the ISP or other LAN router requires a RIP password, enter the password here.

Verify RIP Password: Re-enter the password.

Enable IGMP: IGMP must be enabled if any applications on the LAN participate in a multicast group. If you have a multimedia LAN application that is not receiving content as expected, try enabling IGMP.

DNS Relay: When DNS Relay is enabled, the router plays the role of a DNS server. DNS requests sent to the router are forwarded to the ISP's DNS server. This provides a constant DNS address that LAN computers can use, even when the router obtains a different DNS server address from the ISP upon re-establishing the WAN connection. You should disable DNS relay if you implement a LAN-side DNS server as a virtual server.

DHCP

DHCP Server: Once the router is properly configured and this DHCP Server option is enabled, the DHCP Server will manage the IP addresses and other network configuration information for computers and other devices connected to the Local Area Network. There is no need for you to do this yourself.

The computers (and other devices) connected to your LAN also need to have their TCP/IP configuration set to “DHCP” or “Obtain an IP address automatically”.

DHCP IP Address Range: These two IP values (from and to) define a range of IP addresses that the DHCP Server uses when assigning addresses to computers and devices on your Local Area Network. Any addresses that are outside of this range are not managed by the DHCP Server; these could, therefore, be used for manually configured devices or devices that cannot use DHCP to obtain network address details automatically.

Lease Time: The amount of time that a computer may have an IP address before it is required to renew the lease. The lease functions just as a lease on an apartment would. The initial lease designates the amount of time before the lease expires. If the tenant wishes to retain the address when the lease is expired then a new lease is established. If the lease expires and the address is no longer needed than another tenant may use the address.

Always Broadcast: If all the computers on the LAN successfully obtain their IP addresses from the router's DHCP server as expected, this option can remain disabled. However, if one of the computers on the LAN fails to obtain an IP address from the router's DHCP server, it may have an old DHCP client that incorrectly turns off the broadcast flag of DHCP packets. Enabling this option will cause the router to always broadcast its responses to all clients, thereby working around the problem, at the cost of increased broadcast traffic on the LAN.

DHCP Reservations: In this section you can add reserved IP address to the DHCP Reservations List below or edit existing entries. Each entry in the table lets you reserve an IP addresses, and assign the same IP address to the network device with the specified MAC address any time it requests an IP address. This is almost the same as when a device has a static IP address except that the device must still request an IP address from the router. The router will provide the device the same IP address every time. DHCP Reservations are helpful for server computers on the local network that are hosting applications, such as Web and FTP. Servers on your network should either use a static IP address or use this option.

Computer Name: You can assign a name for each computer that is given a reserved IP address. This may help you keep track of which computers are assigned this way.

IP Address: The LAN address that you want to reserve.

MAC Address: To input the MAC address of your computer, enter it in manually or connect to the router's Web-Management interface from the computer and click the **Clone Your PC** button.

A MAC address is usually located on a sticker on the bottom of a network device. The MAC address is comprised of twelve digits. Each pair of hexadecimal digits are usually separated by dashes or colons such as 00-0D-88-11-22-33 or 00:0D:88:11:22:33. If your network device is a computer and the network card is already located inside the computer, you can connect to the D-Link router from the computer and click the **Clone Your PC** button to enter the MAC address.

Entry: Select either Enabled or Disabled.

DHCP Client: This is a list of the computers or other devices for which you have created Static DHCP entries. You can enable and disable entries with the Enabled checkbox. A Static DHCP entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "Static DHCP" section is activated for editing.

DHCP Reservations List: This is a list of the computers or other devices for which you have created reserved DHCP entries. You can enable and disable entries with the Enabled checkbox. A DHCP Reservation entry can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the "DHCP Reservations" section is activated for editing.

Dynamic DHCP Client List: In this section you can see what LAN devices are currently leasing IP addresses.

Advanced

Virtual Server

Enabled/ Disabled: Each list entry can be active or inactive, according to this selection.

Name: Assign a meaningful name to the virtual server, for example Web Server.

Clear: Clicking this button erases edits you have made to all items in the add/edit area of the screen.

Private IP: The IP address of the system on your internal network that will provide the virtual service, for example 192.168.0.50.

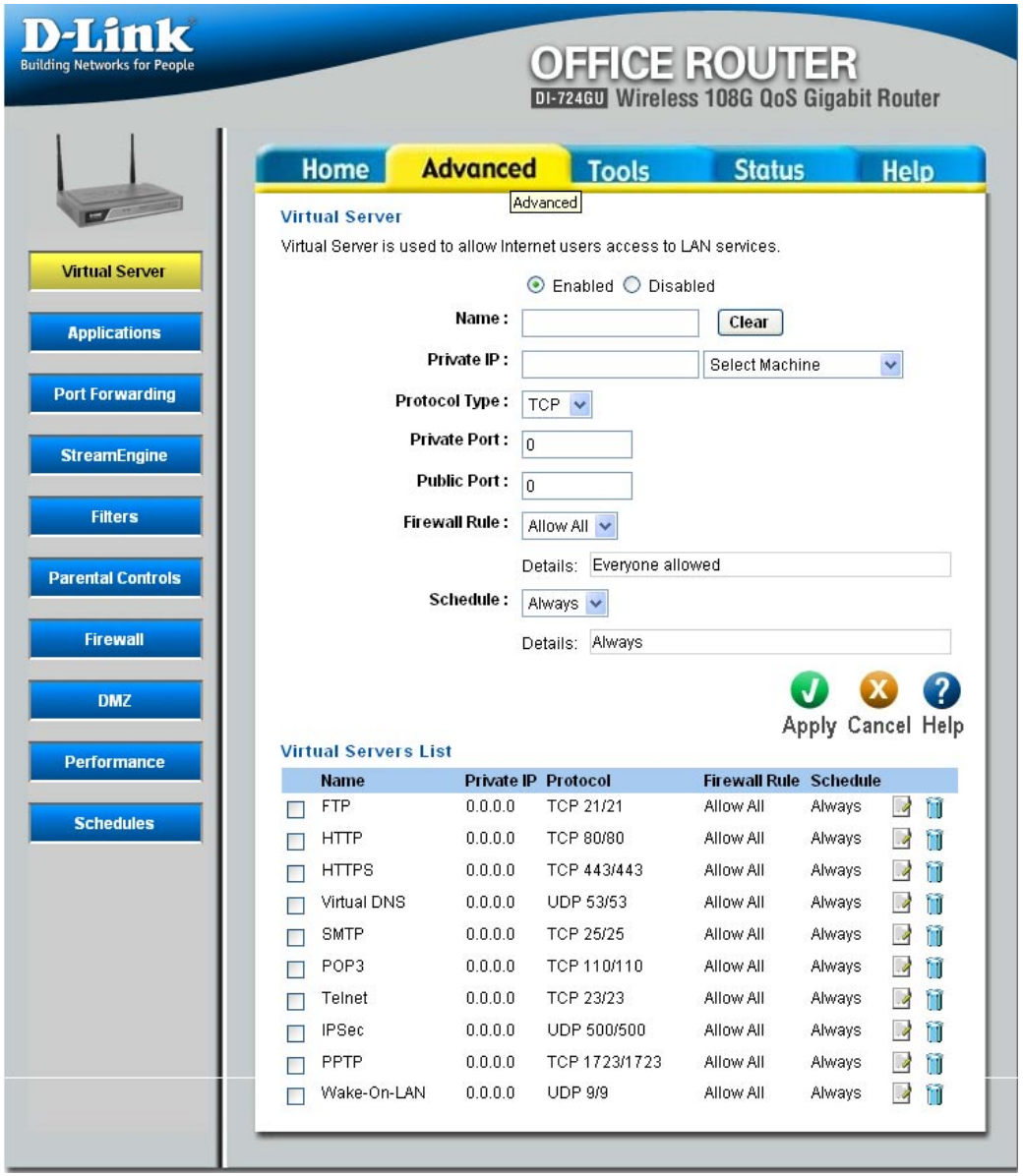
Protocol Type: Select the protocol used by the service.

Protocol Port: The port that will be used on your internal network.

Public Port: The port that will be accessed from the Internet.

Firewall: Select a firewall rule that controls access as needed for this virtual server. If you do not see the firewall rule you need in the list of firewall rules, go to the Advanced -> Firewall page and create a new firewall rule.

Schedule: Select a schedule for when the service will be enabled. If you do not see the schedule you need in the list of schedules, go to the Advanced -> Schedules screen and create a new schedule.



Applications

Enabled/ Disabled: Each list entry can be active or inactive, according to this selection.

Name: Assign a meaningful name to the Application, for example Web Server.

Clear: Clicking this button erases edits you have made to all items in the add/edit area of the screen.

Trigger Port: Enter the outgoing port or range of ports used by your application. [6500-6700]

Trigger Type: Select the outbound protocol used by your application. [Both]

Public Port: Enter the port or range of ports that you want to open up to Internet traffic. [6000-6200]

Public Type: Select the protocol used by the Internet traffic coming back into the router through the opened port range. [Both]

Port Forwarding

Enabled/ Disabled: Each list entry can be active or inactive, according to this selection.

Name: Assign a meaningful name to the Application, for example Web Server.

Clear: Clicking this button erases edits you have made to all items in the add/edit area of the screen.

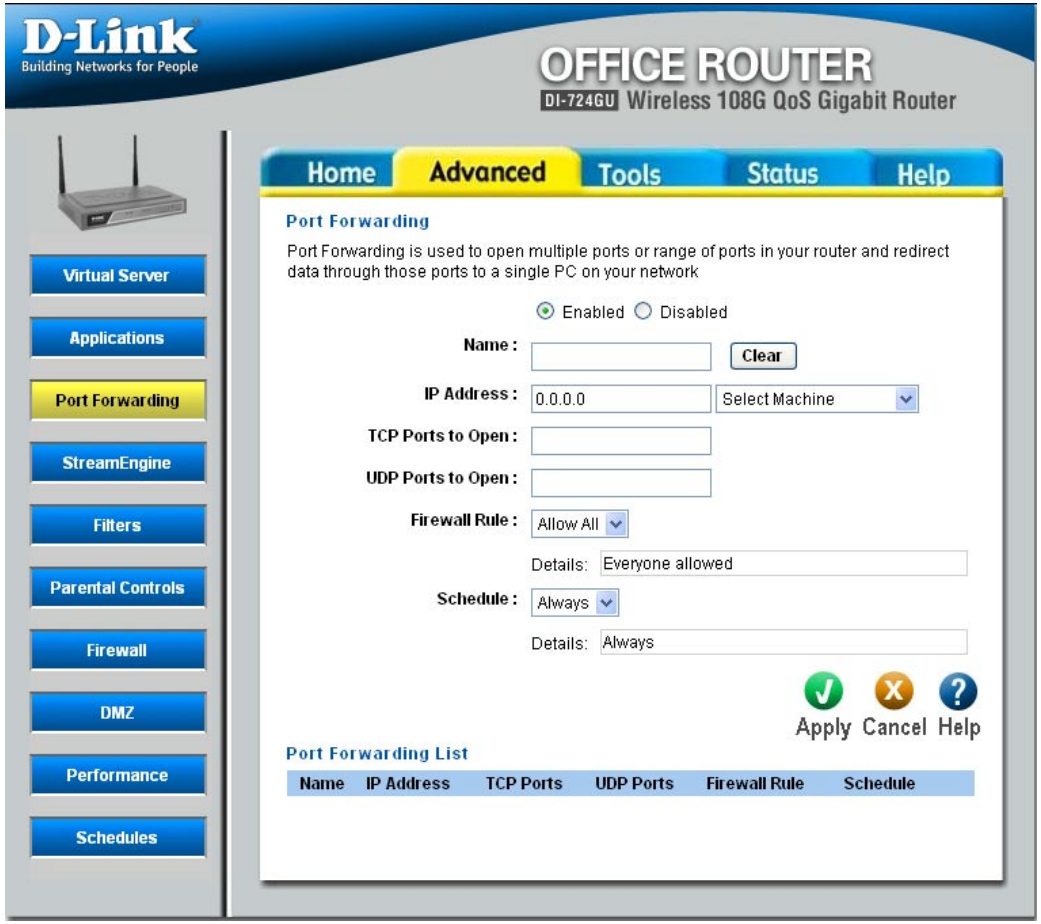
IP Address: Enter the local network IP address of the system hosting the game server, for example 192.168.0.50.

TCP Ports to Open: Enter the TCP ports to open. [6159-6180, 99]

UDP Ports to Open: Enter the UDP ports to open. [6159-6180, 99]

Firewall Rule: Select a firewall rule that controls access as needed for this port forwarding rule. If you do not see the firewall rule you need in the list of firewall rules, go to the Advanced -> Firewall page and create a new firewall rule.

Schedule: Select a schedule for the times when this rule is in effect. If you do not see the schedule you need in the list of schedules, go to the Advanced -> Schedules screen and create a new schedule.



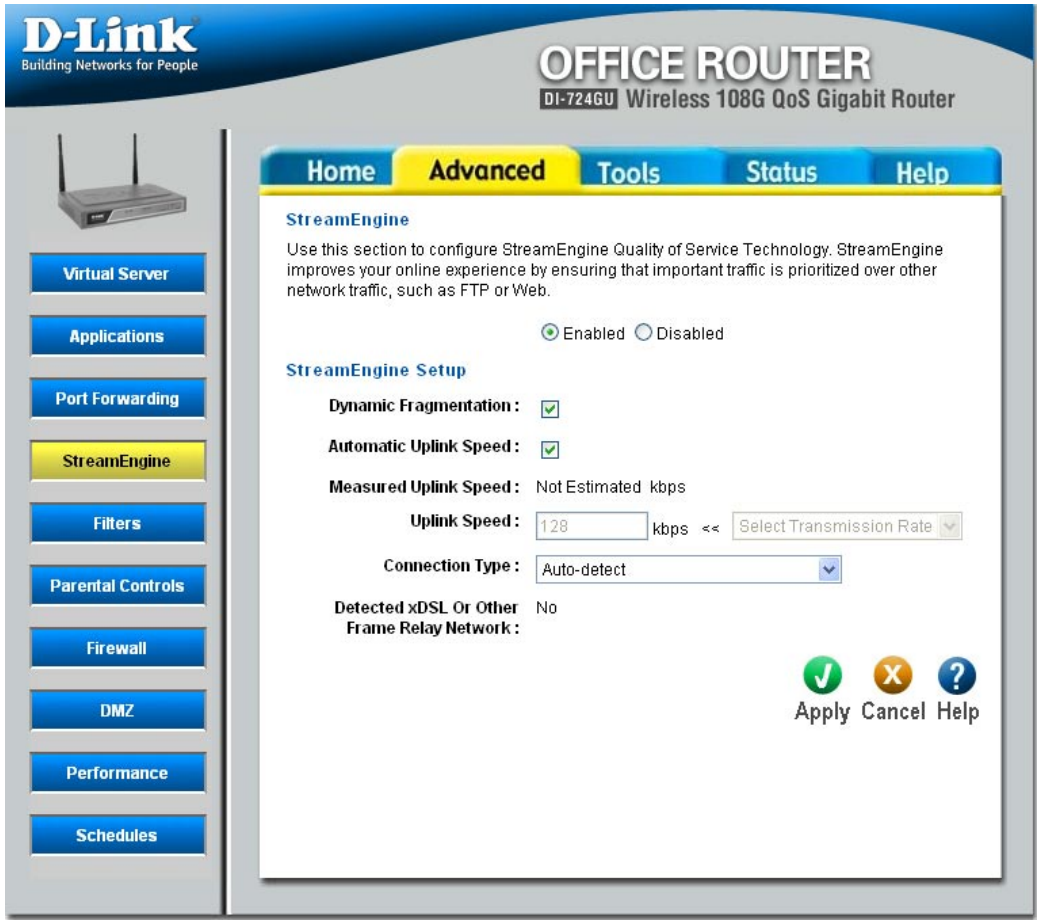
StreamEngine

Enabled/ Disabled: The StreamEngine option is disabled by default. Enable it for better performance and experience with online games and other interactive applications, such as VoIP.

Dynamic Fragmentation: This option should be enabled when you have a slow Internet uplink. It helps to reduce the impact that large low priority network packets can have on more urgent ones by breaking the large packets into several smaller packets.

Automatic Uplink Speed: When enabled, this option causes the router to automatically measure the useful uplink bandwidth each time the WAN interface is re-established (after a reboot, for example).

Measured Uplink Speed: This is the uplink speed measured when the WAN interface was last re-established. The value may be lower than that reported by your ISP as it does not include all of the network protocol overheads associated with your ISP's network. Typically, this figure will be between 87% and 91% of the stated uplink speed for xDSL connections and around 5 kbps lower for cable network connections.



Uplink Speed: If Automatic Uplink Speed is disabled, this options allows you to set the uplink speed manually. Uplink speed is the speed at which data can be transferred from the router to your ISP. This is determined by your ISP. ISPs often specify speed as a downlink/uplink pair; for example, 1.5Mbps/284kbps. For this example, you would enter "284". Alternatively you can test your uplink speed with a service such as http://www.dslreports.com/. Note however that sites such as DSL Reports, because they do not consider as many network protocol overheads, will generally note speeds slightly lower than the Measured Uplink Speed or the ISP rated speed.

Connection Type: By default, the router automatically determines whether the underlying connection is an xDSL/Frame-relay network or some other connection type (such as cable modem or Ethernet), and it displays the result as Detected xDSL or Frame Relay Network. If you have an unusual network connection in which you are actually connected via xDSL but for which you configure either “Static” or “DHCP” in the WAN settings, setting this option to xDSL or Other Frame Relay Network ensures that the router will recognize that it needs to shape traffic slightly differently in order to give the best performance. Choosing xDSL or Other Frame Relay Network causes the measured uplink speed to be reported slightly lower than before on such connections, but gives much better results.

Detected xDSL or Other Frame Relay Network : When Connection Type is set to Auto-detect, the automatically detected connection type is displayed here.

Filters

IP Filters

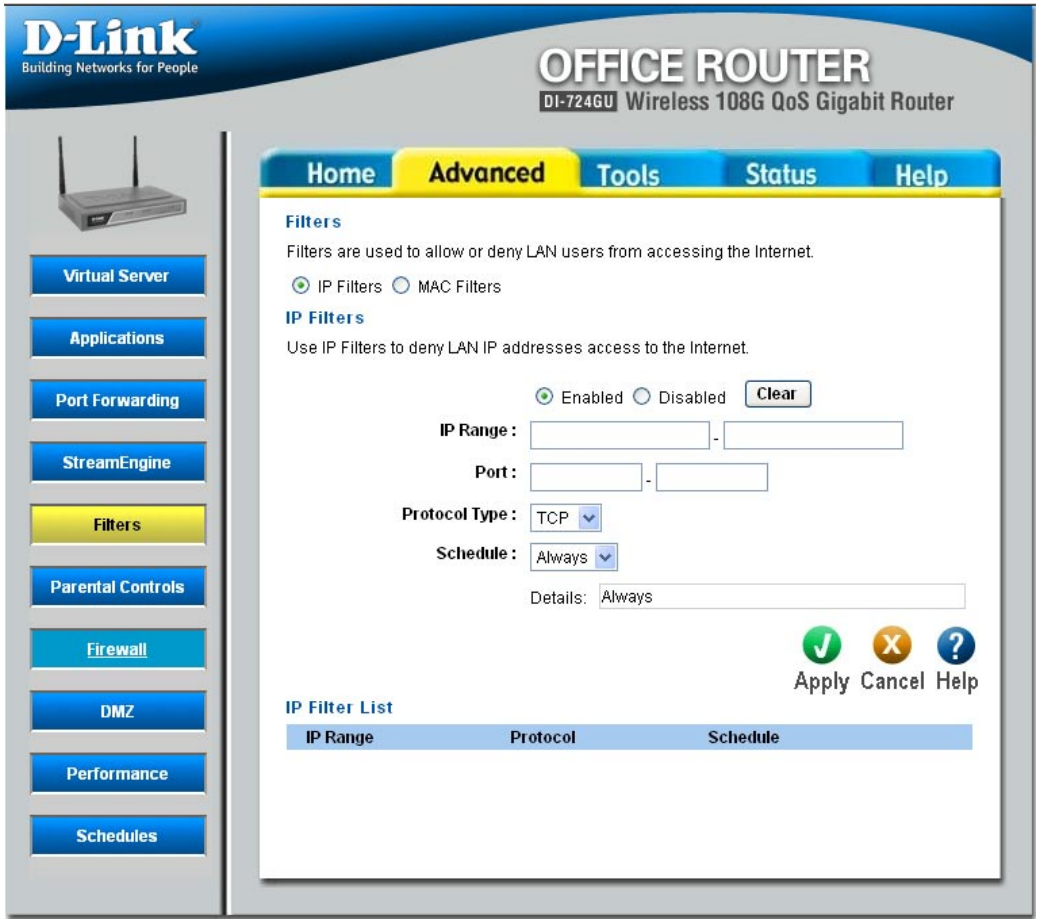
Enabled/ Disabled: Each list entry can be active or inactive, according to this selection.

Clear: Clicking this button erases edits you have made to all items in the add/edit area of the screen.

IP Range: Enter the range of IP addresses of the LAN machines that you want the access control rule to apply to. To specify a single IP address, enter the address in both the starting and ending address boxes. Make sure that the device on the LAN either has a static IP address (that is, one that is not in the DHCP range) or is in the DHCP Reservations List (see Home -> DHCP).

Port: The range of ports that will be denied access to the Internet. Enter both starting and ending port numbers. To specify a single port, enter the port number in both the starting and ending boxes.

Protocol Type: The type of packets that will be blocked from reaching the Internet. You can block UDP packets, TCP packets, or both.



Schedule: Select a schedule for the times when you want the filter to apply. If you do not see the schedule you need in the list of schedules, go to the Advanced -> Schedules screen and create a new schedule.

IP Filter List: This section shows the current IP Filter rules. Rules can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the “IP Filters” section is activated for editing.

MAC Filters

Disabled MAC Filters: With this selection you can disable all the filters in the MAC Filter List.

Only allow computers with MAC address listed below to access the network: Select this option if you want only selected computers to have network access, and you want all other computers not to have network access.

Note: *Misconfiguration of this feature can prevent any machine from accessing the network. In such a situation, you can regain access by activating the factory defaults button on the router itself.*

Only deny computers with MAC address listed below to access the network: Select this option if you want all computers to have network access except those computers in the list.

MAC Filters

Only allow computers with MAC address listed below to access the network

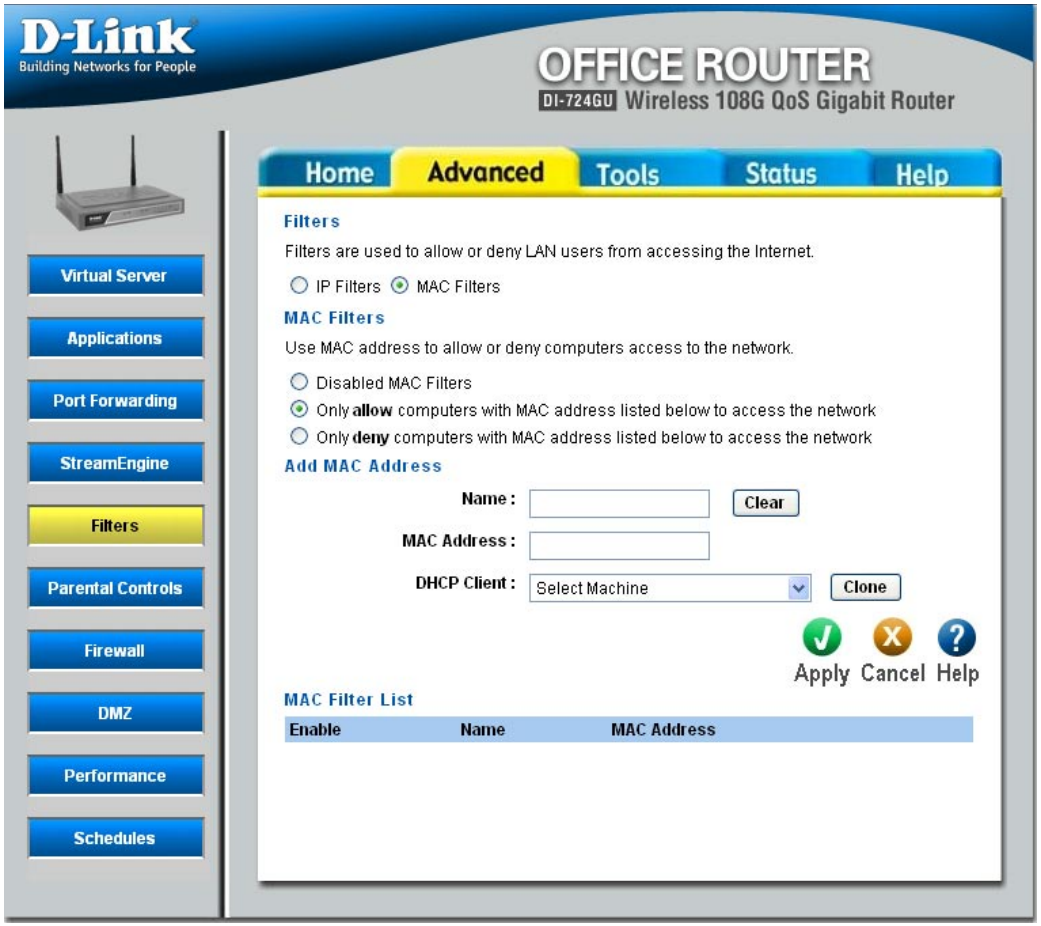
Only deny computers with MAC address listed below to access the network

Name: Create a name for this filter that is meaningful to you. Typically this would be a computer name or user name; for example “Casey’s Laptop”.

Clear: Clicking this button erases edits you have made to all items in the add/edit area of the screen.

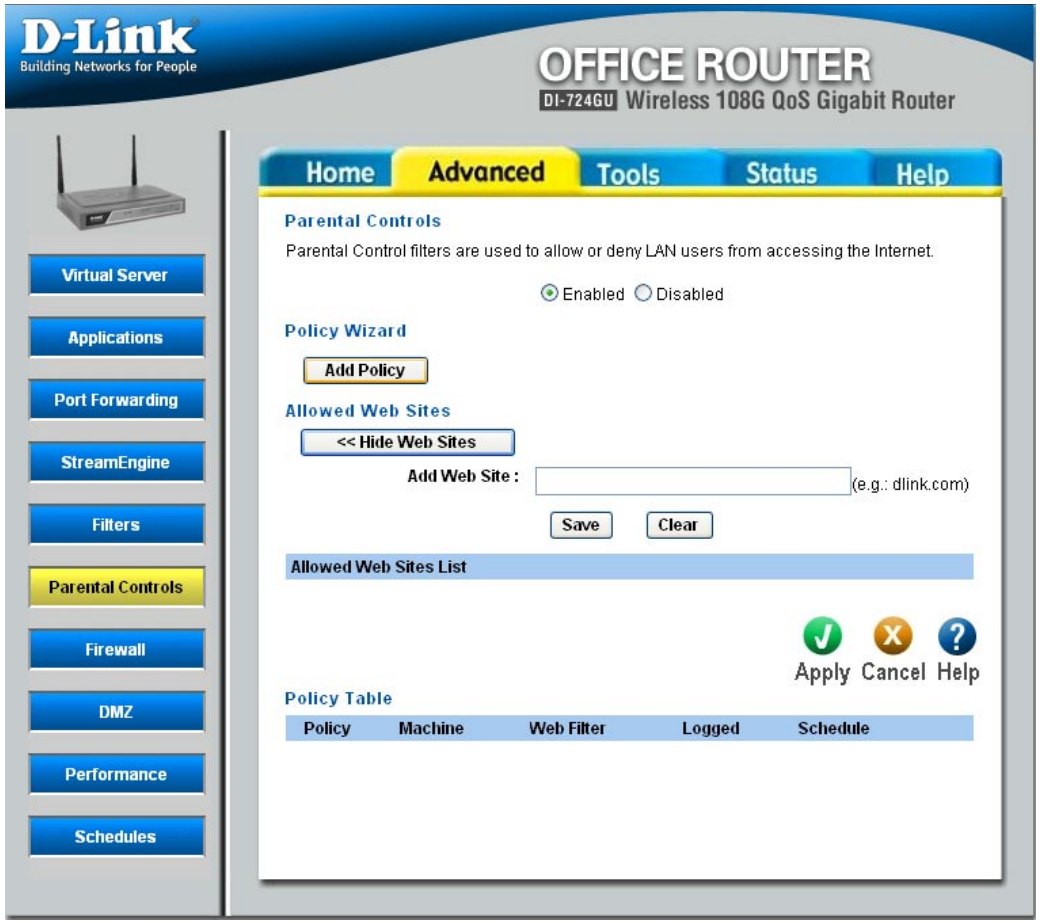
MAC Address: Enter the MAC address of the desired computer. You can type the MAC address manually in this box, or retrieve a MAC address automatically by using the DHCP Client control below.

DHCP Client: All currently connected LAN devices under DHCP will be listed here by their current IP address. Select the computer whose access you want to control from the “DHCP Client” list. Then click the **Clone** button to capture its MAC address in the MAC Address box above.



Parental Control

Enabled/ Disabled: If you want to control access from specific LAN computers to specific Web sites, enable this option. When this option is enabled, the following sections are visible. The page has several work areas, each of when can be hidden when not in use: a list of web sites, a list of control policies, and the Policy Wizard -- a sequence of steps that guide you through the creation and modification of policies.



Add Policy: Click this button to start creating a new parental controls policy.

DHCP Client: When the Allowed Web Sites List is displayed, you can click here to hide it.

Enter the domain name of a web site to which you want to allow access; for example: google.com. Do not enter the http:// preceding the URL. Enter the most inclusive domain; for example, enter dlink.com and access will be permitted to both www.dlink.com and support.dlink.com.

Note: *Many web sites construct pages with images and content from other web sites. Access will be forbidden if you do not enable all the web sites used to construct a page. For example, to access my.yahoo.com, you need to enable access to yahoo.com, yimg.com, and doubleclick.net.*

Save: Clicking the **Save** button saves the new or edited entry in the following list.

Clear: Clicking this button erases edits you have made to the “Add Web Site” text.

Firewall

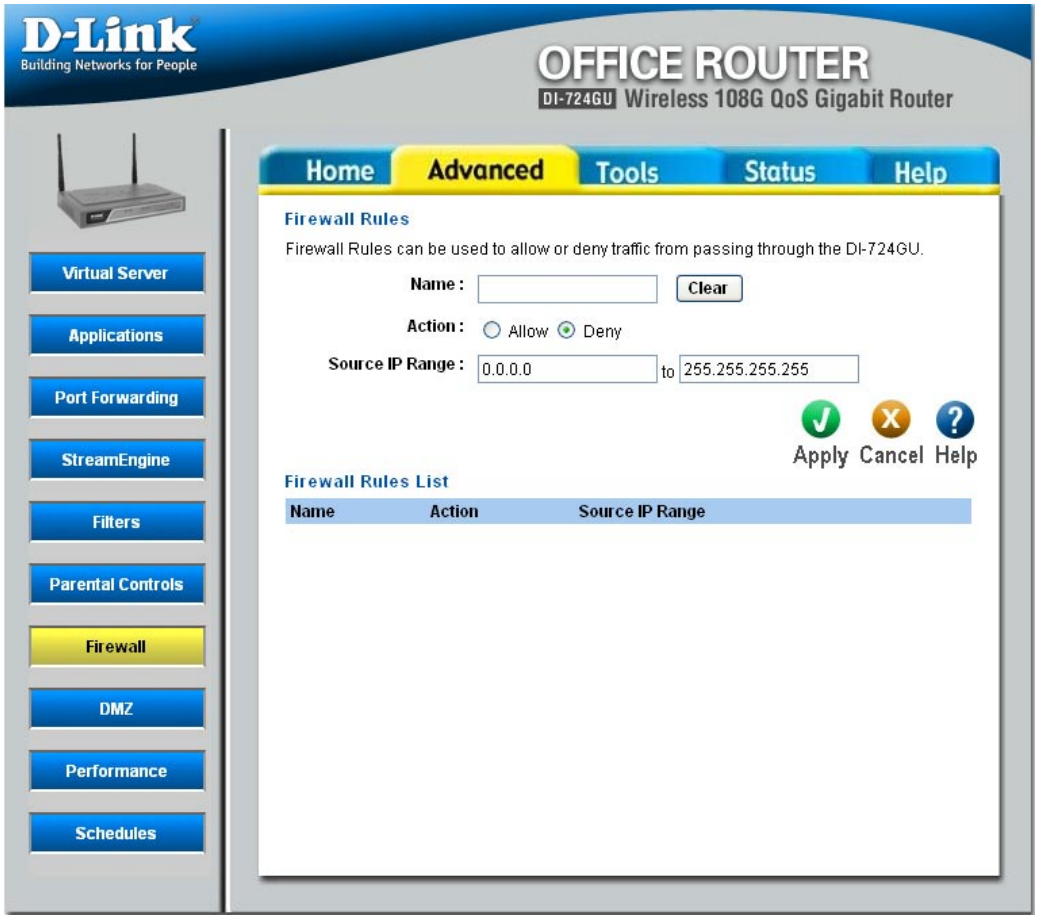
Name: Enter a name for the rule that is meaningful to you.

Clear: Clicking this button erases edits you have made to all items in the add/edit area of the screen.

Action: The rule can either Allow or Deny messages.

Source IP Range: Define the range of Internet addresses this rule applies to.

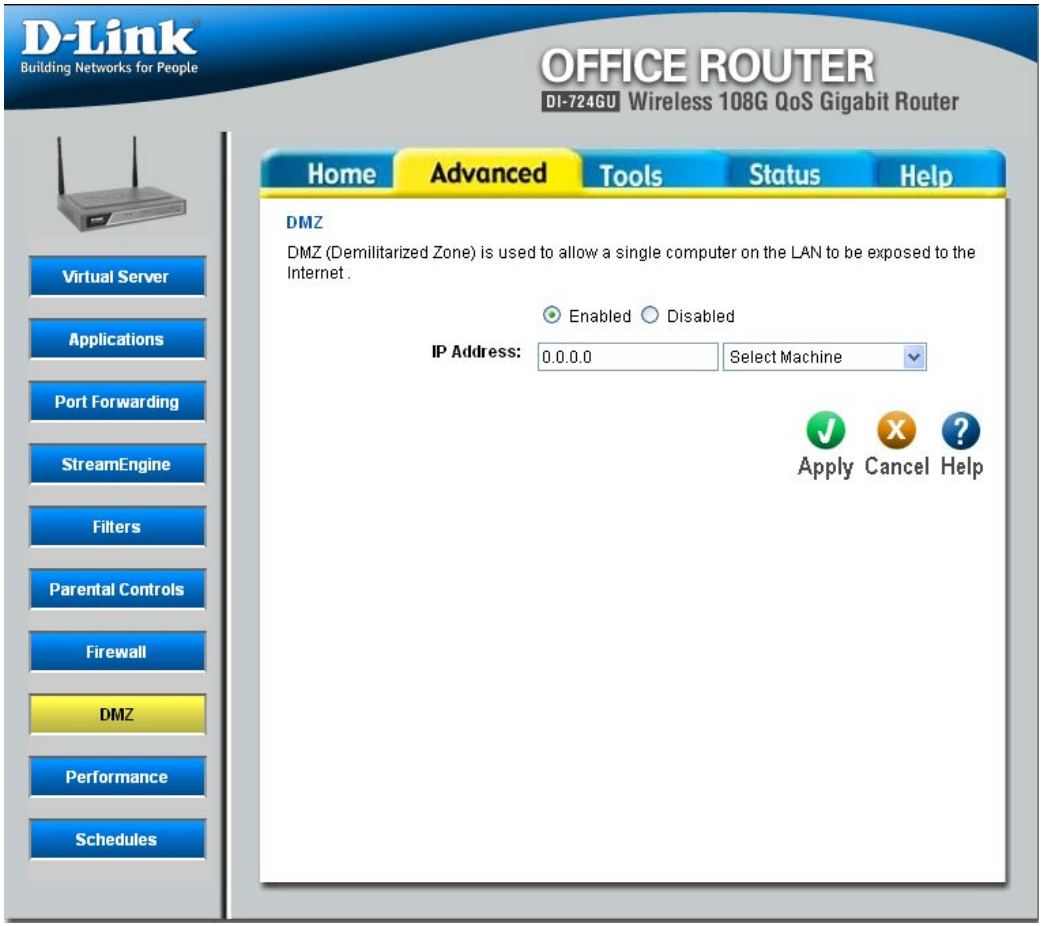
Firewall Rules List: The section lists the defined Firewall Rules. A Firewall Rule can be changed by clicking the Edit icon, or deleted by clicking the Delete icon. When you click the Edit icon, the item is highlighted, and the “Firewall Rules” section is activated for editing.



DMZ

Enabled/ Disabled: The DMZ capability can be active or inactive, according to this selection.

IP Address: Specify the IP address of the computer on the LAN that you want to have unrestricted Internet communication. If this computer obtains its address Automatically using DHCP, then you may want to make a DHCP reservation on the Home -> DHCP page, so that the IP address of the DMZ machine does not change.



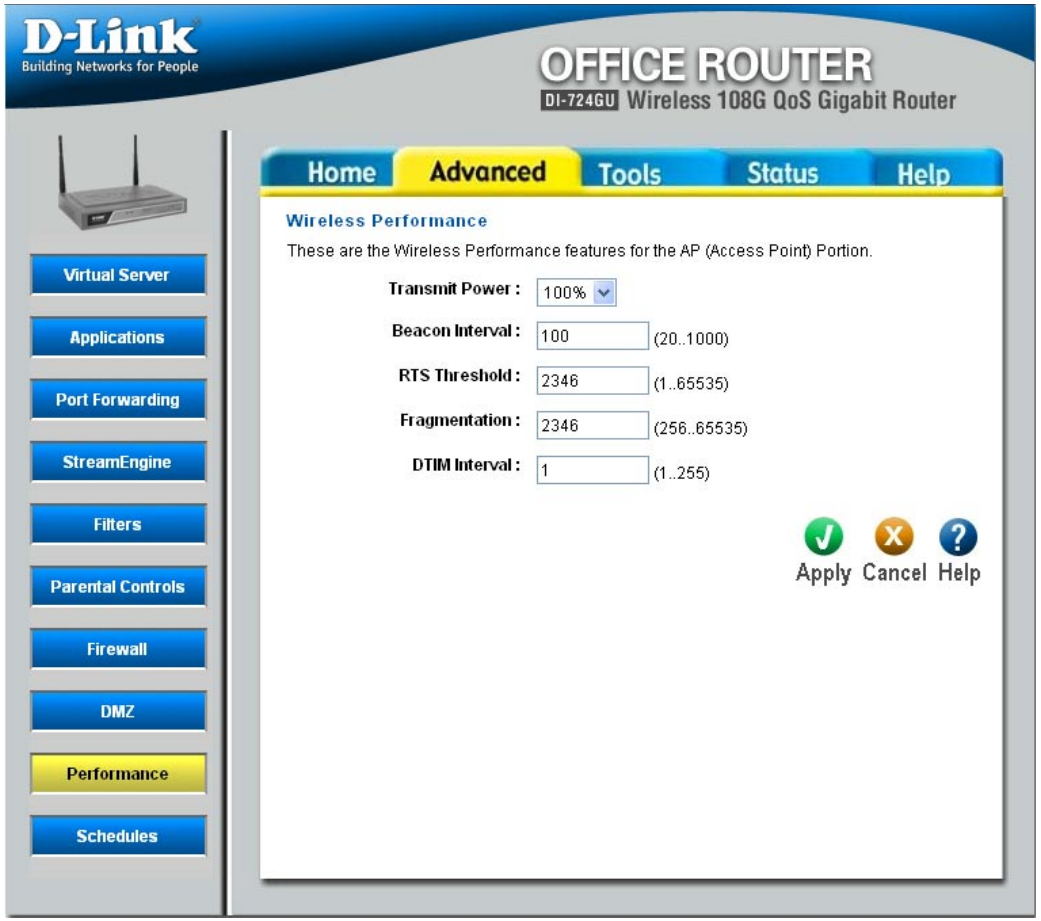
Performance

Transmit Power: Normally the wireless transmitter operates at 100% power. In some circumstances, however, there might be a need to isolate specific frequencies to a smaller area. By reducing the power of the radio, you can prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

Beacon Interval: Beacons are packets sent by a wireless router to synchronize wireless devices. Specify a Beacon Interval value between 20 and 1000 milliseconds. The default value is 100 milliseconds.

RTS Threshold: This setting should remain at its default value of 2346. If you encounter inconsistent data flow, only minor modifications to the value are recommended.

Fragmentation: This setting should remain at its default value of 2346. Setting the Fragmentation value too low may result in poor performance.



DTIM Interval: A DTIM is a countdown for informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Wireless clients detect the beacons and awaken to receive the broadcast and multicast messages. The default value is 1. Valid settings are between 1 and 255.

Schedules

Name: Give the schedule a name that is meaningful to you, such as “Weekday rule”.

Clear: Clicking this button erases edits you have made to all items in the add/edit area of the screen.

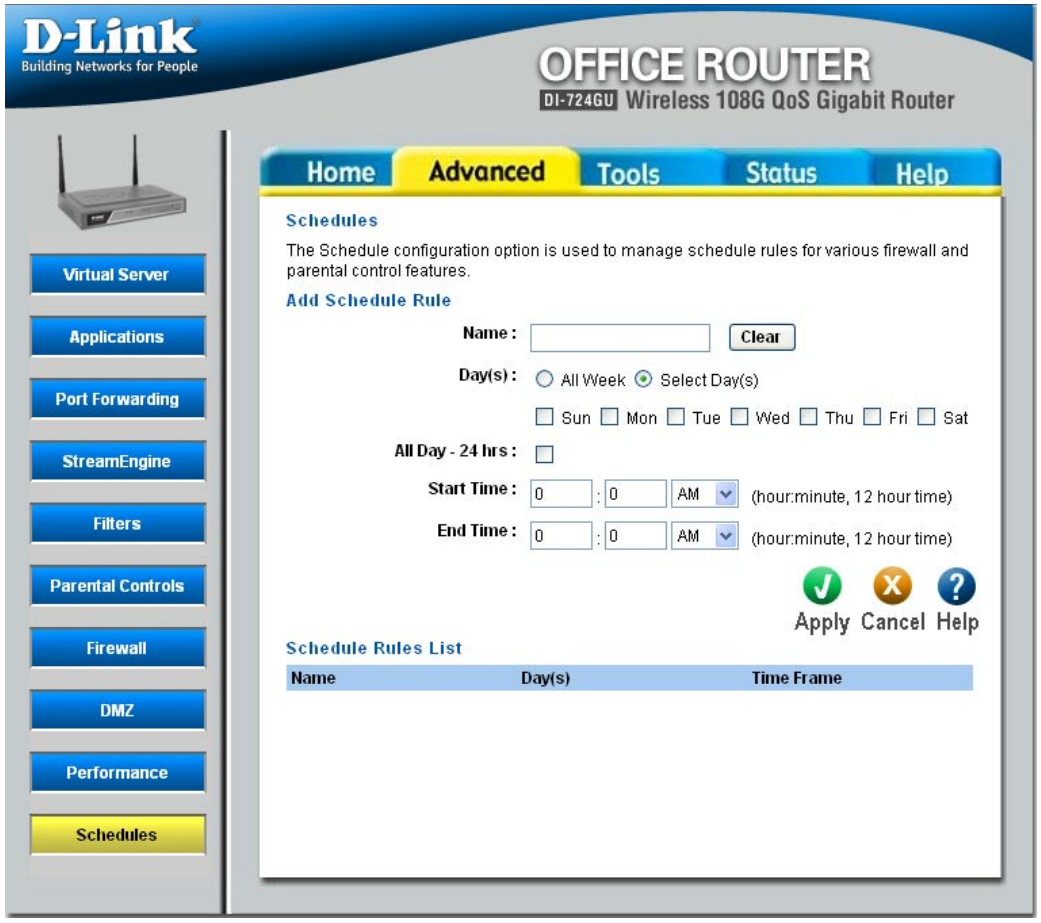
Day(s): Place a checkmark in the boxes for the desired days, or select the All Week radio button to schedule all seven days of the week.

All Day - 24hrs:

Select this option if you want this schedule in effect all day for the selected day(s).

Start Time:

If you don’t use the All Day option, then you enter the time here. The start time is entered in two fields. The first box is for the hour and the second box is for the minute. Email events are normally triggered only by the start time.



End Time:

The end time is entered in the same format as the start time. The hour in the first box and the minutes in the second box. The end time is used for most other rules, but is not normally used for email events.

Tools

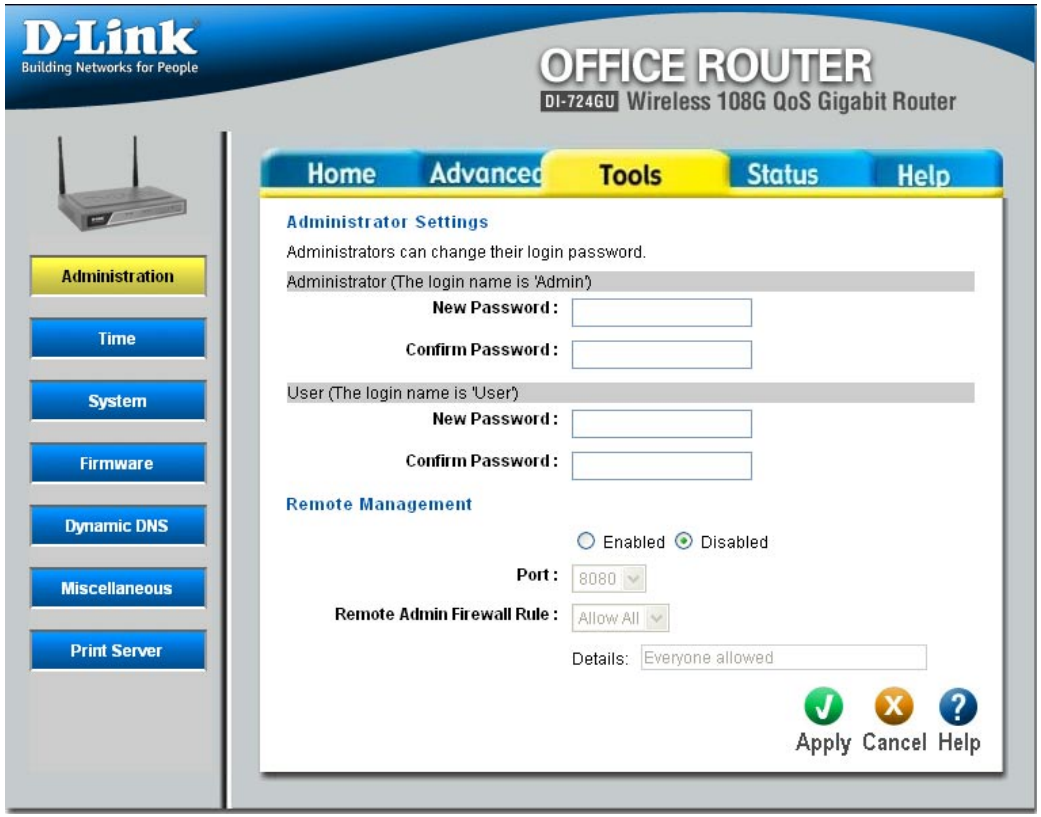
Administration

Administrator: Enter a password for the user “Admin”, who will have full access to the Web-based management interface.

User: Enter a password for the user “User”, who will have read-only access to the Web-based management interface.

Remote Management: Enabling Remote Management allows you to manage the router from anywhere on the Internet. Disabling Remote Management allows you to manage the router only from computers on your LAN.

Port: The port that you will use to address the management interface from the Internet. For example, if you choose port 1080 here, then, to access the router from the Internet, you would use a URL of the form: http://my.domain.com:1080/.



Remote Admin Firewall Rule: Select a firewall rule that controls access as needed for this admin port. If you do not see the firewall rule you need in the list of firewall rules, go to the Advanced -> Firewall page and create a new firewall rule.

Time

Device Time: The time currently maintained by the router.

Automatic:

Select this option if you want the router's clock synchronized to a Network Time Server over the Internet. If you are using schedules or logs, this is the best way to ensure that the schedules and logs are kept accurate.

NTP Server:

Select a Network Time Server for synchronization. You can type in the address of a time server. If your ISP offers a Network Time Server, that is the best choice. If there is no nearby Network Time Server, enter a public time server such as pool.ntp.org.

Interval:

The router always fetches the time when it is switched on and also updates its time periodically by sending a query to the configured Network Time Server. Here you can select how often you want the router to update its time from the Network Time Server. To avoid overloading Network Time Servers, do not specify an interval smaller than necessary to maintain accurate time.

Manual:

If you do not have the NTP Server option in effect, you can either manually set the time for your router here, or you can click the **Copy** button to copy the time from the computer you are using. (Make sure that computer's time is set correctly.)

Note: *If the router loses power for any reason, it cannot keep its clock running, and will not have the correct time when it is started again. To maintain correct time for schedules and logs, either you must enter the correct time after you restart the router, or you must enable the NTP Server option.*

Time Zone: Select your time zone from the pull-down menu.

Daylight Saving: Enable this option if daylight saving time is observed in your location. The router will automatically update the hour on the start and end dates specified below.

Start/End: Select the starting and ending weeks for the change to and from daylight saving time. For example, suppose for the start you select Month="Oct" and Week="3rd". This is the same as saying: "Daylight saving starts on the third Sunday of October."

System

Save Settings To Local Hard Drive: Use this option to save the current router configuration settings to a file on the hard disk of the computer you are using. First, click the **Save** button. You will then see a file dialog, where you can select a location and file name for the settings.

Load Settings From Local Hard Drive: Use this option to load previously saved router configuration settings. First, use the **Browse** control to find a previously save file of configuration settings. Then, click the **Load** button to transfer those settings to the router.

Restore to Factory Defaults: This option will restore all configuration settings back to the settings that were in effect at the time the router was shipped from the factory. Any settings that have not been saved will be lost, including any rules that you have created. If you want to save the current router configuration settings, use the **Save** button above.

DDNS

Enabled/ Disabled: Enable this option only if you have purchased your own domain name and registered with a dynamic DNS service provider. The following parameters are active when the option is enabled.

Server Address: Select a dynamic DNS service provider from the pull-down list.

Host Name: Enter your host name, fully qualified; for example: myhost.mydomain.net.

Username or Key: Enter the username or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Password or Key: Enter the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Verify Password or Key: Re-type the password or key provided by your service provider. If the Dynamic DNS provider supplies only a key, enter that key in all three fields.

Note: *If a dynamic DNS update fails for any reason (for example, when incorrect parameters are entered), the router automatically disables the Dynamic DNS feature and records the failure in the log.*

Note: *After configuring the router for dynamic DNS, you can open a browser and navigate to the URL for your domain (for example http://www.mydomain.info) and the router will attempt to forward the request to port 80 on your LAN. If, however, you do this from a LAN-side computer and there is no virtual server defined for port 80, the router will return the router's configuration home page. Refer to the Advanced -> Virtual Server configuration page to set up a virtual server.*

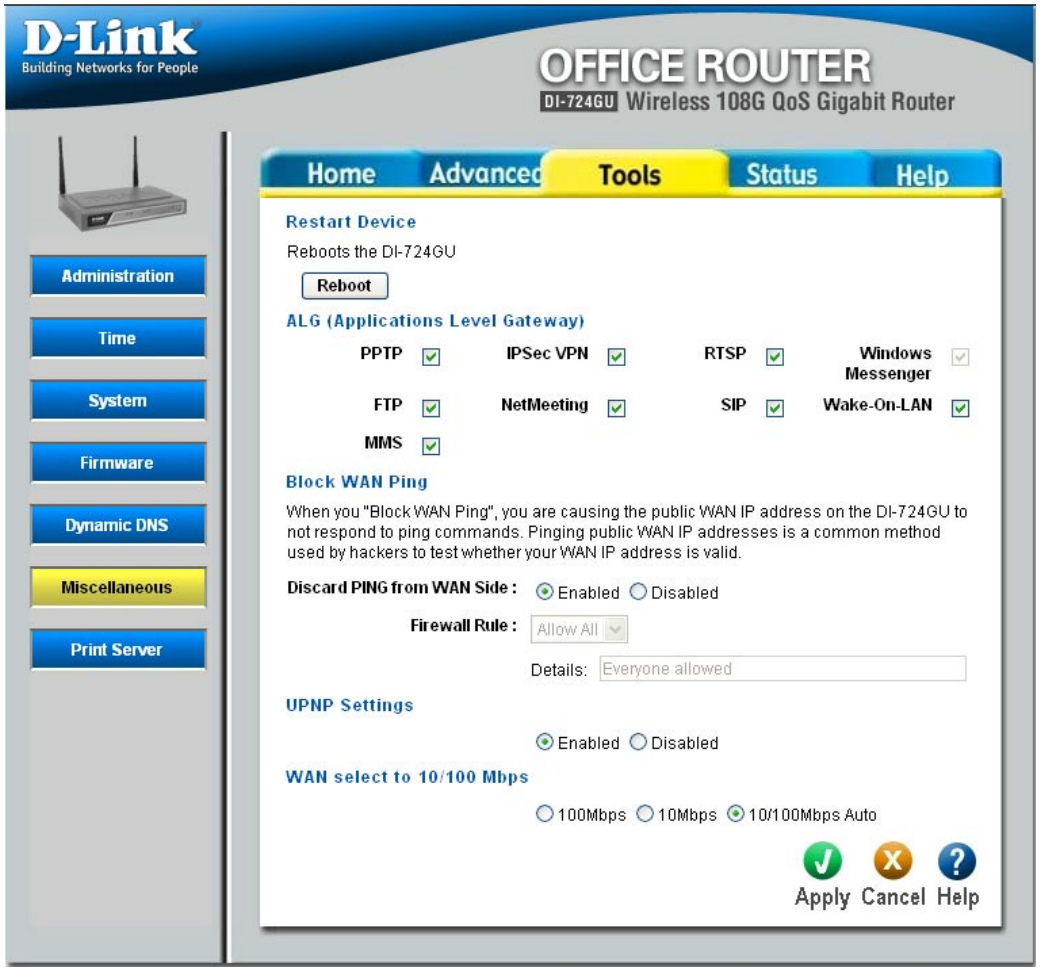
Miscellaneous

Restart Device: Clicking the **Reboot** button will restart the router. This is useful for restarting when you are not near the router.

Discard Ping from WAN Side: If you enable this option, you are causing the router not to respond to ping commands to the public WAN IP address of the router. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

Firewall Rule: Select a firewall rule that controls access as needed for ping commands. If you do not see the firewall rule you need in the list of firewall rules, go to the Advanced -> Firewall page and create a new firewall rule.

UPnP: UPnP is short for Universal Plug and Play, which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. This router has optional UPnP capability, and can work with other UPnP devices and software. If you do need to use the UPnP functionality, you can enable it here.



Gaming Mode: If you are experiencing difficulties when playing online games or even certain applications that use voice data, you may need to enable Gaming Mode for these applications to work correctly. When not playing games or using these voice applications, it is recommended that Gaming Mode be disabled.

Multiple VPN Pass-Through using ALG: When the VPN ALG is enabled, LAN computers can establish VPN connections either with the same or with different VPN servers. When the VPN ALG is disabled, the ALG does not function; however, the router allows VPN operation in a restricted way. When the VPN ALG is disabled, LAN computers are typically able to establish VPN tunnels to different VPN Internet servers but not to the same server. The advantage of disabling the ALG is to increase VPN performance (the ALG does not "get in the way" of the communication). Enabling a VPN ALG also allows incoming VPN connections (refer to Virtual Services) to a LAN side VPN server.

Note: *The L2TP VPN connections typically use IPSec to secure the connection. To achieve multiple VPN pass-through in this case, the IPSec ALG must be enabled.*

WAN Speed Select: Normally, this is set to "auto". If you have trouble connecting to the WAN, try the other settings.

Print Server

Raw Port Printing: Causes the router to support TCP raw (also known as Port 9100). Printers are identified by port numbers (9100 being the customary starting port number). This option must be enabled for the Print Wizard to function.

LPD/LPR Printing: Causes the router to support the LPD/LPR protocol. Printers are identified by a symbolic queue name. This option is disabled by default; enable it if required by the devices on the LAN. This method of printing is generally preferred for Unix or Macintosh (starting with Mac OS 8.1).

Status

Device Info

All of your Internet and network connection details are displayed on the Device Information page. This is primarily a recap of all the WAN, LAN, Wireless, and DHCP options that are set from the Home tab. The firmware version is also displayed here.

Note: *Some browsers have limitations that make it impossible to update the WAN status display when the status changes. Some browsers require that you refresh the display to obtain updated status. Some browsers report an error condition when trying to obtain WAN status.*

DHCP Connection: Clicking the **DHCP Release** button unassigns the router's IP address. The router will not respond to IP messages from the WAN side until you click the **DHCP Renew** button or power-up the router again. Clicking the **DHCP Renew** button causes the router to request a new IP address from the ISP's server.

PPPoE, PPTP, L2TP Connection: Depending on whether the WAN connection is currently established, you can click either the **Connect** button to attempt to establish the WAN connection or the **Disconnect** button to break the WAN connection.

BigPond Connection: Depending on whether you are currently logged in to BigPond, you can click either the **BigPond Login** button to attempt to establish the WAN connection or the **BigPond Logout** button to break the WAN connection.

LAN Computers: This area of the screen continually updates to show all DHCP enabled computers and devices connected to the LAN side of your router. The detection "range" is limited to the address range as configured in DHCP Server. Computers that have an address outside of this range will not show. If the DHCP Client (i.e. a computer configured to "Automatically obtain an

address") supplies a Host Name, that will also be shown. Any computer or device that has a static IP address that lies within the detection "range" may show; however, its host name will not.

IGMP Multicast memberships: If IGMP is enabled, this area of the screen show all multicast groups of which any LAN devices are members.

Routing Table: The routing section displays all of the routing details configured for your router.

A value of 0.0.0.0 for gateway means there is no next hop, and the IP address is directly connected to the router on the interface specified: LAN or WAN. A value of 0.0.0.0 in both the destination IP and netmask means that this is the default route.

Log

What to View: Select the kinds of events that you want to view between **Firewall and Security**, **System**, and **Router Status**.

Logging Levels: Select the level of events that you want to view between **Critical**, **Warning**, and **Informational**

SMTP Server Address: Enter the SMTP server address for sending email.

Account Name: Enter your account for sending email.

Password: Enter the password associated with the account.

Verify Password: Re-type the password associated with the account.

To Email address: Enter the email address where you want the email sent.

On Log Full: Select this option if you want logs to be sent by email when the log is full.

On Schedule: Select this option if you want logs to be sent by email according to a schedule.

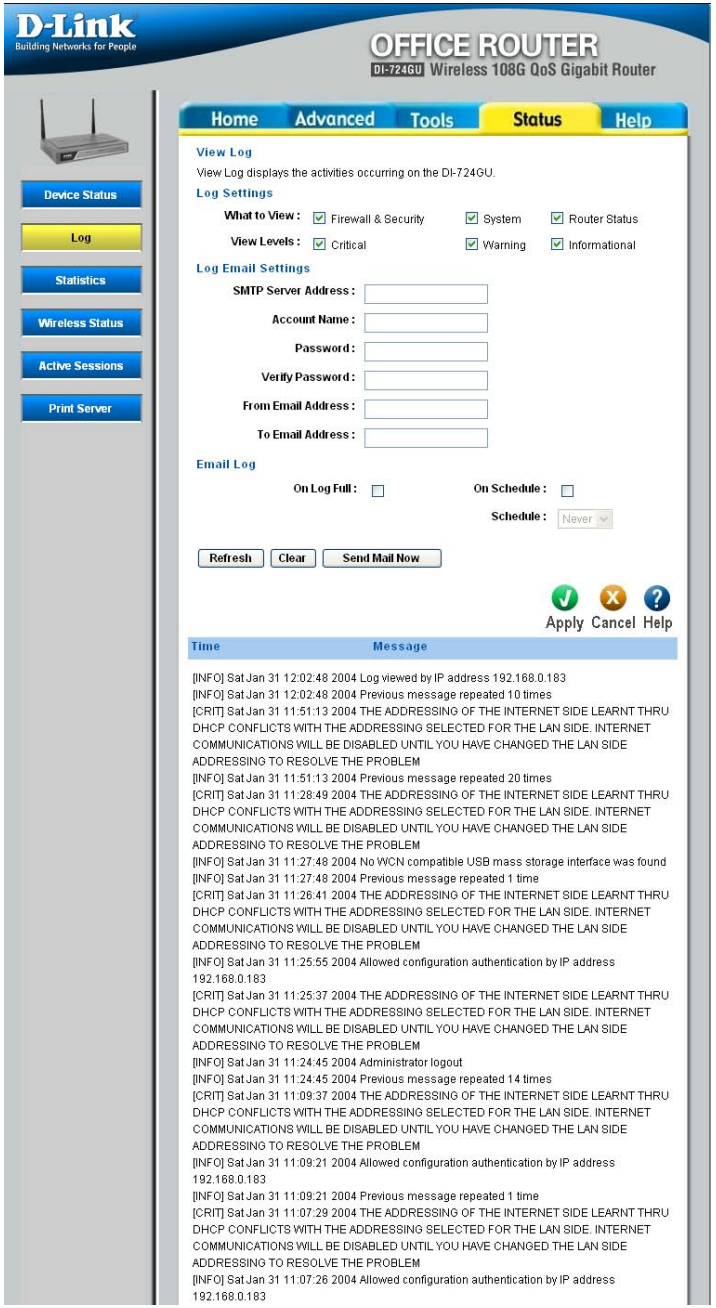
Schedule: If you selected the On Schedule option, select one of the defined schedule rules. If you do not see the schedule you need in the list of schedules, go to the Advanced -> Schedules screen and create a new schedule.

Note: *Email is sent at the start time defined for a schedule; the schedule end time is not used for email.*

Refresh: Clicking this button refreshes the display of log entries. There may be new events since the last time you accessed the log.

Clear: Clicking this button empties the log by erasing all log entries.

Send Mail Now: If you provided email information with the Tools -> Miscellaneous screen, clicking the **Send Mail Now** button sends the router log to the configured email address.



Statistics

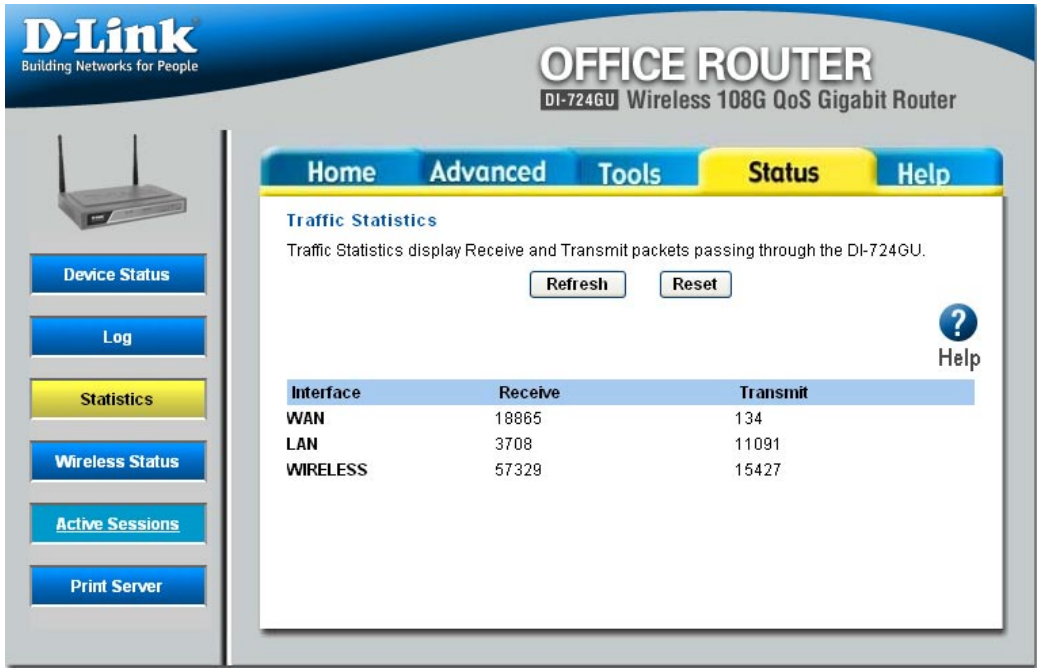
The Statistics page displays all of the LAN, WAN, and Wireless packet transmit and receive statistics.

The Statistics page displays all of the LAN and WAN packet transmit and receive statistics.

Clicking the **Refresh** button updates the display by retrieving the latest packet tallies from the router. Clicking the **Reset** button restarts the packet tallies from zero.

Receive: The number of packets received by the router.

Transmit: The number of packets sent from the router.



Wireless Status

The wireless section allows you to view information about the wireless clients that are connected to your wireless router.

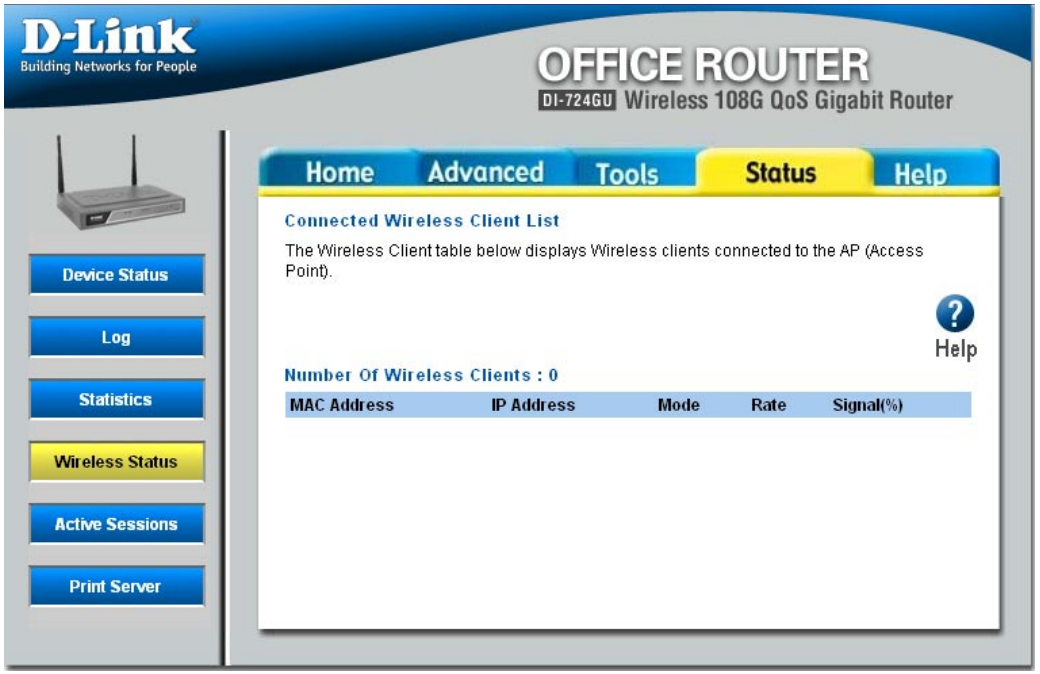
MAC Address: The Ethernet ID (MAC address) of the wireless client.

IP Address: The LAN-side IP address of the client.

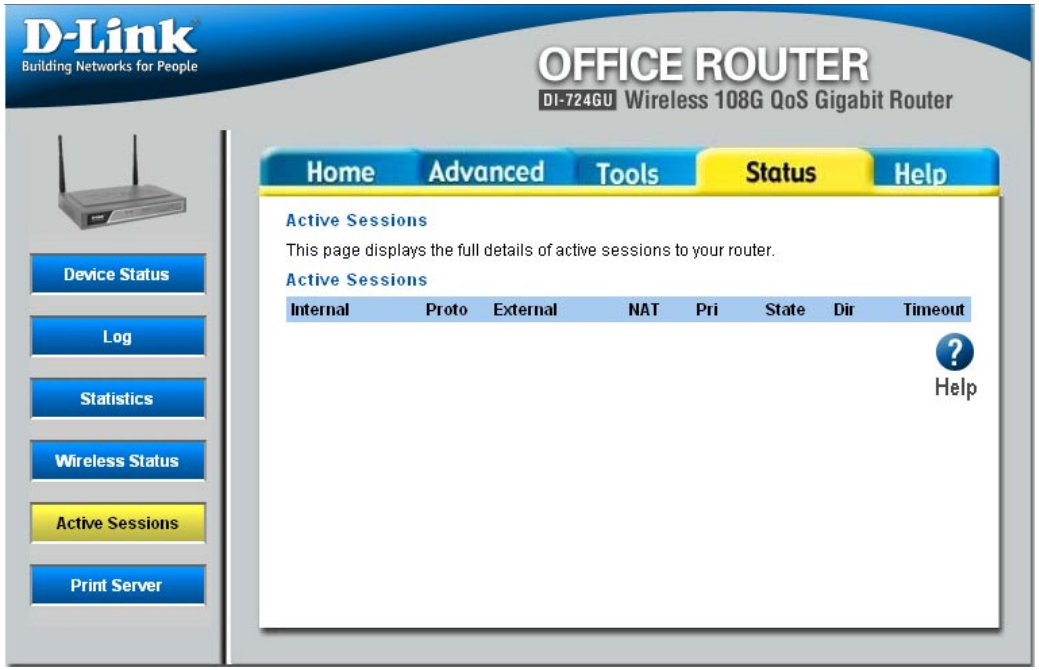
Mode: The transmission standard being used by the client. Values are 11b, or 11g for 802.11b, or 802.11g respectively.

Rate: The actual transmission rate of the client in megabits per second.

Signal: This is a relative measure of signal quality. The value is expressed as a percentage of theoretical best quality. Signal quality can be reduced by distance, by interference from other radio-frequency sources (such as cordless telephones or neighboring wireless networks), and by obstacles between the router and the wireless device.



Active Sessions



Internal: The IP address and port number of the LAN-side application.

Protocol: The communications protocol used for the conversation.

External: The IP address and port number of the WAN-side application.

NAT: The port number of the LAN-side application as viewed by the WAN-side application.

Priority: The preference given to outbound packets of this conversation by the GameFuel logic. Smaller numbers represent higher priority.

State: When SPI (Stateful Packet Inspection) is enabled, this is the state for sessions that use the TCP protocol.

Dir: The direction of initiation of the conversation:
Egress: Initiated from LAN to WAN.
Ingress: Initiated from WAN to LAN.

Time Out: The number of seconds of idle time until the router considers the session terminated.

Print Server

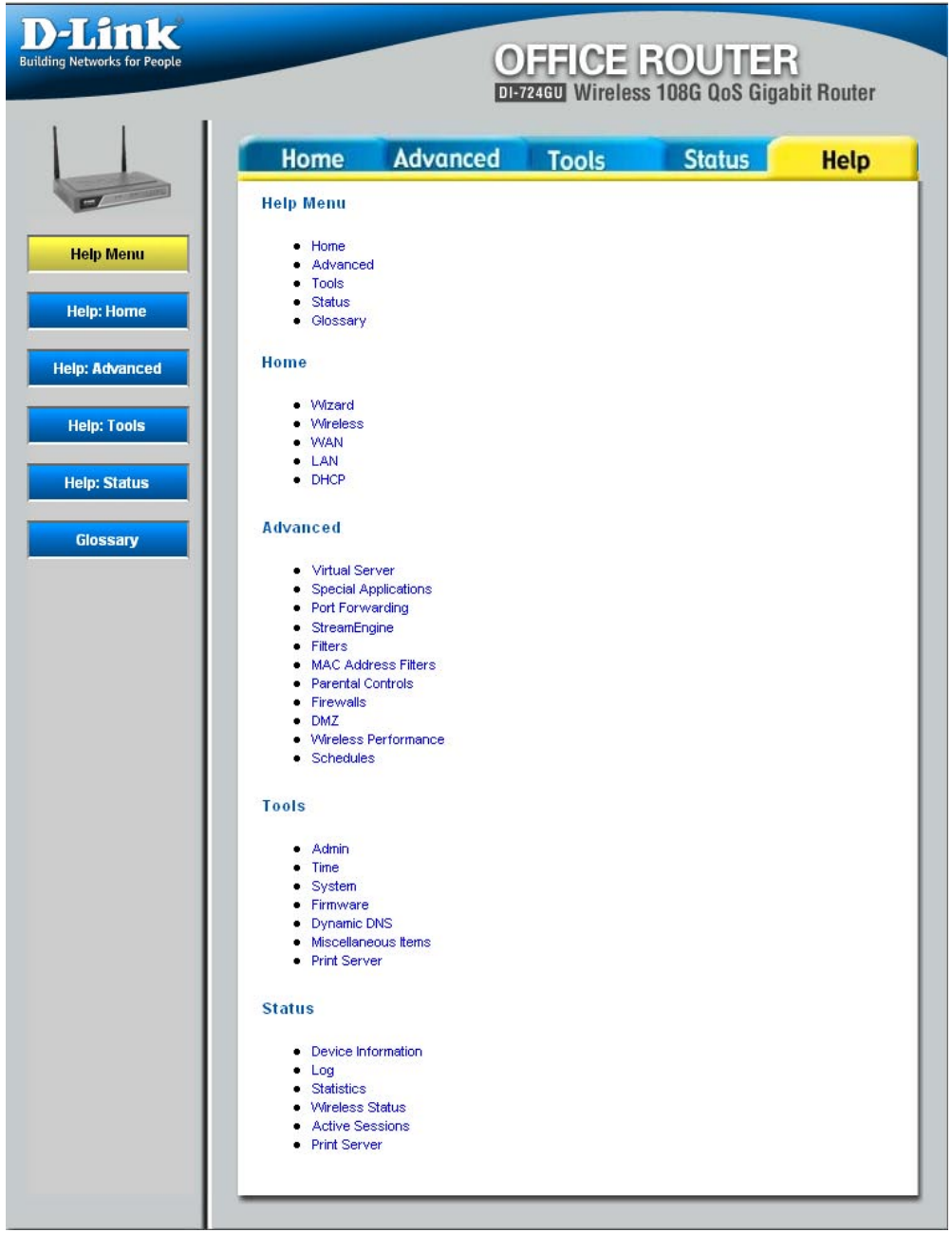
Printer Status: Shows the status of the printer attached to the router.

Note: *Certain printers (for example, the HP Business Inkjet 2300 printer) do not report status to the router; therefore, such a printer always shows a status of "Offline".*

Raw TCP Port Printing: Shows the "IP Address" and "TCP Port" values that you need to enter when you configure your computer to use the printer in TCP Raw mode.

LPD/LPR Printing: Shows the "IP Address" and "Queue Name" values that you need to enter when you configure your computer to use the printer in LPR/LPD mode.

Help


D-Link
Building Networks for People
OFFICE ROUTER
DI-724GU Wireless 108G QoS Gigabit Router
Home
Advanced
Tools
Status
Help
Help Menu
Help: Home
Help: Advanced
Help: Tools
Help: Status
Glossary
Help Menu
Home
Advanced
Tools
Status
Glossary
Home
Wizard
Wireless
WAN
LAN
DHCP
Advanced
Virtual Server
Special Applications
Port Forwarding
StreamEngine
Filters
MAC Address Filters
Parental Controls
Firewalls
DMZ
Wireless Performance
Schedules
Tools
Admin
Time
System
Firmware
Dynamic DNS
Miscellaneous Items
Print Server
Status
Device Information
Log
Statistics
Wireless Status
Active Sessions
Print Server

Troubleshooting

1 What variables may cause my wireless products to lose reception?

D-Link products let you access your network from virtually anywhere you want. However, the positioning of the products within your environment will affect the wireless range. Please refer to Installation Considerations in the Wireless Basics section of this manual for further information about the most advantageous placement of your D-Link wireless products.

2. Why does my wireless connection keep dropping?

Antenna Orientation- Try different antenna orientations for the DI-724GU. Try to keep the antenna at least 6 inches away from the wall or other objects.

If you are using 2.4GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, and lights, your wireless connection will degrade dramatically or drop altogether. Try changing the Channel on your Router, Access Point and Wireless adapter to a different Channel to avoid interference.

Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, Monitors, electric motors, etc.

3. Why can't I get a wireless connection?

If you have enabled Encryption on the DI-724GU, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- For 802.11b, the Encryption settings are: 64 or 128 bit. Make sure that the encryption bit level is the same on the Router and the Wireless Client.
- Make sure that the SSID on the Router and the Wireless Client are exactly the same. If they are not, wireless connection will not be established.
- Move the DI-724GU and the wireless client into the same room and then test the wireless connection.
- Disable all security settings. (WEP, MAC Address Control)
- Turn off your DI-724GU and the client. Turn the DI-724GU back on again, and then turn on the client.

- Make sure that all devices are set to Infrastructure mode.
- Check that the LED indicators are indicating normal activity. If not, check that the AC power and Ethernet cables are firmly connected.
- Check that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, and lights, your wireless connection will degrade dramatically or drop altogether. Try changing the Channel on your DI-724GU, and on all the devices in your network to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, Monitors, electric motors, etc.

4. What do I do if I forgot my encryption key.?

Reset the DI-724GU to its factory default settings and restore the other devices on your network to their default settings. You may do this by pressing the **Reset** button on the back of the unit. You will lose the current configuration settings.

5. Resetting the DI-724GU to Factory Default Settings?

The InternetAfter you have tried other methods for troubleshooting your network, you may choose to Reset the DI-724GU to the factory default settings. Remember that D-Link Wireless 108G products network together, out of the box, at the factory default settings.

- To hard-reset the DI-724GU to Factory Default Settings, please do the following:
- Locate the **Reset** button on the back of the DI-724GU.
- Use a paper clip to press the **Reset** button.
- Hold for about 10 seconds and then release.
- After the DI-724GU reboots (this may take a few minutes) it will reset to the factory Default settings.

Wireless Basics

D-Link wireless products are based on industry standards to provide easy-to-use and compatible high-speed wireless connectivity within your home, business or public access wireless networks. Strictly adhering to the IEEE standard, the D-Link wireless family of products will allow you to securely access the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking delivers.

A wireless local area network (WLAN) is a cellular computer network that transmits and receives data with radio signals instead of wires. Wireless LANs are used increasingly in both home and office environments, and public areas such as airports, coffee shops and universities. Innovative ways to utilize WLAN technology are helping people to work and communicate more efficiently. Increased mobility and the absence of cabling and other fixed infrastructure have proven to be beneficial for many users.

Under many circumstances, it may be desirable for mobile network devices to link to a conventional Ethernet LAN in order to use servers, printers or an Internet connection supplied through the wired LAN. A Wireless Router is a device used to provide this link.

What is Wireless?

Wireless or WiFi technology is another way of connecting your computer to the network without using wires. WiFi uses radio frequency to connect wirelessly, so you have the freedom to connect computers anywhere in your home or office network.

Why D-Link Wireless?

D-Link is the worldwide leader and award winning designer, developer, and manufacturer of networking products. D-Link delivers the performance you need at a price you can afford. D-Link has all the products you need to build your network.

How does wireless work?

Wireless works similar to how cordless phone work, through radio signals to transmit data from one point A to point B. But wireless technology has restrictions as to how you can access the network. You must be within the wireless network range area to be able to connect your computer. There are two different types of wireless networks Wireless Local Area Network (WLAN), and Wireless Personal Area Network (WPAN).

Wireless Local Area Network (WLAN)

In a wireless local area network, a device called an Access Point (AP) connects computers to the network. The access point has a small antenna attached to it, which allows it to transmit data back and forth over radio signals. With an indoor access point as seen in the picture, the signal can travel up to 300 feet. With an outdoor access point the signal can reach out up to 30 miles to serve places like manufacturing plants, industrial locations, college and high school campuses, airports, golf courses, and many other outdoor venues.

Who uses wireless?

Wireless technology as become so popular in recent years that almost everyone is using it, whether it's for home, office, business, D-Link has a wireless solution for it.

Home

- Gives everyone at home broadband access
- Surf the web, check email, instant message, and etc
- Gets rid of the cables around the house
- Simple and easy to use

Small Office and Home Office

- Stay on top of everything at home as you would at office
- Remotely access your office network from home
- Share Internet connection and printer with multiple computers
- No need to dedicate office space

Where is wireless used?

Wireless technology is expanding everywhere not just at home or office. People like the freedom of mobility and it's becoming so popular that more and more public facilities now provide wireless access to attract people. The wireless connection in public places is usually called "hotspots".

Using a D-Link Cardbus Adapter with your laptop, you can access the hotspot to connect to Internet from remote locations like: Airports, Hotels, Coffee Shops, Libraries, Restaurants, and Convention Centers.

Wireless network is easy to setup, but if you're installing it for the first time it could be quite a task not knowing where to start. That's why we've put together a few setup steps and tips to help you through the process of setting up a wireless network.

Tips

Here are a few things to keep in mind, when you install a wireless network.

Centralize your router or Access Point

Make sure you place the router/access point in a centralized location within your network for the best performance. Try to place the router/access point as high as possible in the room, so the signal gets dispersed throughout your home. If you have a two-story home, you may need a repeater to boost the signal to extend the range.

Eliminate Interference

Place home appliances such as cordless telephones, microwaves, and televisions as away as possible from the router/access point. This would significantly reduce any interfere that the appliances might cause since they operate on same frequency.

Security

Don't let you next-door neighbors or intruders connect to your wireless network. Secure your wireless network by turning on the WPA or WEP security feature on the router. Refer to product manual for detail information on how to set it up.

Wireless Modes

There are basically two modes of networking:

- **Infrastructure** – All wireless clients will connect to an access point or wireless router.

- **Ad-Hoc** – Directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DI-724GU wireless network Cardbus adapters.

An Infrastructure network contains an Access Point or wireless router. All the wireless devices, or clients, will connect to the wireless router or access point.

An Ad-Hoc network contains only clients, such as laptops with wireless cardbus adapters. All the adapters must be in Ad-Hoc mode to communicate.

Networking Basics

Check your IP Address

After you install your new D-Link adapter, by default, the TCP/IP settings should be set to obtain an IP address from a DHCP server (i.e. wireless router) automatically. To verify your IP address, please follow the steps below.

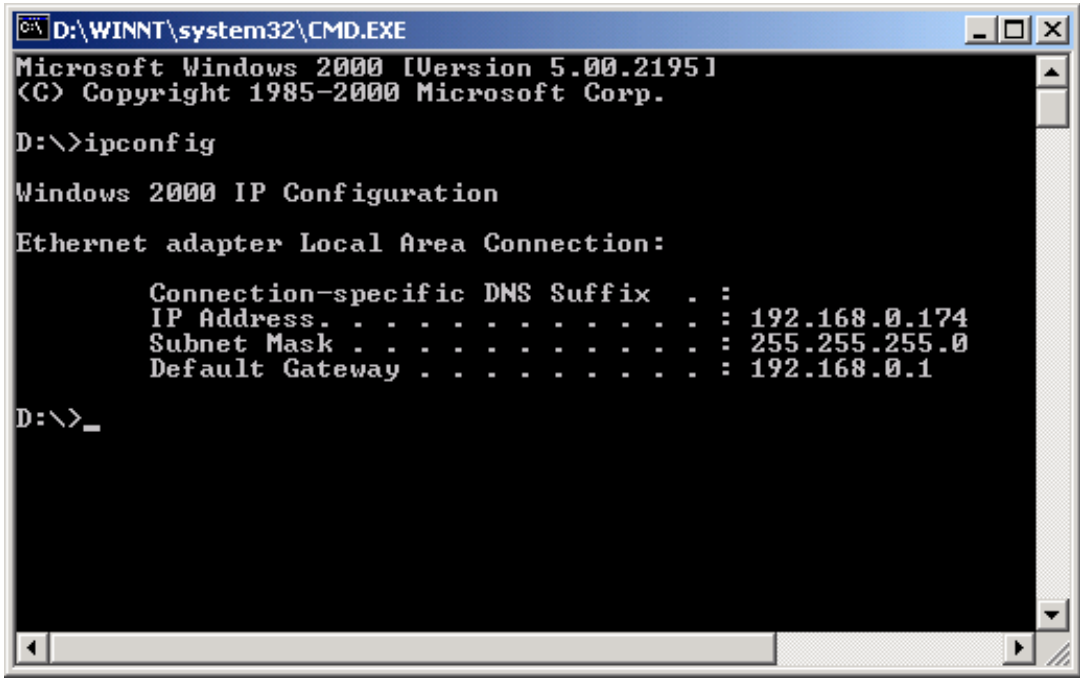
Click on **Start** > **Run**. In the run box type ***cmd*** and click **OK**.

At the prompt, type ***ipconfig*** and press **Enter**.

This will display the IP address, subnet mask, and the default gateway of your adapter.

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your router. Some firewall software programs may block a DHCP request on newly installed adapters.

If you are connecting to a wireless network at a hotspot (e.g. hotel, coffee shop, airport), please contact an employee or administrator to verify their wireless network settings.



Statically Assign an IP Address

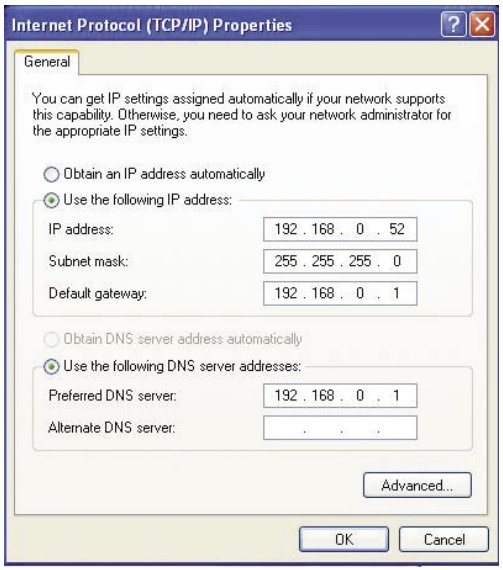
If you are not using a DHCP capable gateway/router, or you need to assign a static IP address, please follow the steps below:

Step 1
Windows® XP - Click on **Start** > **Control Panel** > **Network Connections**.
Windows® 2000 - From the desktop, right-click **My Network Places** > **Properties**.

Step 2
Right-click on the **Local Area Connection** which represents your D-Link network adapter and select **Properties**.

Step 3
Highlight **Internet Protocol (TCP/IP)** and click **Properties**.

Step 4
Click **Use the following IP address** and enter an IP address that is on the same subnet as your network or the LAN IP address on your router.



Example: If the router´s LAN IP address is 192.168.0.1, make your IP address 192.168.0.X where X is a number between 2 and 99. Make sure that the number you choose is not in use on the network. Set Default Gateway the same as the LAN IP address of your router (192.168.0.1).

Set Primary DNS the same as the LAN IP address of your router (192.168.0.1). The Secondary DNS is not needed or you may enter a DNS server from your ISP.

Step 5
Click OK twice to save your settings.

Technical Specifications

Standards

- IEEE 802.11g
- IEEE 802.11b
- IEEE 802.3
- IEEE 802.3b

VPN Pass Through/Multi-Sessions

- PPTP
- L2TP
- BigPond
- IPSec

Device Management

- Internet Explorer v6 or later
- Netscape® Navigator v7 or later
- Other Java-enabled browsers
- DHCP Server and Client

Advanced Firewall Features

- NAT with VPN Passthrough (Network Address Translation)
- MAC Filtering
- URL Filtering
- Scheduling

Wireless Operating Range

- Indoors - up to 328 feet (100 meters)
- Outdoors - up to 1312 feet (400 meters)

Operating Temperature

- 32°F to 131°F (0°C to 55°C)

Humidity

- 95% maximum (non-condensing)

Safety and Emissions

- FCC

Wireless Frequency Range

- 2.4GHz to 2.462GHz

Viewing System Requirement Protocol

ActiveX

Operating System

- Microsoft Windows® XP/2000

Browser

Internet Explorer v6

LEDs

Two-Color LED

Power

- External Power Supply
- 5V DC 3A

Dimensions

4.5” (L) x 3.125” (W) x 1.625” (H)

Warranty

1-Year

Maximum wireless signal rate derived from IEEE Standard 802.11g specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate. Environmental factors will adversely affect wireless signal range.

Technical Support

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

If you require product support, we encourage you to browse our FAQ section on the Web Site before contacting the Support line. We have many FAQ's which we hope will provide you a speedy resolution for your problem.

For Customers within The United Kingdom & Ireland:

D-Link UK & Ireland Technical Support over the Internet:

http://www.dlink.co.uk
ftp://ftp.dlink.co.uk

D-Link UK & Ireland Technical Support over the Telephone:

08456 12 0003 (United Kingdom)
+1890 886 899 (Ireland)
Lines Open
8.00am-10.00pm Mon-Fri
10.00am-7.00pm Sat & Sun

For Customers within Canada:

D-Link Canada Technical Support over the Telephone:

1-800-361-5265 (Canada)
Mon. to Fri. 7:30AM to 9:00PM EST

D-Link Canada Technical Support over the Internet:

http://support.dlink.ca
email: support@dlink.ca

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com