D-Link
DI-624S

High-Speed 2.4 GHz
Wireless Storage Router

Manual

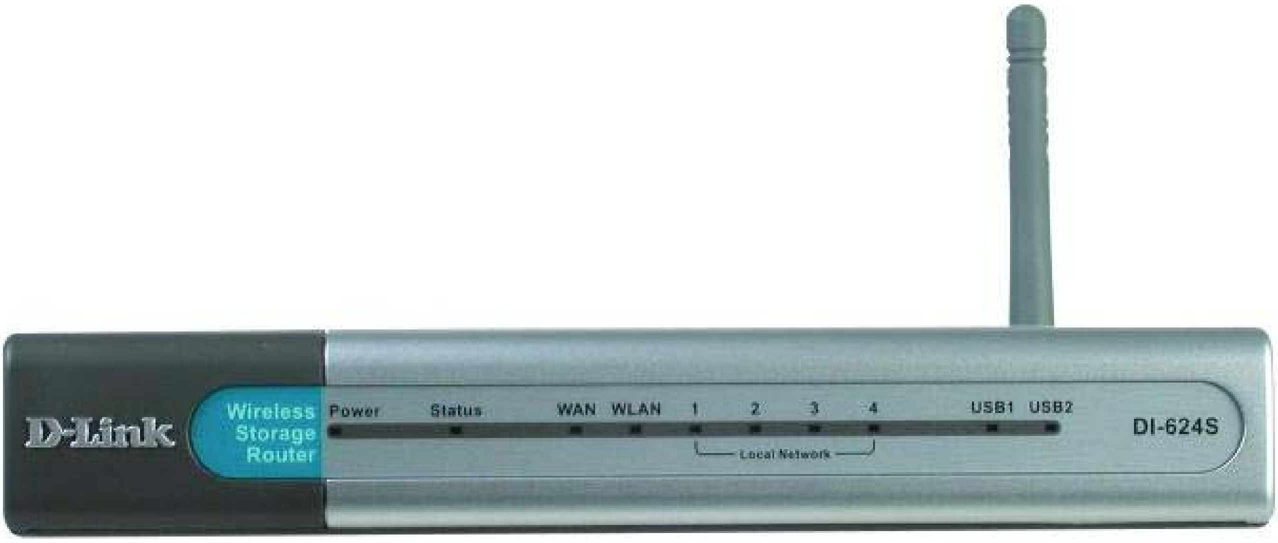
D-Link®

Building Networks for People

Ver 1.00

Contents

Package Contents



Contents of Package:

- D-Link DI-624S 2.4GHz Wireless Storage Router
- Power Adapter-DC 5V, 3A
- Manual and Warranty on CD
- Quick Installation Guide
- Ethernet Cable (All the DI-624S's Ethernet ports are Auto-MDIX)

Note: Using a power supply with a different voltage rating than the one included with the DI-624S will cause damage and void the warranty for this product.

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

- System Requirements for Configuration
- Ethernet-Based Cable or DSL Modem
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Computers with Windows, Macintosh, or Linux-based operating systems with an installed Ethernet adapter
- Internet Explorer Version 6.0 or Netscape Navigator Version 7.0 and Above

Introduction

The D-Link DI-624S Wireless Storage Router is an 802.11b/g high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places.

Unlike most routers, the DI-624S provides data transfers at up to 8X (compared to the standard 11 Mbps) when used with other D-Link 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-624S has the newest, strongest, most advanced security features available today. When used with other 802.11g WPA or WPA2 (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.)

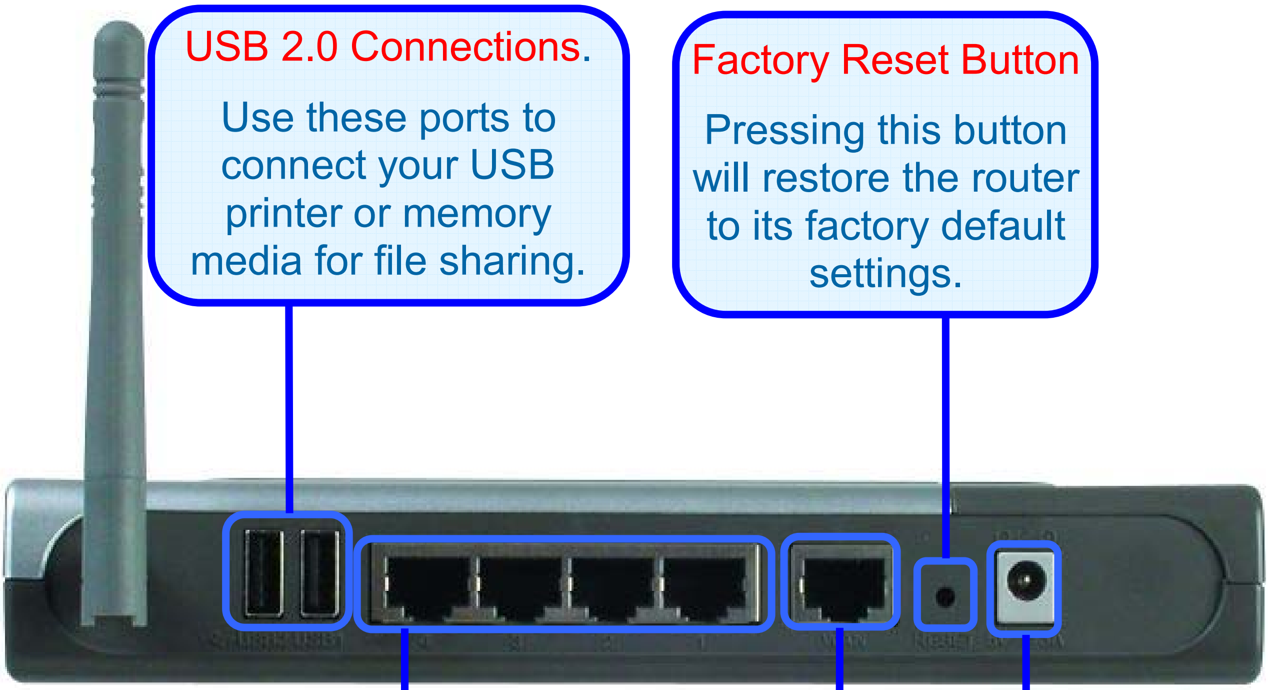
WPA2, based on the IEEE 802.1i Wi-Fi certified standard, goes a level beyond the previous WPA by enhancing security with a new encryption code. Employing AES (Advanced Encryption Standard), and yet still backwards compatible with WPA, WPA2 utilizes 802.1X and EAP (Extensible Authentication Protocol) to verify users on the wireless network using a Pre-Shared Key. Once all users on the LAN have been authenticated, there can be a securely encrypted flow of information between all parties on the LAN.

For home users that will not incorporate a RADIUS server in their network, the security for the DI-624S, 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-624S 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. No longer will you have to manually input a new WEP key frequently to ensure security, with the DI-624S, you will automatically receive a new key every time you connect, vastly increasing the safety of your communications.

The DI-624S comes equipped with two 2.0 USB ports on the rear panel. These ports increase the functionality of the router exponentially. Utilizing any of these USB ports, the administrator can now enable the router to be a print server as well. These ports are especially ideal for outside users wanting to view files on your D-Link Media Lounge using the UPnP AV function on the router. You may also share files with users on you LAN or WAN by attaching a network storage device to one of these USB ports and using one of the sharing functions on the router, either the file server or the FTP Server function.

Connections

All Ethernet Ports (WAN and LAN) are auto MDI/MDIX, meaning you can use either a straight-through or a crossover Ethernet cable.



USB 2.0 Connections.

Use these ports to connect your USB printer or memory media for file sharing.

Factory Reset Button

Pressing this button will restore the router to its factory default settings.

Auto MDI/MDIX LAN Ports

Connect the Ethernet cable from computers on your LAN to these ports.

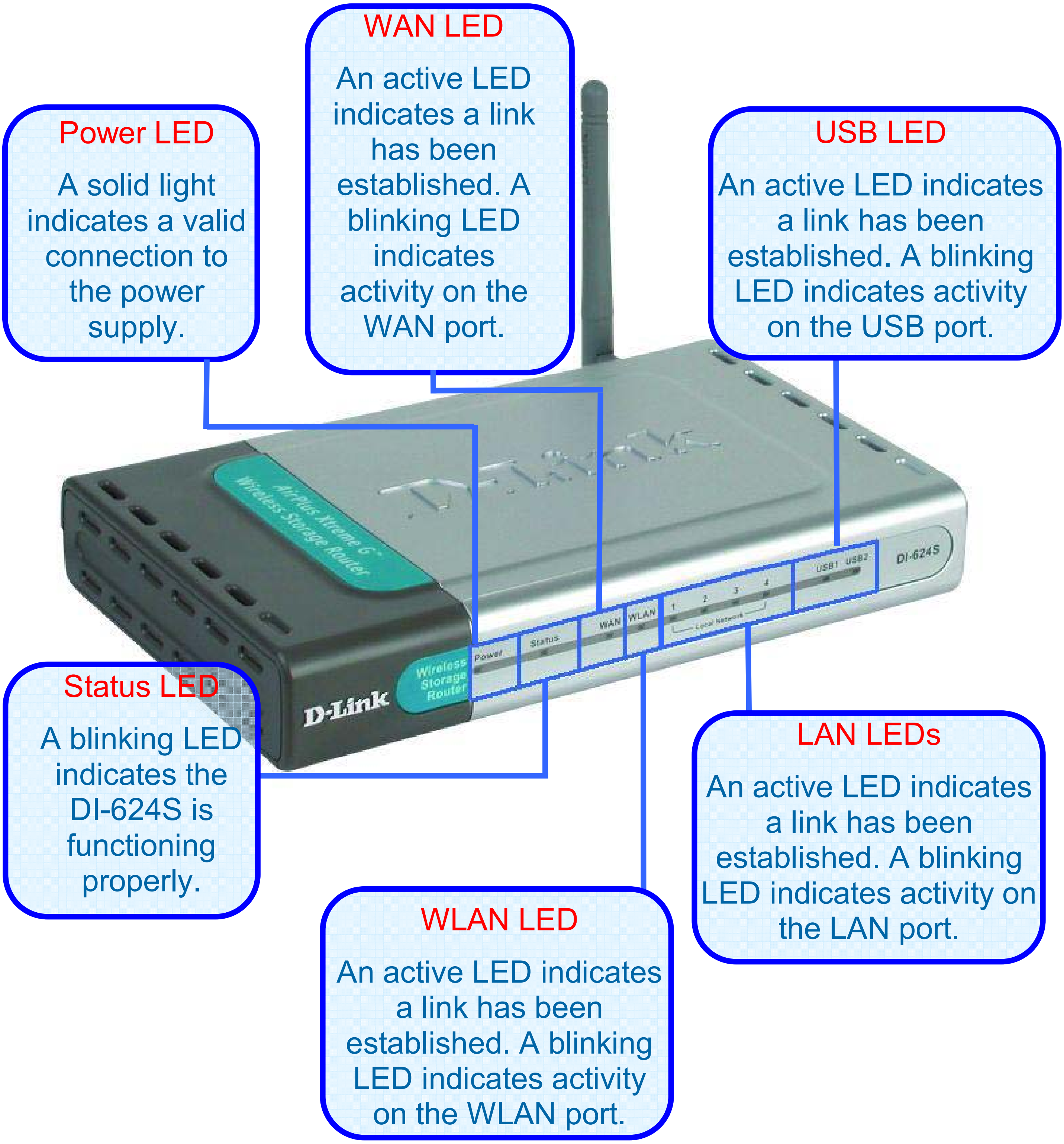
WAN Port

Connect the Ethernet cable from your ADSL modem to this port.

Power Adapter

Connect your 5V 3A power adapter here.

LEDs



Power LED

A solid light indicates a valid connection to the power supply.

WAN LED

An active LED indicates a link has been established. A blinking LED indicates activity on the WAN port.

USB LED

An active LED indicates a link has been established. A blinking LED indicates activity on the USB port.

Status LED

A blinking LED indicates the DI-624S is functioning properly.

WLAN LED

An active LED indicates a link has been established. A blinking LED indicates activity on the WLAN port.

LAN LEDs

An active LED indicates a link has been established. A blinking LED indicates activity on the LAN port.

Features

- Fully compatible with the 802.11g standard to provide a wireless data rate of up to 54Mbps
- Backwards compatible with the 802.11b standard to provide a wireless data rate of up to 11 Mbps
- WPA 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
- New WPA2 enhanced wireless security authenticates using 802.1X and a Pre-Shared key, and encrypts the data with the AES encryption standard. Wi-Fi certified, WPA2 is also compatible with WPA and can be used for a large network or for the SOHO environment
- 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
- IP Filtering
- URL Filtering
- Domain Blocking
- Scheduling
- DHCP server supported 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 10/100Mbps Ethernet ports, 1 WAN port, Auto MDI/MDIX
- Equipped with two 2.0USB ports at the rear of the router used to connect

various devices to be shared over a network, such as USB storage devices and printers

- VPN Pass Through
- DMZ and DDNS functions
- Stateful Packet Inspection for protection against unwanted packets
- Quality of Service (QoS) for prioritizing ports and IP addresses
- UPnP AV function for sharing audio and video files using a media storage device
- Multiple users and administrators with configurable privileges for each
- Intrusion detection for ICMP, SYN, UDP flood, Land, IP spoof, Ping of Death, Port Scan, Smurf, Steal Fin, Syn with data, Tear Drop, and UDP bomb attacks
- Statistics for all main functions on the router

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. D-Link wireless products will allow you access to the data you want, when and where you want it. You will be able to enjoy the freedom that wireless networking brings.

A WLAN is a cellular computer network that transmits and receives data with radio signals instead of wires. WLANs 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.

Wireless users can use the same applications they use on a wired network. Wireless adapter cards used on laptop and desktop systems support the same protocols as Ethernet adapter cards.

People use wireless LAN technology for many different purposes:

Mobility - Productivity increases when people have access to data in any location within the operating range of the WLAN. Management decisions based on real-time information can significantly improve worker efficiency.

Low Implementation Costs – WLANs are easy to set up, manage, change and relocate. Networks that frequently change can benefit from WLANs ease of implementation. WLANs can operate in locations where installation of wiring may be impractical.

Installation and Network Expansion - Installing a WLAN system can be fast and easy and can eliminate the need to pull cable through walls and ceilings. Wireless technology allows the network to go where wires cannot go - even outside the home or office.

Scalability – WLANs can be configured in a variety of topologies to meet the needs of specific applications and installations. Configurations are easily changed and range from peer-to-peer networks suitable for a small number of users to larger infrastructure networks to accommodate hundreds or thousands of users, depending on the number of wireless devices deployed.

Inexpensive Solution - Wireless network devices are as competitively priced as conventional Ethernet network devices.

Standards-Based Technology

The DI-624S Wireless Broadband Router utilizes the new 802.11g standard.

The IEEE 802.11g standard is an extension of the 802.11b standard. It increases the data rate up to 54 Mbps within the 2.4GHz band, utilizing OFDM technology.

This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high speed digital data over a radio wave utilizing OFDM (Orthogonal Frequency Division Multiplexing) technology. OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk (interference) in signal transmissions.

The DI-624S is backwards compatible with 802.11 b devices. This means that if you have an existing 802.11 b network, the devices in that network will be compatible with 802.11g devices at speeds of up to 11 Mbps in the 2.4GHz range.

Installation Considerations

The D-Link DI-624S lets you access your network, using a wireless connection, from virtually anywhere within its operating range. 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 DI-624S and other network devices to a minimum - each wall or ceiling can reduce your D-Link wireless product’s range from 3-90 feet (1-30 meters.) Position your devices so that the number of walls or ceilings is minimized.

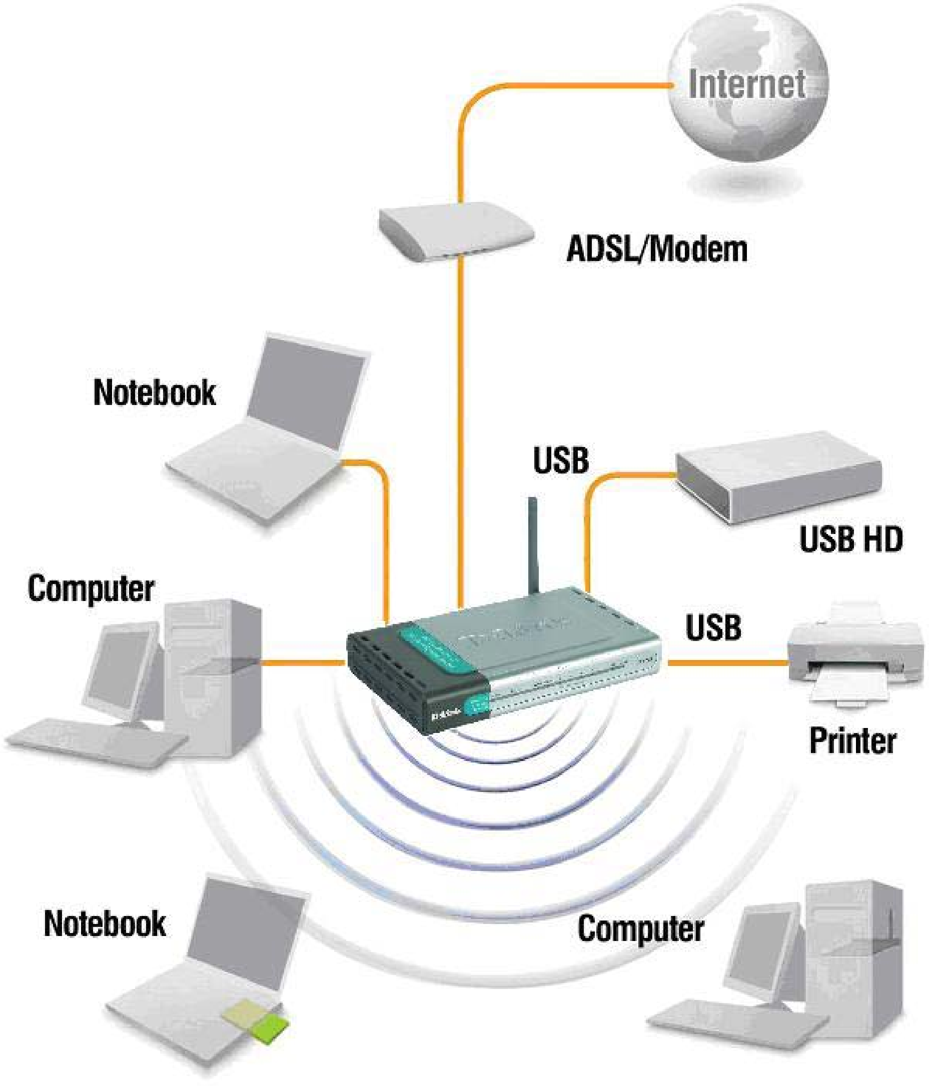
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or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

3. Building Materials can impede the wireless signal - a solid metal door or aluminum studs may have a negative effect on range. Try to position wireless devices and computers with wireless adapters so that the signal passes through drywall or open doorways and not other materials.

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

Getting Started

Setting up a Wireless Infrastructure Network



Please remember that D-Link AirPlus G wireless devices are pre-configured to connect together, right out of the box, with their default settings. For a typical wireless setup at home (as shown above), please do the following:

1. You will need broadband Internet access (a Cable or DSL-subscriber line into your home or office)
2. Consult with your Cable or DSL provider for proper installation of the modem
3. Connect the Cable or DSL modem to the DI-624S Wireless Storage Router (see the printed Quick Installation Guide included with your router.)
4. If you are connecting a desktop computer to your network, install the D-Link AirPlus G DWL-G520 wireless PCI adapter into an available PCI slot on your desktop computer. You may also install the DWL-G520.

5. (See the printed Quick Installation Guide included with the network adapter.)

6. Install the D-Link DWL-G650 wireless Cardbus adapter into a laptop computer. (See the printed Quick Installation Guide included with the DWL-G650.)

7. Install the D-Link DFE-530TX+ adapter into a desktop computer. The four Ethernet LAN ports of the DI-624S are Auto MDI/MDIX and will work with both Straight-Through and Cross-Over cable.

(See the printed Quick Installation Guide included with the DFE-530TX+.)

Connect your printer to the printer port on the DI-624S. Please refer to the quick installation guide for loading the print server software.

Installing the Print Server

To avoid any problems that may arise when you install your USB printer, follow this procedure. If the print server is powered on before a network connection is established, configuration problems may arise.

1. Before connecting your printer to the DI-624S, make sure that your printer is functioning properly.

2. Once you have made sure that it is working properly, turn off the power to the printer.

3. Confirm that your computer network is functioning properly.

4. Connect the DI-624S to your network, using a standard Ethernet cable. Leave the router powered off.

5. While the printer is still powered off, connect the printer to one of the available USB slots at the rear of the router.

6. Power on your USB printer.

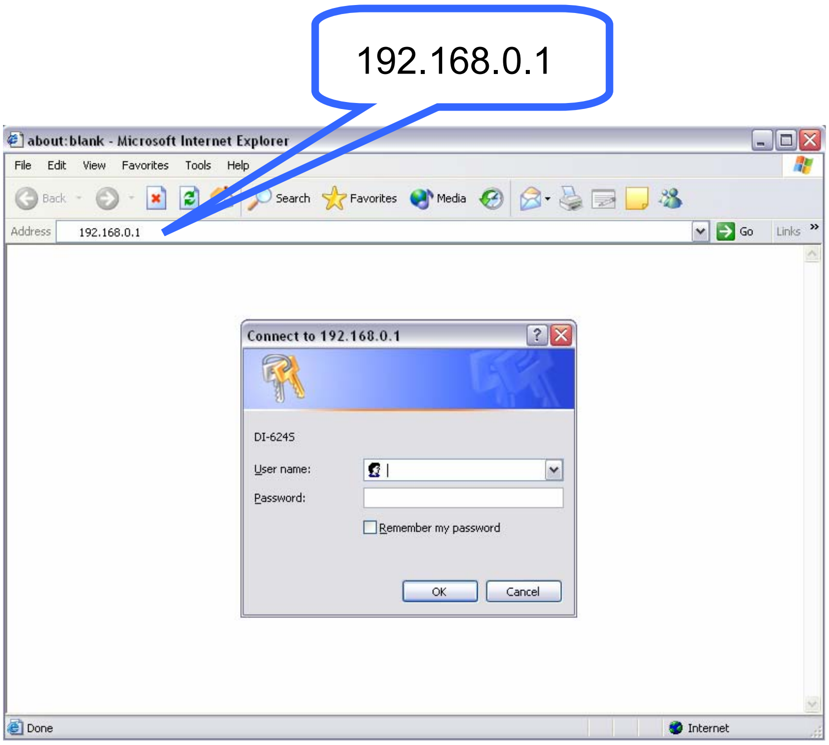
7. Plug the power adapter into the available power adapter slot at the back of the router.

8. Plug the other end of the power adapter into an available power outlet. This will supply electricity to the Router since there is no external power switch. The corresponding green USB LED at the front of the router should light green, indicating a valid connection to the router.

To configure the router for use on your LAN, please go to the Advanced section of this manual, under the heading **Home > LAN**.

Using the Configuration Wizard

Whenever you want to configure your network or the DI-624S, you can access the Configuration Menu by opening the web-browser and typing in the IP Address of the DI-624S. The DI-624S default IP Address is shown to the right:



192.168.0.1

about:blank - Microsoft Internet Explorer

Address: 192.168.0.1

Connect to 192.168.0.1

DI-624S

User name:

Password:

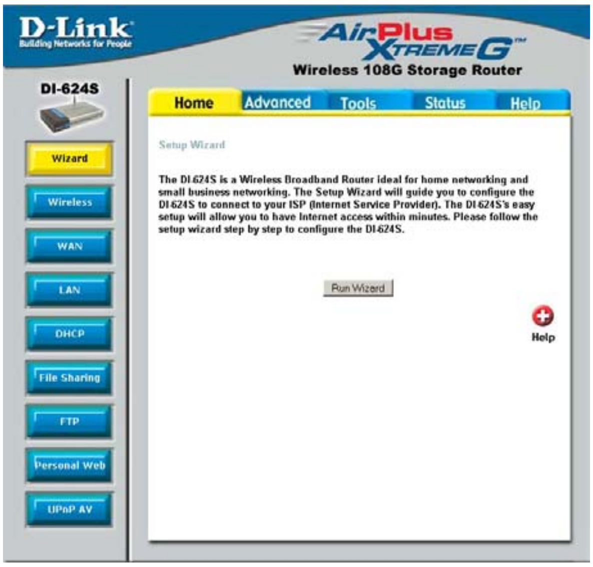
□ Remember my password

OK Cancel

File Edit View Favorites Tools Help
Back Search Favorites Media
Go Links
Done
Internet

- Open the web browser
- Type in the IP Address of the Router (http://192.168.0.1)
- Type admin in the User Name field
- Leave the Password blank
- Click OK

The **Home > Wizard** screen will appear. Please refer to the Quick Installation Guide for more information regarding the Setup Wizard.



Setup Wizard

The DI-624S is a Wireless Broadband Router ideal for home networking and small business networking. The Setup Wizard will guide you to configure the DI-624S to connect to your ISP (Internet Service Provider). The DI-624S's easy setup will allow you to have Internet access within minutes. Please follow the setup wizard step by step to configure the DI-624S.

These buttons appear on most of the configuration screens in this section. Please click on the appropriate button at the bottom of each screen after you have made a configuration change.

Note: if you have changed the default IP Address assigned to the DI-624S, make sure to enter the correct IP Address.

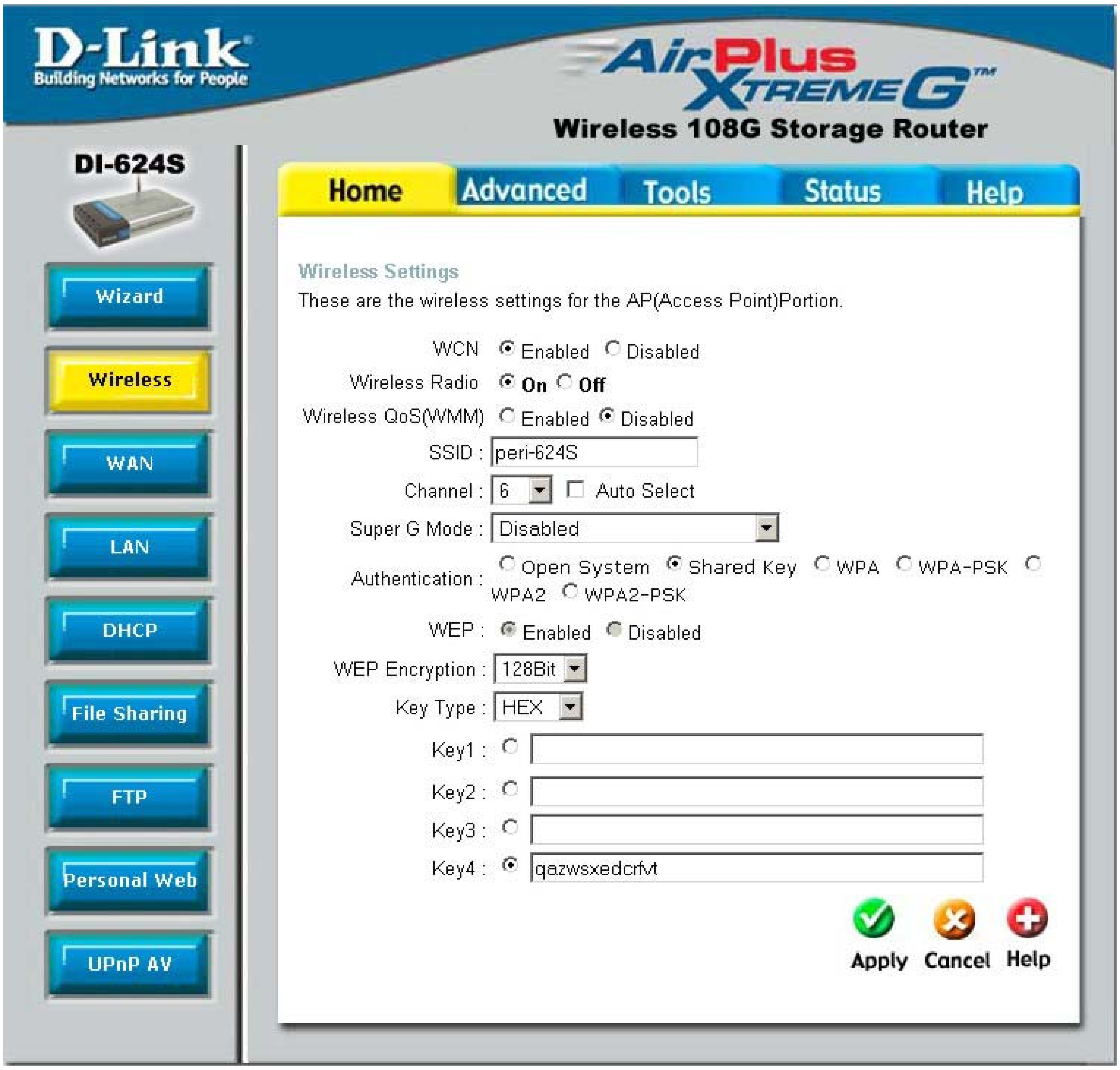
Apply — Clicking this button will save configured settings to the router.

Cancel — Clicking Cancel will clear changes made to the current page.

Help — Clicking Help will provide the user with helpful information about the current window.

Refresh — Click refresh will refresh the statistics of the current window.

Home > Wireless



Wireless Settings

These are the wireless settings for the AP(Access Point)Portion.

WCN ● Enabled ○ Disabled

Wireless Radio ● On ○ Off

Wireless QoS(WMM) ○ Enabled ● Disabled

SSID : peri-624S

Channel : 6 □ Auto Select

Super G Mode : Disabled

Authentication : ○ Open System ● Shared Key ○ WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK

WEP : ● Enabled ○ Disabled

WEP Encryption : 128Bit

Key Type : HEX

Key1 : ○

Key2 : ○

Key3 : ○

Key4 : ● qazwsxedcrfvt

WCN

WCN or Windows Connect Now Technology is used to automatically configure the wireless settings for this device. The WCN must be previously configured on computer running a Windows XP operating system, which has Service Pack 2 installed. Once the configuration has been completed by running the Wireless Network Setup Wizard, it must be saved to a USB enabled memory device and then uploaded automatically to the router and any other device to be put on this wireless network, using this method. No configuration will be necessary except for ensuring that this WCN radio button is enabled before connecting the memory drive to the router. For a concise explanation on configuring the WCN on Windows XP, see the Appendix at the back of this manual. *(Note: For the client implementation of this function, please see the user manual for the associated client PC)*

Wireless Radio

Click the appropriate radio button to enable or disable the Wireless Access part of this device.

Wireless QoS (WMM)

Clicking the Enabled radio button in this section will enable QoS for WiFi MultiMedia (WMM). This function will give priority to audio and video information travelling over the wirless network. This function is especially important in sharing files over your LAN using a media server, such as the D-Link Media Lounge and thus will help provide a continuous media stream.

SSID

Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is DI-624S. The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network. This field will be automatically configured for users who have uploaded a WCN configuration.

Channel

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

Super G Mode

Enabling this function will aid in the throughput performance of the router by adding Dynamic Packet Bursting, Fast Frames, Hardware Encryption and Compression and Turbo Mode. The default setting is Disabled. The user has three choices:

None – Super G Mode is disabled.

Super G without Turbo – Will enable Dynamic Packet Bursting, Fast Frames and Hardware Encryption and Compression, while leaving the Turbo Mode disabled.

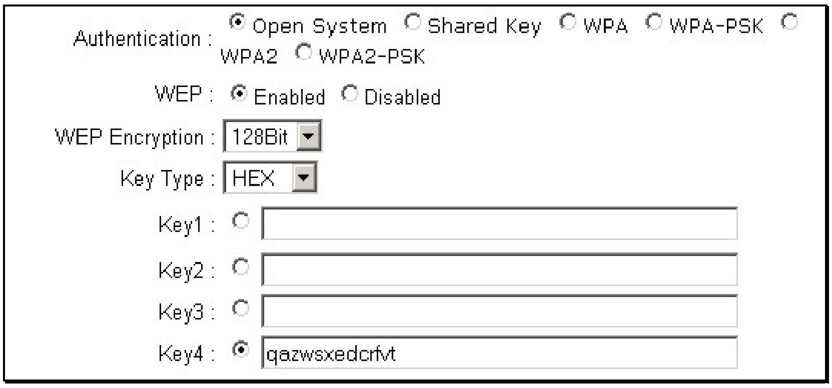
Super G with Dynamic Turbo – Enabling this function will enable Dynamic Packet Bursting, Fast Frames and Hardware Encryption and Compression, and Dynamic Turbo mode. This mode allows the router to use two radio channels to double the data transfer rate. All nodes on the wireless network must be Turbo capable for this function to work. If not, all devices on this wireless network will have a normal data transfer rate. Turbo mode is only enabled for use when all devices on the wireless LAN are turbo enabled. This turbo mode is backwards compatible with non-Turbo legacy devices.

Authentication

This router employs three basic types of Authentication for access to the router's wireless network, Open System/Shared Key 802.1X (RADIUS) and PSK (Pre-Shared Key), which can be selected by clicking the corresponding radio button. Each selection will alter the window to accommodate the entry of the selected Authentication. See the explanation below for more information.

Open System/Shared Key

The Open System/Shared Key choice for Authentication will produce the same screen for the user's configuration. The Open System choice is for general use and utilizes the basic WEP encryption. The Shared Key choice is used between cooperating devices that share a common encryption key. WEP (Wireless Encryption Protocol or Wired Equivalent Privacy) encryption can be enabled for security and privacy. WEP encrypts the data portion of each frame transmitted from the wireless adapter using one of the predefined keys. Decryption of the data contained in each packet can only be done if the both the receiver and transmitter have the correct shared key.



Authentication : ● Open System ○ Shared Key ○ WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK

WEP : ● Enabled ○ Disabled

WEP Encryption : 128Bit

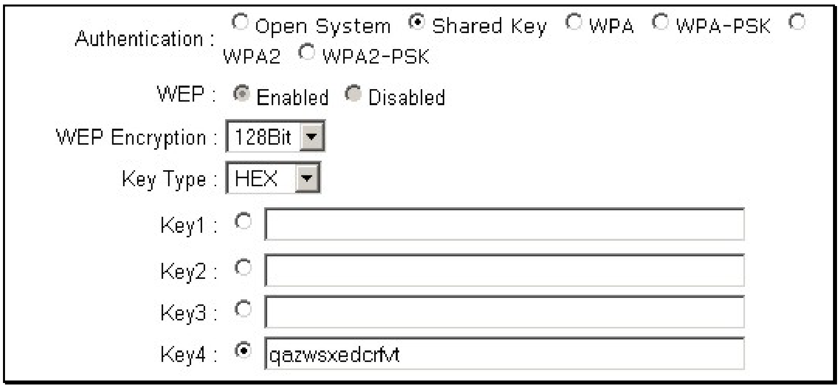
Key Type : HEX

Key1 : ○

Key2 : ○

Key3 : ○

Key4 : ● qazwsxedcrfvt



Authentication : ○ Open System ● Shared Key ○ WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK

WEP : ● Enabled ○ Disabled

WEP Encryption : 128Bit

Key Type : HEX

Key1 : ○

Key2 : ○

Key3 : ○

Key4 : ● qazwsxedcrfvt

WEP – Click the Enabled radio button to employ WEP encryption on the router.

WEP Encryption - Use the drop down menu to select the type of WEP encryption. Select *64 Bit* to enabled 64 bit Hexadecimal encryption, *128 Bit* to enable 128 bit Hexadecimal encryption. For 64-bit encryption, the (ASCII) characters are converted automatically and listed as 10-digit hexadecimal keys. 64-bit encryption allows you to select one of four active keys. For 128-bit encryption, the characters are converted and listed as a 26 digit hexadecimal key. 128-bit encryption allows you to select one of four active keys. 128-bit keys are to be from 5-13 inputted characters in length and 256-bit keys must be from 10-26 inputted characters in length. Failing to have the same key on the server and its clients will result in the clients not receiving any information from the router or its connected devices.

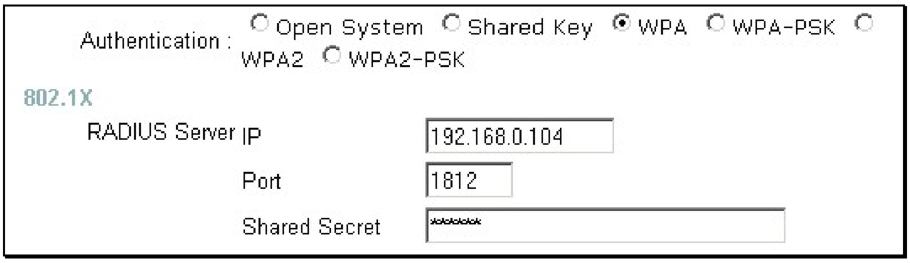
Key Type – Use the pull-down menu to select the type of Key to be used for encryption. The user may choose **HEX** (Hexidecimal) or **ASCII** (American Standard Code for Information Interchange). Both will require the user to enter a key in the following field.

Key – The user may enter up to four keys to be used for encryption. Only the key selected using the corresponding radio button will be used for encryption.

Click **Apply** to set the information in the router's memory. *(Note: For the client implementation of this function, please see the user manual for the associated client PC)*

WPA

WPA or Wireless Protection Access is a new an improved standard of wireless security. WPA offers encryption keys of up to 256-bits that automatically change frequently. On this router, the WPA utilizes the RADIUS protocol, which utilizes a server to authorize the user by matching a Shared Secret password listed in its RADIUS database. There are two choices for the user to choose from. **WPA** and **WPA2** which uses the Advanced Encryption Standard (AES). In order to use this function, a RADIUS server must be established on a computer on the LAN. This RADIUS server must be configured to have the same key as the users on the LAN accessing it.



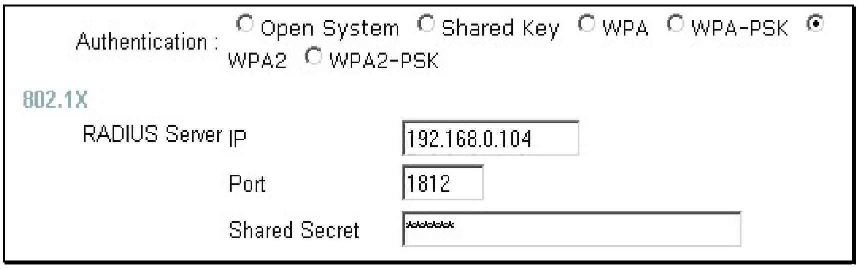
Authentication : ○ Open System ○ Shared Key ● WPA ○ WPA-PSK ○ WPA2 ○ WPA2-PSK

802.1X

RADIUS Server IP 192.168.0.104

Port 1812

Shared Secret ******



Authentication : ○ Open System ○ Shared Key ○ WPA ○ WPA-PSK ● WPA2 ○ WPA2-PSK

802.1X

RADIUS Server IP 192.168.0.104

Port 1812

Shared Secret ******

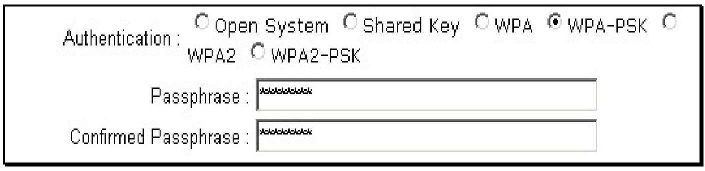
RADIUS Server IP – Enter the IP address of the remote RADIUS server through which you will be authenticated.

Port – Enter the virtual port number to which to connect through the RADIUS server. Common port numbers for RADIUS are 1812 and 1813.

Shared Secret – Enter the password which will be used to authenticate you on the wireless network. This password must be the same on the RADIUS server in order for you to be authorized. *(Note: For the client implementation of this function, please see the user manual for the associated client PC)*

WPA-PSK

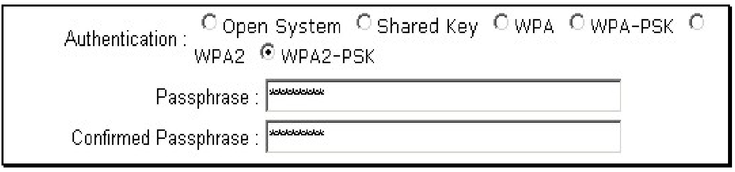
WPA-PSK (Pre-Shared Key) uses the same encryption as the WPA but is implemented differently. All devices on the wireless network share the same key (Passphrase) to activate the WPA security. There are two choices for the user to choose from. **WPA-PSK** and **WPA2-PSK** which uses the Advanced Encryption Standard (AES). To utilize, select one of the previous choices, enter the Passphrase, confirm it in the second field and click **Apply**. *(Note: For the client implementation of this function, please see the user manual for the associated client PC)*



Authentication : ○ Open System ○ Shared Key ○ WPA ● WPA-PSK ○ WPA2 ○ WPA2-PSK

Passphrase : ********

Confirmed Passphrase : ********

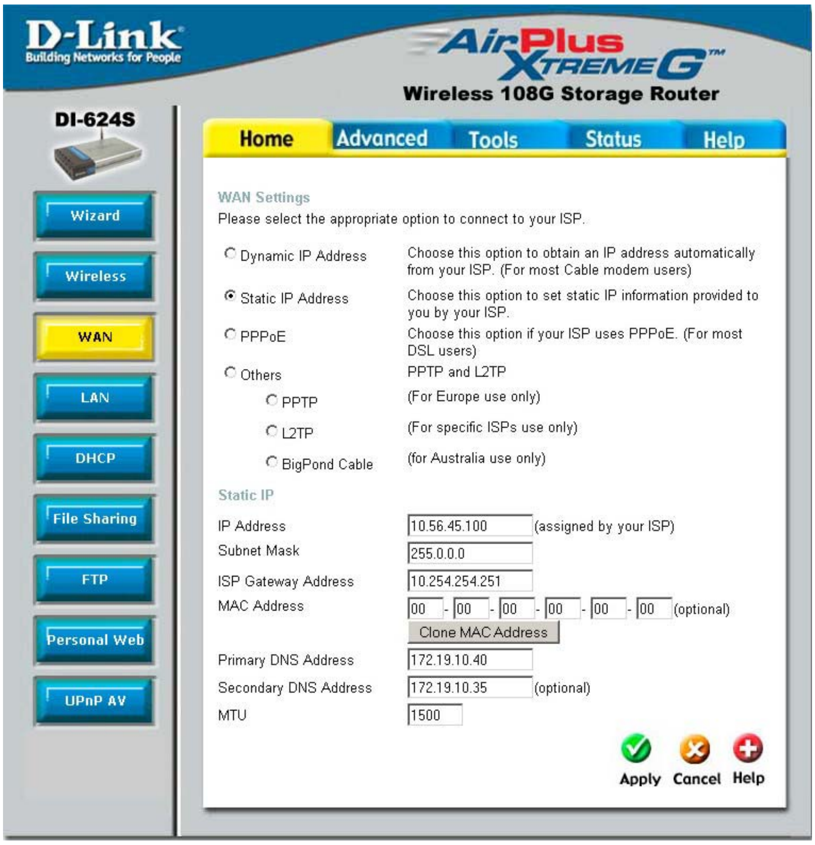


Authentication : ○ Open System ○ Shared Key ○ WPA ○ WPA-PSK ○ WPA2 ● WPA2-PSK

Passphrase : ********

Confirmed Passphrase : ********

Home > WAN



WAN Settings

Please select the appropriate option to connect to your ISP.

○ Dynamic IP Address — Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)

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

○ PPPoE — Choose this option if your ISP uses PPPoE. (For most DSL users)

○ Others — PPTP and L2TP

○ PPTP — (For Europe use only)

○ L2TP — (For specific ISPs use only)

○ BigPond Cable — (for Australia use only)

Static IP

IP Address: 10.56.45.100 (assigned by your ISP)

Subnet Mask: 255.0.0.0

ISP Gateway Address: 10.254.254.251

MAC Address: 00 - 00 - 00 - 00 - 00 - 00 (optional)

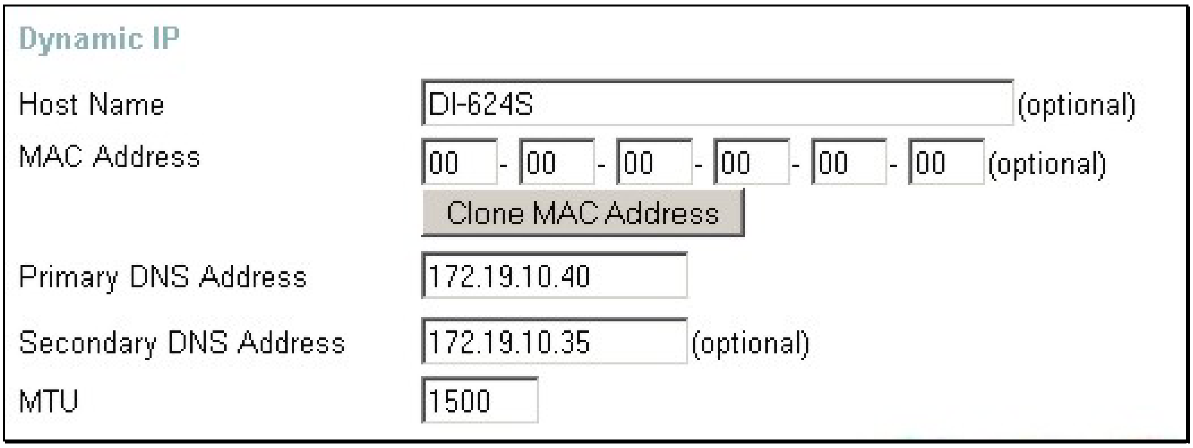
Primary DNS Address: 172.19.10.40

Secondary DNS Address: 172.19.10.35 (optional)

MTU: 1500

Static IP Address	Choose Static IP Address if all WAN IP information is provided to you by your ISP. You will need to enter in the IP address, subnet mask, gateway address, and DNS address(es) provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Router will not accept the IP address if it is not in this format.
IP Address	Input the public IP Address provided by your ISP.
Subnet Mask	Input your Subnet mask. (All devices in the network must have the same subnet mask.)
ISP Gateway Address-	Input the public IP address of the ISP to which you are connecting.
Primary DNS Address	Input the primary DNS (Domain Name Server) IP address provided by your ISP
Secondary DNS Address	This is an optional DNS Address entry to be used if the primary DNS fails.
MTU	Enter an MTU value only if required by your ISP. Otherwise, leave it at the default setting.

Dynamic IP Address



Dynamic IP

Host Name: DI-624S (optional)

MAC Address: 00 - 00 - 00 - 00 - 00 - 00 (optional)

Primary DNS Address: 172.19.10.40

Secondary DNS Address: 172.19.10.35 (optional)

MTU: 1500

Dynamic

Choose **Dynamic IP Address** to obtain IP address information automatically from your ISP. This option should be selected if your ISP has not supplied you with an IP address. This option is commonly used for Cable modem services.

Host Name

The **Host Name** is optional but may be required by some ISPs. The default host name is the device name of the Router and may be changed.

MAC Address

The default MAC Address is set to the WAN's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

Clone MAC Address

The default MAC address is set to the WAN's physical interface MAC address on the Broadband Router. You can use the "**Clone MAC Address**" button to copy the MAC address of the Ethernet Card installed by your ISP and replace the WAN MAC address with the MAC address of the router. It is not recommended that you change the default MAC address unless required by your ISP.

Primary/Secondary DNS Address

Enter a DNS Address if you wish not to use the address provided by your ISP.

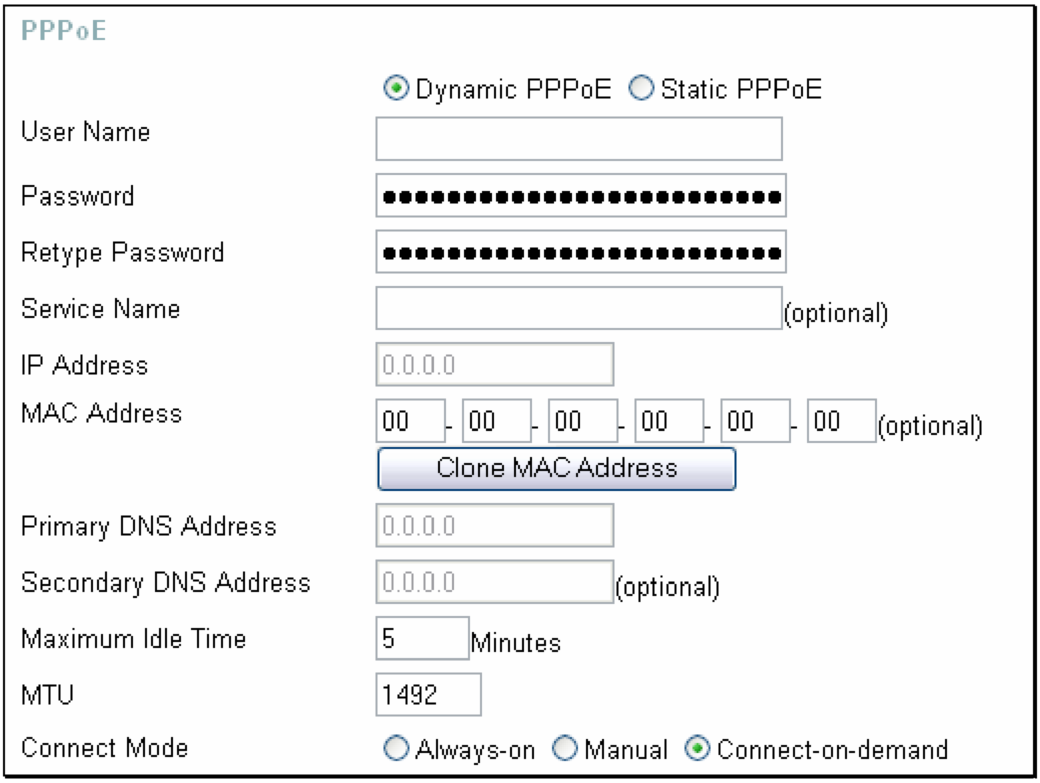
MTU

Enter an MTU value only if required by your ISP. Otherwise, leave it at the default setting.

Please be sure to remove any existing PPPoE client software installed on your computers.

Home > WAN > PPPoE

Choose PPPoE (Point to Point Protocol over Ethernet) if your ISP uses a PPPoE connection. Your ISP will provide you with a username and password. This option is typically used for DSL services. Select **Dynamic PPPoE** to obtain an IP address automatically for your PPPoE connection. Select **Static PPPoE** to use a static IP address for your PPPoE connection.



PPPoE

	● Dynamic PPPoE ○ Static PPPoE
User Name	
Password	••••••••••••••••••••••••••
Retype Password	••••••••••••••••••••••••••
Service Name	(optional)
IP Address	0.0.0.0
MAC Address	00 - 00 - 00 - 00 - 00 - 00 (optional)
	Clone MAC Address
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0 (optional)
Maximum Idle Time	5 Minutes
MTU	1492
Connect Mode	○ Always-on ○ Manual ● Connect-on-demand

PPPoE — Choose this option if your ISP uses PPPoE. (Most DSL users will select this option.)

Dynamic PPPoE Choose this option to receive an IP Address automatically from your ISP.

Static PPPoE Choose this option to you have an assigned (static) IP Address.

Password — Enter The PPPoE user name provided to you by your ISP.

Retype Password — Retype the password entered in the previous field.

Service Name — Enter the **Service Name** provided by your ISP (optional).

IP Address — This option is only available for Static PPPoE. Enter the static IP address for the PPPoE connection.

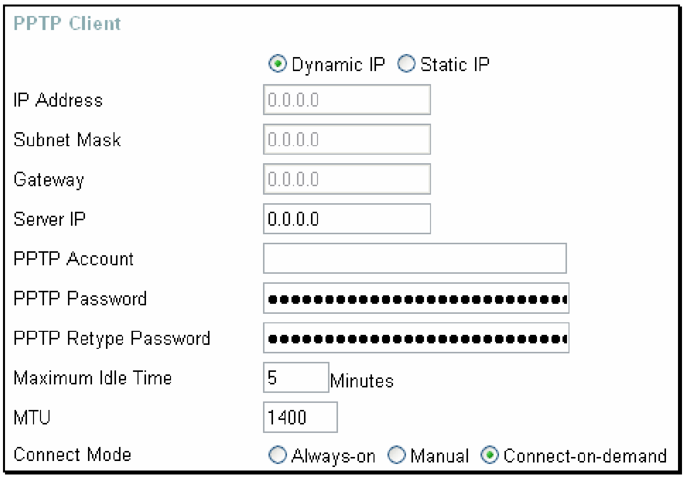
MAC Address — The default MAC Address is set to the WAN's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

Clone MAC Address	The default MAC address is set to the WAN's physical interface MAC address on the Broadband Router. You can use the "Clone MAC Address" button to copy the MAC address of the Ethernet Card installed by your ISP and replace the WAN MAC address with the MAC address of the router. It is not recommended that you change the default MAC address unless required by your ISP.
Primary DNS Address	Input the primary DNS (Domain Name Server) IP address provided by your ISP
Secondary DNS Address	This is an optional DNS Address entry to be used if the primary DNS fails.
Maximum Idle Time	The amount of time of inactivity before the device will disconnect time your PPPoE session. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the defined Maximum Idle Time, then the connect ion will be dropped. Either set the value for idle time to zero or enable Auto-reconnect to disable this feature.
MTU	Enter an MTU value only if required by your ISP. Otherwise, leave it at the default setting.
Connect Mode	Allows the user to choose a method of connecting to the ISP. Always-On will keep the router connected through Idle times. Manual will require the user to connect manually using the router anytime a connection to the ISP has timed out. Connect-on-demand will instruct the router to connect to the ISP anytime information is sent from the connected computer on the LAN.

Click **Apply** to set any changes made to the memory of the router.

Home > WAN > Others > PPTP

PPTP or Point-to-Point Protocol is a safe method of sending information between VPN's securely using encryption over PPP. You, as the client, need to enter the correct information that the server has in order to create that secure tunnel. Using Dynamic IP, the router will set your basic IP parameters for you, such as the IP Address, Subnet Mask and Gateway. For Static IP, this information must be set manually by the user. All information in this window should be provided by your ISP.



PPTP Client

	● Dynamic IP ○ Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Server IP	0.0.0.0
PPTP Account	
PPTP Password	••••••••••••••••••••••••••••
PPTP Retype Password	••••••••••••••••••••••••••••
Maximum Idle Time	5 Minutes
MTU	1400
Connect Mode	○ Always-on ○ Manual ● Connect-on-demand

PPTP

Choose between **Dynamic** and **Static** IP.

IP Address

Enter the IP address of the router for a static IP entry. Dynamic IP requires no input here.

Subnet Mask

Enter the Subnet Mask address of the router for a static IP entry. Dynamic IP requires no input here.

Gateway

Enter the gateway address here. This is the IP address of the ISP server.

Server IP

Enter the IP address of the PPTP's server computer. This is how the user will become authenticated to use PPTP.

PPTP Account

Enter the name of the PPTP account as provided to you by your ISP.

PPTP Password

Enter the PPTP password as provided to you by your ISP.

PPTP Retype Password

Retype the password entered in the PPTP Password field.

Maximum Idle Time

A value of 0 means that the PPP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the Router after the WAN connection has been idle for the amount of time specified. The default value = 5.

MTU

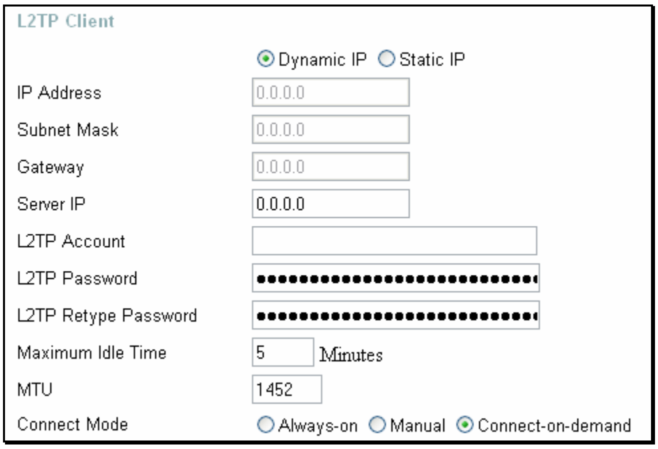
Enter an MTU value only if required by your ISP. Otherwise, leave it at the default setting.

Connect Mode

This function, with **Connect-on-demand** selected, will allow the router to connect any workstation on your LAN to the Internet upon request. If this function is set at **Always-on**, no request from the workstation will be needed to connect to the Internet. If **Manual** is selected, it will be necessary for the workstation on the LAN to manually connect to the Internet through this router.

Home > WAN > Others > L2TP

Some ISPs may require the user to uplink using the **L**ayer **2** **P**rotocol **T**unneling (L2PT) method. L2PT is a VPN protocol that will ensure a direct connection to the server using an authentication process that guarantees the data originated from the claimed sender and was not damaged or altered in transit. Once connected to the VPN tunnel, it seems to the user that the client computer is directly connected to the internal network. To set up your L2PT connection, enter the following data that was provided to you by your ISP.



L2TP Client

	◉ Dynamic IP ○ Static IP
IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Server IP	0.0.0.0
L2TP Account	
L2TP Password	••••••••••••••••••••••••••••
L2TP Retype Password	••••••••••••••••••••••••••••
Maximum Idle Time	5 Minutes
MTU	1452
Connect Mode	○ Always-on ○ Manual ◉ Connect-on-demand

L2PT

Choose between **Dynamic** and **Static** IP. Using Dynamic IP, the router will set your basic IP parameters, such as the IP Address, Subnet Mask and Gateway. For Static IP, this information must be set manually by the user.

IP Address

The IP address that will be assigned to your router for this connection, as stated by your ISP. Dynamic IP requires no input here.

Subnet Mask

The IP address of the corresponding Subnet Mask, as stated to you by your ISP. Dynamic IP requires no input here.

Gateway

The IP address of the gateway device, as stated to you by your ISP. Dynamic IP requires no input here.

Server IP

The IP address of your ISP's server computer, as stated to you by your ISP.

L2PT Account

The account name of the L2PT account that has been assigned to you by your ISP.

L2PT Password

The password of the L2PT account that was supplied to you by your ISP.

L2PT Retype Password

Retype the password that was entered in the L2PT field. Ensure that these two passwords are identical or an error will occur.

Maximum Idle Time

A value of 0 means the PPP connection will remain connected. If your network account is billed according to the amount of time the Router is actually connected to the Internet, enter an appropriate Idle Time value (in seconds). This will disconnect the Router after the WAN connection has been idle for the amount of time specified. The default value = 5.

MTU

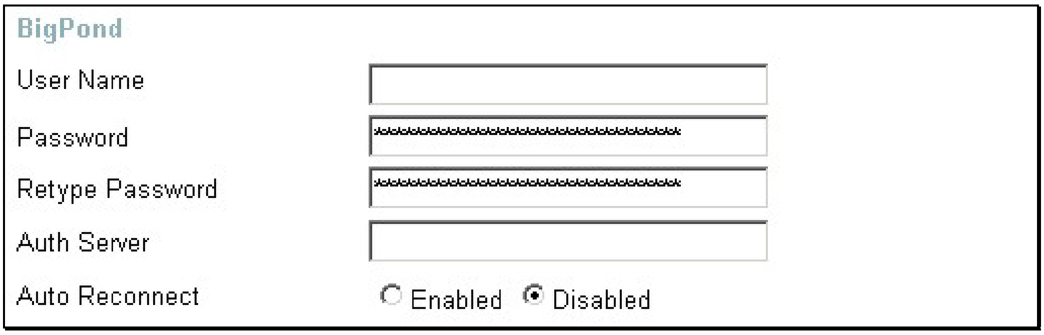
Enter an MTU value only if required by your ISP. Otherwise, leave it at the default setting.

Connect Mode

If **Connect-on-demand is** selected, will allow the router to connect any workstation on your LAN to the Internet upon request. If **Always-on**, no request from the workstation will be needed to connect to the Internet. If **Manual** is selected, the workstation on the LAN must manually connect to the Internet through this router.

Home > WAN > Others > BigPond Cable

This selection is for users having Big Pond Cable as their ISP. Enter the following information, as provided to you by your ISP.



BigPond

User Name	
Password	********************************
Retype Password	********************************
Auth Server	
Auto Reconnect	○ Enabled ● Disabled

User Name
Enter the user name as provided to you by your ISP.

Password
Enter The PPPoE user name provided to you by your ISP.

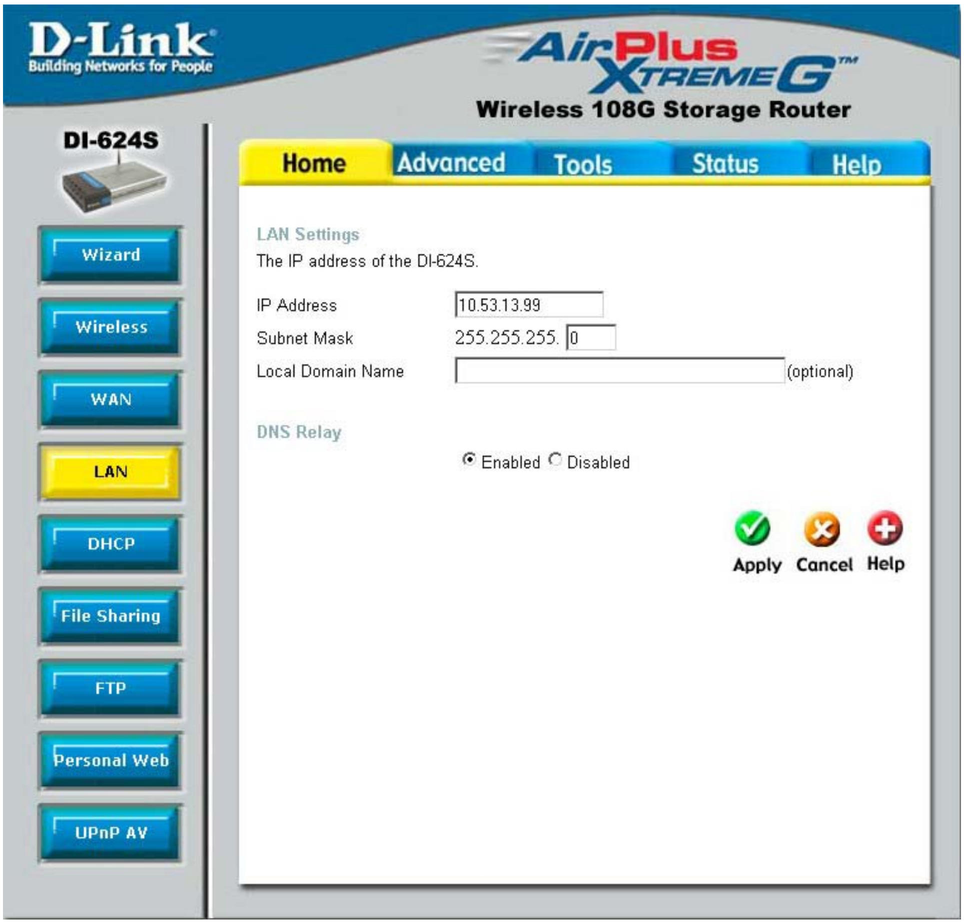
Retype Password
Retype the password entered in the previous field.

Auth Server
Enter the name of the Authentication Server as provided to you by your ISP. This is the computer that will accept your user name and password to be authenticated on the network.

Auto Reconnect
Checking the **Enabled** radio button will allow the router to reconnect to the network automatically if it becomes disconnected.

Home > LAN

LAN is short for Local Area Network. This is considered your internal network. These are the IP settings of the LAN interface for the DI-624S and may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.



LAN Settings
The IP address of the DI-624S.

IP Address 10.53.13.99
Subnet Mask 255.255.255. 0
Local Domain Name (optional)

DNS Relay
● Enabled ○ Disabled

IP Address

The IP address of the LAN interface. The default IP address is 192.168.0.1.

Subnet Mask

The subnet mask of the LAN interface. The default subnet mask is 255.255.255.0.

Local Domain Name

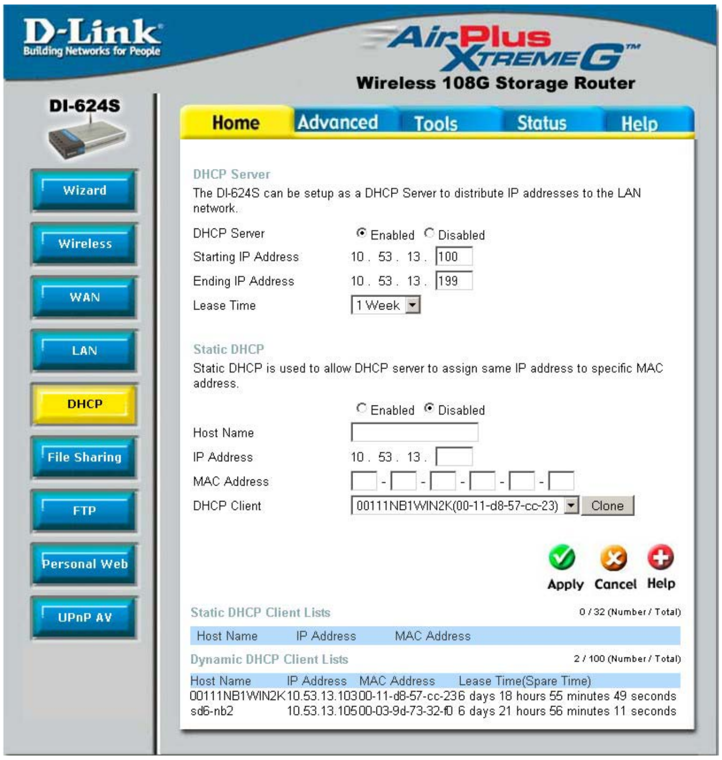
This entry is for the local Domain set on your network, if you have given it a name previously. This field is for your personal use and unnecessary for proper configuration of this window.

DNS Relay

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

Home > DHCP

Dynamic Host Configuration Protocol (DHCP) allows the gateway to automatically obtain the IP address from a DHCP server on the service provider's network. The service provider assigns a global IP address from a pool of addresses available to the service provider. Typically the IP address assigned has a long lease time, so it will likely be the same address each time the Router requests an IP address. If DHCP is not enabled on the Router, it is necessary for the user to assign a static IP address to each computer on your LAN.



DHCP Server

The DI-624S can be setup as a DHCP Server to distribute IP addresses to the LAN network.

DHCP Server	● Enabled ○ Disabled
Starting IP Address	10 . 53 . 13 . 100
Ending IP Address	10 . 53 . 13 . 199
Lease Time	1 Week

Static DHCP

Static DHCP is used to allow DHCP server to assign same IP address to specific MAC address.

	○ Enabled ● Disabled
Host Name	
IP Address	10 . 53 . 13 .
MAC Address	- - - - -
DHCP Client	00111NB1WIN2K(00-11-d8-57-cc-23) Clone

Static DHCP Client Lists 0 / 32 (Number / Total)

Host Name	IP Address	MAC Address

Dynamic DHCP Client Lists 2 / 100 (Number / Total)

Host Name	IP Address	MAC Address	Lease Time(Spare Time)
00111NB1WIN2K	10.53.13.103	00-11-d8-57-cc-23	6 days 18 hours 55 minutes 49 seconds
sd6-nb2	10.53.13.105	00-03-9d-73-32-f0	6 days 21 hours 56 minutes 11 seconds

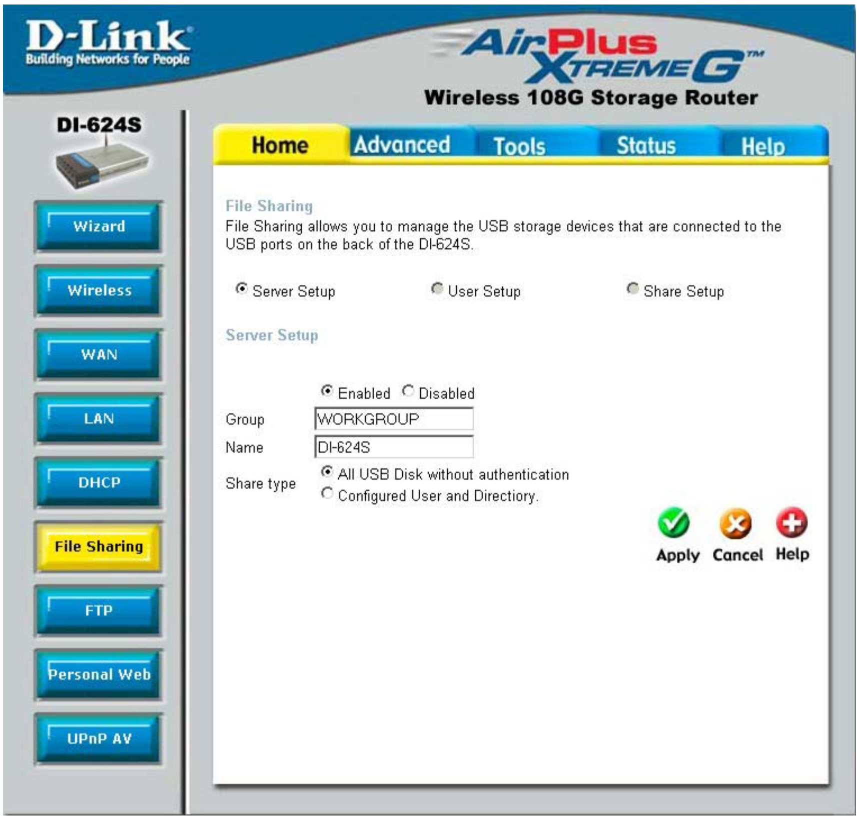
To setup DHCP for your LAN, first enable the Router as a DHCP server by clicking the corresponding **Enabled** radio button in the window above. The next step is to set a range of IP addresses that you wish to allot to the devices on your LAN by entering a **Starting IP Address** and an **Ending IP Address**. This may be in a range from 2 to 254 (192.168.0.2 – 192.168.0.254). Computers on your LAN will have an IP address within this range then automatically assigned to them. Finally, using the pull-down menu, choose the **Lease Time**, which is the time the Server will set for devices using DHCP to re-request an IP Address. Clients authorized for DHCP will be listed in the table at the bottom of the page. Click **Apply** to implement information set in this table. The DHCP Server is enabled by default.

DHCP may also be statically configured as well. This method allows the router to assign the same IP address information to a specific computer on the network, defined by its MAC address. This computer will get the same DHCP implemented IP address information every time the computer is turned on and this IP address will be specific to that computer's IP address on the local network. No other computer can be assigned this address. This is useful for computers on the LAN that are hosting applications such as HTTP or FTP. First, the user must enable the Static DHCP function by clicking the corresponding Enabled radio button. Next the user must enter the host name and the IP address for that computer by entering the last numbers into the space provided in the **IP Address** field. Next, the user is to enter the MAC address of the computer into the space provided. Click **Apply** to implement these static settings.

The **DHCP Client** field will allow users to Clone the settings from their computer that were learned from the DHCP server. Simply use the pull down menu to select the MAC address of the computer to be cloned and then click the Clone button. The settings from this computer will be implemented in the Static DHCP configuration area. Click **Apply** to implement these static settings.

Home > File Sharing

The following window and explanation describes how to set up your DI-624S as a file-sharing server. Using Samba technology, the router will be able to share files between computers with little regard to the operating system in use on a computer that has been given access to this file sharing service. The file sharing service is implemented using either or both of the two USB ports at the back of the router. You may attach any sort of USB file sharing device to these ports, such as a network attached storage device, a portable hard drive or even a USB flash memory stick. The USB ports are hot swappable so you can change storage devices at any time without powering off the router.



File Sharing

File Sharing allows you to manage the USB storage devices that are connected to the USB ports on the back of the DI-624S.

● Server Setup ○ User Setup ○ Share Setup

Server Setup

● Enabled ○ Disabled

Group: WORKGROUP

Name: DI-624S

Share type: ● All USB Disk without authentication
○ Configured User and Directory.

To set up the DI-624S as a file server, the user needs to configure four parts associated with this window. Each part has a corresponding radio button and when clicked, will open up to a new window to configure.

1. The **Server Setup** window is used to configure the settings for the DI-624S as a server.

2. The **User Setup** window is used to configure users who will want to access the information through the router.

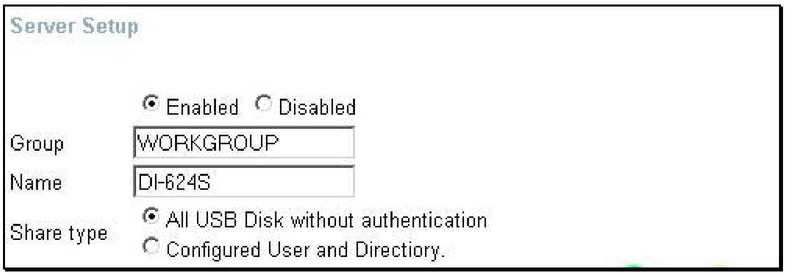
3. The **Group Setup** window is used to configure sets of users who have similar access rights into groups for better management.

4. Finally, the **Share Setup** window is used to define users and groups privileges when accessing the file share through the router.

See the following explanation for a better understand of how to configure the file-sharing feature of this device.

Advanced > File Sharing > Server Setup

The **Server Setup** window is used to configure the router to be a file-sharing device on the network.



Server Setup

	● Enabled ○ Disabled
Group	WORKGROUP
Name	DI-624S
Share type	● All USB Disk without authentication ○ Configured User and Directory.

Server Setup

Click the corresponding radio button if you wish to enable or disable the File Server function on the Router.

Group

Enter the name of the share group on the internal network with whom you wish to share files.

Name

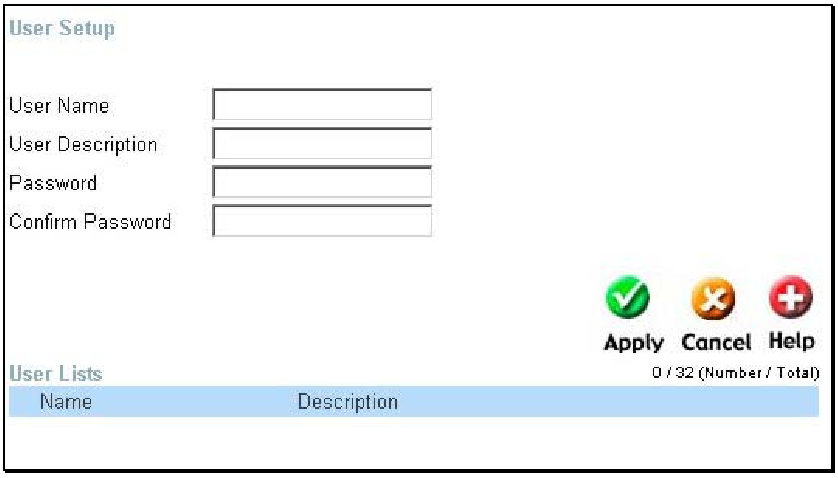
Enter the name of the device to be used as the file sharing server. As shown in the window above, this should be the DI-624S.

Share type

The administrator has two choices of places where to share files. If "**All USB Disk without authentication**" is chosen, the administrator will allow outside users access to USB devices attached to the router, without the need for authentication. "**Configured User and Directory**" will require outside users to be authenticated by the router before gaining access. The administrator will need to pre-define user names and passwords for these users attempting to access the shared files.

Advanced > File Sharing > User Setup

The **User Setup** window is used to configure users on the network to gain access to the router. To gain access to this window, the user must first choose the "Configured User and Directory" setting and click **Apply**. Once returned to the screen, the user may choose this option to be configured. Properly configured users will be listed in the User Lists table at the bottom of the window. Up to 32 users can be configured here. To edit the parameters for a configured user click its corresponding edit icon. To delete the user, click the corresponding delete icon.



User Setup

User Name	
User Description	
Password	
Confirm Password	

User Lists

0 / 32 (Number / Total)

Name	Description

User Name

Enter the name of the user to be added to the user group. This name must be identical to the one the user will input when asked for authorization by the router.

User Description

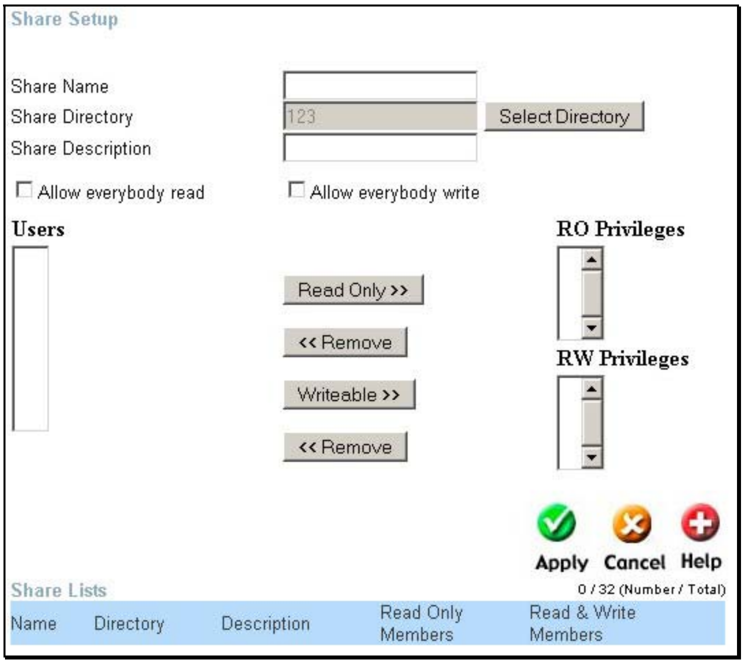
Enter a description of the user to identify that person to the administrator. This is an optional field.

Password / Confirm Password

Enter the password used to authorize this user on the router, then confirm that password in the following field. This password must be identical to the one the user will input when asked for authorization by the router.

Advanced > File Sharing > Share Setup

This window is used to configure directories to be shared through the router and to assign privileges to users and groups on the shared network. To set up the share system, configure the parameters below and click **Apply**. To assign privilege rights, highlight the group or user in the Users window and click the appropriate button to assign a privilege, which will move that name to one of the two privilege windows. Read Only will allow users to only read information in the file share. Writeable will allow users to both read and edit information in the file share. Share setup information will appear in the bottom of the screen in the Share Lists. To edit an entry, click the edit icon. To delete that entry, click the delete icon.



Share Setup

Share Name

Share Directory 123

Share Description

□ Allow everybody read □ Allow everybody write

Share Lists 0 / 32 (Number / Total)

Name	Directory	Description	Read Only Members	Read & Write Members

Share Name

Create a name of the file you wish to share. This name should be known to people on your share network.

Share Directory

Choose a directory on the file sharing system to be shared. This must be done by clicking the **Select Directory** button which will open a pop up window for the user to configure.

Share Description

This optional field is used to describe the file to be shared on the network.

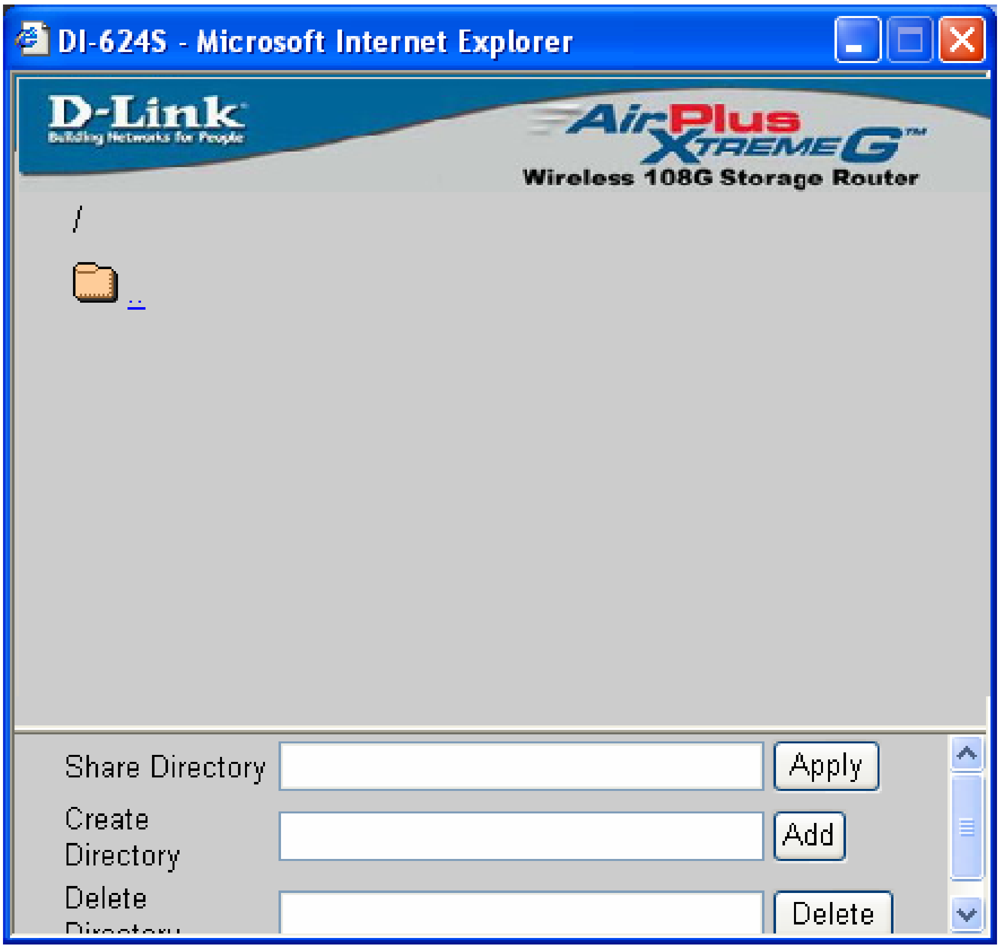
Allow everybody read

Click this box if the selected files will have read only permissions for users.

Allow everybody write

Click this box if you wish the selected file to have read and write permissions for users. Write permissions will allow users to alter files and documents in this folder.

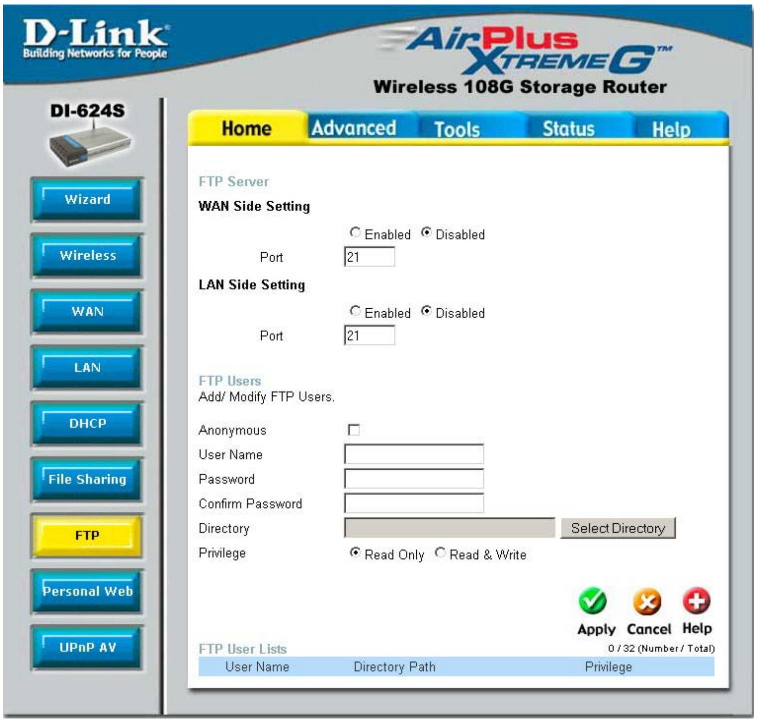
Select Directory Pop-Up Window


DI-624S - Microsoft Internet Explorer
D-Link
Building Networks for People
AirPlus XtremeG™
Wireless 108G Storage Router
/
..
Share Directory
Apply
Create Directory
Add
Delete Directory
Delete

This window will appear when the **Select Directory** button is clicked in the previous window. Using this window, the administrator can create directories for sharing on the network. To create a directory, enter a name of your choice in the **Create Directory** field and click **Add**. Once entered, it will appear in the window above. You may then click on the directory to enter it in the **Select Directory** and **Delete Directory** fields. Clicking **Apply** will enter the directory name into the **Share Directory** field in the **File Sharing** window where it can be given permissions for outside users. To delete the file, click the **Delete** button. *(Note: For the client implementation of this function, please see the user manual for the associated client PC)*

Home > FTP

Utilizing the USB ports and an external file sharing system, you may use this device with the FTP protocol. FTP or File Transfer Protocol allows computer users running various operating systems to share files. This feature is very similar to the file sharing feature described in the previous section both in implementation and usage. The FTP service may be enabled for the WAN (external), LAN (internal) or both networks. The common virtual port number for FTP is 21. To set up your router to be a FTP server, configure the following parameters and click Apply. The Select directory button will open a pop up window, identical to the Select Directory Pop-up window described in the previous section. *(Note: For the client implementation of this function, please see the user manual for the associated client PC)*



FTP Server

WAN Side Setting

○ Enabled ● Disabled

Port 21

LAN Side Setting

○ Enabled ● Disabled

Port 21

FTP Users

Add/ Modify FTP Users.

Anonymous □

User Name

Password

Confirm Password

Directory [Select Directory]

Privilege ● Read Only ○ Read & Write

FTP User Lists 0 / 32 (Number / Total)

User Name	Directory Path	Privilege

WAN Side Setting

Click the **Enabled** radio button to open the file sharing system on the WAN. The user may also enter a virtual port number for which to use this protocol. The common port number for FTP is 21.

LAN Side Setting

Click the **Enabled** radio button to open the file sharing system on the LAN. The user may also enter a virtual Port number for which to use this protocol. The common port number for FTP is 21.

User Name

Enter the name of the user who will be uploading files through your router. This name must be exactly entered by the outside user to access the shared files.

Password / Confirm Password

Enter the password used to authorize this user on the router, then confirm that password in the following field. This password must be identical to the one the user will input when asked for authorization by the router.

Directory

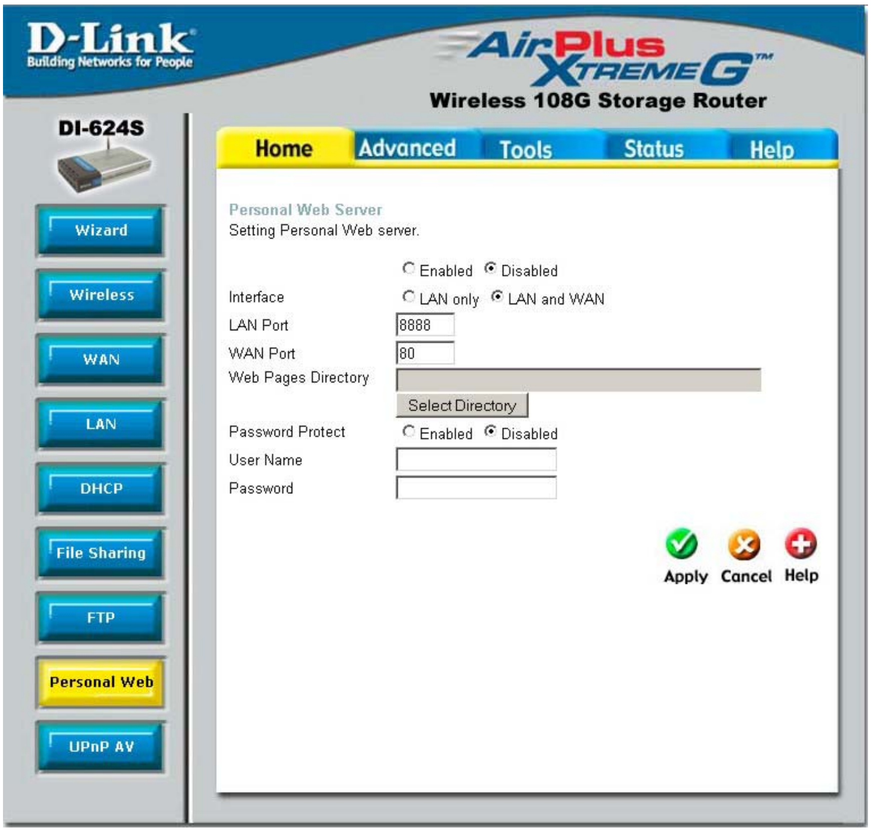
Choose a directory on the file sharing system to be shared through this router. This must be done by clicking the **Select Directory** button, which will open a pop up window for the user to configure.

Privilege

Choose the permissions to be set for the user. List Only will allow the user to only view the list of files set for sharing. **Read Only** will allow the user to download but only read files on the share server. **Read & Write** will allow the user to download, read and alter files on the server.

Home > Personal Web

The Personal Web screen will allow the user to set up a web page for guests to use for accessing stored files on one of the router's USB ports. In order for this to properly function, the administrator must have an HTML documents stored on a USB-connected memory device. Through this HTML page, guests can access files on the USB storage device, just as they could on an Internet WWW page. Just complete the following fields to set up your Personal Web server.



Personal Web Server
Setting Personal Web server.

○ Enabled ● Disabled

Interface ○ LAN only ● LAN and WAN

LAN Port 8888

WAN Port 80

Web Pages Directory

Select Directory

Password Protect ○ Enabled ● Disabled

User Name

Password

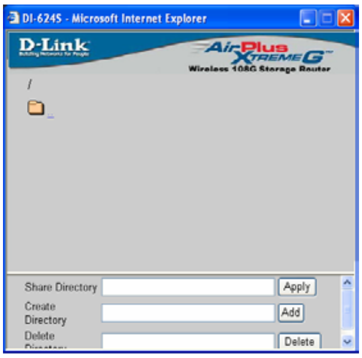
Personal Web Server — Click the Enabled radio button to enable the DI-624S as a Personal Web server.

Interface — Choose the interface on which to set up your Personal web server. LAN only will allow users on the LAN (internal) to access this HTML interface. LAN and WAN will allow all users, internal and external (Internet), to access this HTML interface.

LAN Port — Enter the virtual port on the LAN through which this Personal Web file can be accessed.

WAN Port — Enter the virtual port on the WAN through which this Personal Web file can be accessed.

Web Pages Directory — Enter the directory, or use the **Select Directory** pop-up window to choose a web-page, configured on one of the USB port devices to be shared through HTML. The **Select Directory** pop-up window will produce a new screen to use and configure to complete this task.


DI-624S - Microsoft Internet Explorer
D-Link
AirPlus Xtreme G
Wireless 108G Storage Router
/
Apply
Add
Delete

Share Directory

Create Directory

Delete Directory

Password Protect — Select **Enabled** to protect entry to this web page through the use of a username and a password.

User Name

Enter the User Name you wish to allot this Personal Web page. This is the **User Name**, along with the **Password** in the next field, that will be required to access the Personal Web page on a USB storage device connected to the Router.

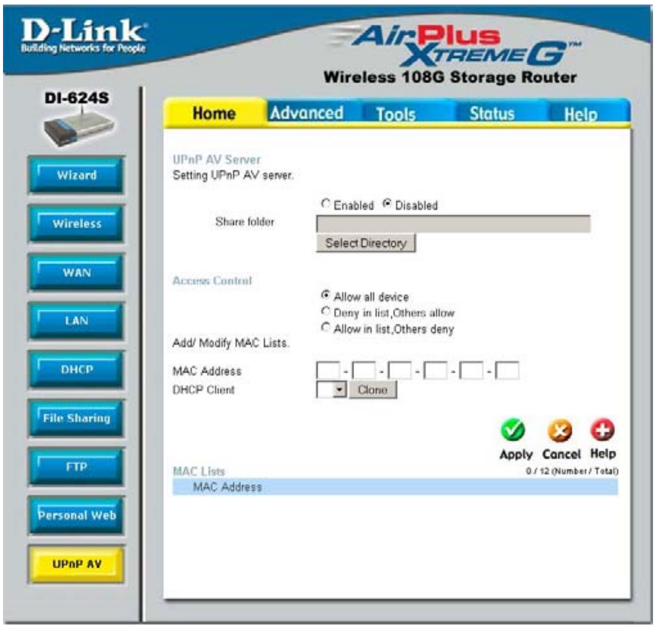
Password

Enter the Password you wish to allot this Personal Web page. This is the **Password**, along with the **User Name** in the previous field, that will be required to access the **Personal Web** page on a USB storage device connected to the Router.

Click Apply to set these changes to the memory of the router.

Home > UPnP AV

The UPnP (Universal Plug and Play) AV screen will allow the administrator to share audio and video files for viewing or listening over the network. These files, which would be stored on an external file-sharing device attached to one of the USB ports, can be added or adjusted by using the Select Directory Pop-up window previously described. No username or password will be necessary to view these files, yet clients who want to view or listen to these files must be running the UPnP AV protocol on their computer. The user may add up to 12 devices for sharing AV files through this router. External file sharing devices may be added to the UPnP function by entering its MAC address and clicking Apply. These entries will be listed in the MAC List table at the bottom of the screen. *(Note: For the client implementation of this function, please see the user manual for the associated client PC)*



UPnP AV Server
Setting UPnP AV server.

○ Enabled ● Disabled

Share folder [ ]
Select Directory

Access Control

● Allow all device
○ Deny in list,Others allow
○ Allow in list,Others deny

Add/ Modify MAC Lists.

MAC Address [ ] - [ ] - [ ] - [ ] - [ ] - [ ]
DHCP Client [▾] Clone

MAC Lists 0 / 12 (Number / Total)

MAC Address

UPnP AV Server
Click Enabled to enable the DI-624S as a UPnP server.

Interface
Choose an interface on which to make AV files accessible. Choosing LAN only will restrict viewing and listening to clients on the local network. Choosing LAN and WAN will open the AV files to the entire network.

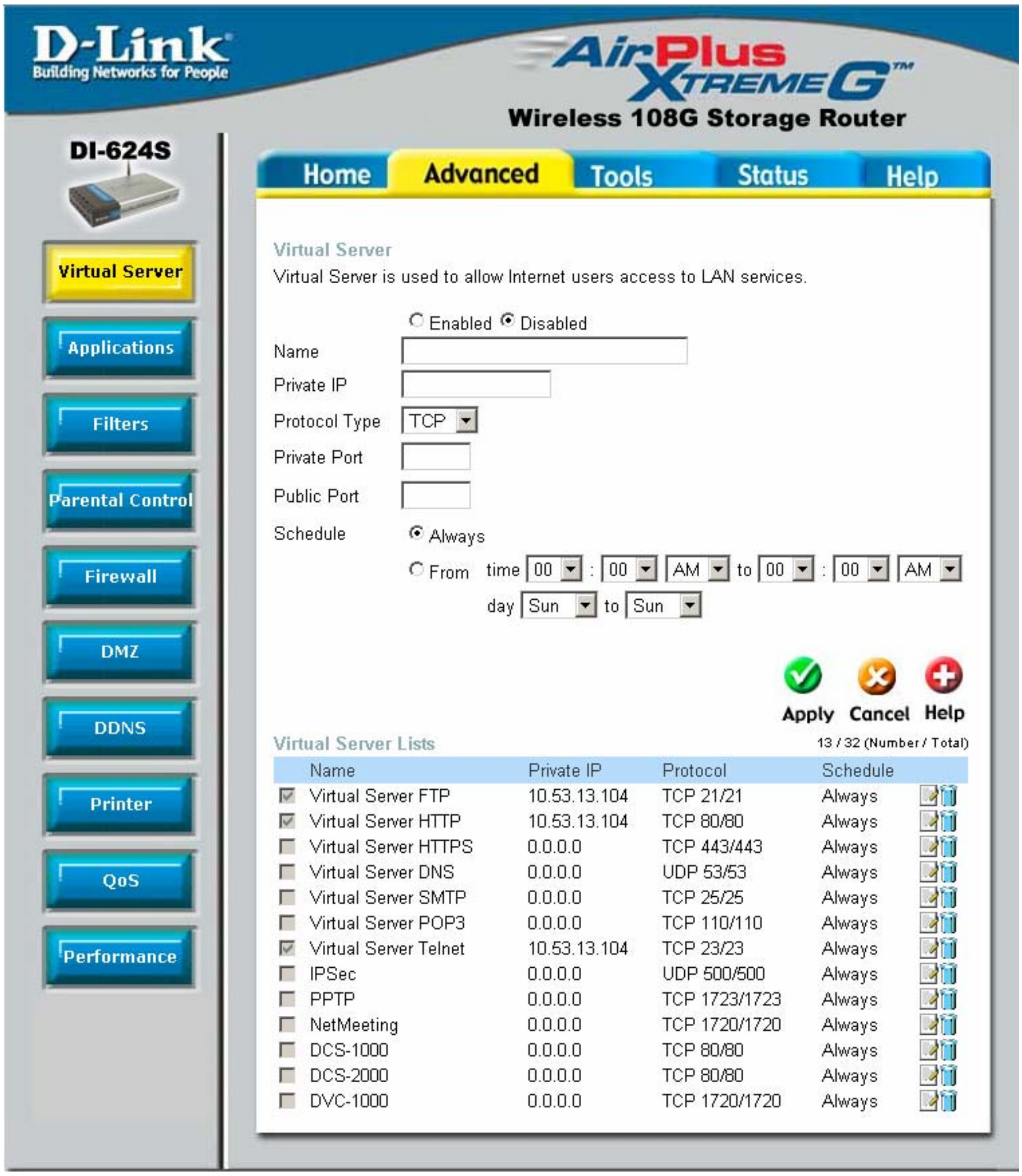
Share folder
Choose a directory on the file sharing system to be open for viewing or listening. This must be done by clicking the **Select Directory** button which will open the **Select Directory** pop-up window for the user to configure.

Access Control
This field is used to allow or deny external file sharing systems usage on the network. **Allow all device** will allow any device connected to the USB ports to be accessed. **Deny in list, Others allow** will deny devices in the list from being accessed. **Allow in list, Others deny** will permit access to only the listed devices.

MAC Address
Enter the MAC address of the device that will be used for AV usage through this router. Click **Apply** to set this address in the MAC List at the bottom of the screen.

DHCP client
Use the pull-down menu to choose the DHCP client or click **Clone** to clone the MAC address of the device running DHCP. This function will assign IP addresses to devices running DHCP so they can have access to or denied access from UPnP devices on the LAN, depending on the choice made in the Access Control field.

Advanced > Virtual Server



Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

○ Enabled ● Disabled

Name

Private IP

Protocol Type TCP

Private Port

Public Port

Schedule ● Always

○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

Virtual Server Lists 13 / 32 (Number / Total)

	Name	Private IP	Protocol	Schedule
☑	Virtual Server FTP	10.53.13.104	TCP 21/21	Always
☑	Virtual Server HTTP	10.53.13.104	TCP 80/80	Always
□	Virtual Server HTTPS	0.0.0.0	TCP 443/443	Always
□	Virtual Server DNS	0.0.0.0	UDP 53/53	Always
□	Virtual Server SMTP	0.0.0.0	TCP 25/25	Always
□	Virtual Server POP3	0.0.0.0	TCP 110/110	Always
☑	Virtual Server Telnet	10.53.13.104	TCP 23/23	Always
□	IPSec	0.0.0.0	UDP 500/500	Always
□	PPTP	0.0.0.0	TCP 1723/1723	Always
□	NetMeeting	0.0.0.0	TCP 1720/1720	Always
□	DCS-1000	0.0.0.0	TCP 80/80	Always
□	DCS-2000	0.0.0.0	TCP 80/80	Always
□	DVC-1000	0.0.0.0	TCP 1720/1720	Always

To view the following window, click on the **Advanced** tab at the top of the window and then click the **Virtual Server** button to the left. The **Virtual Server** will allow remote users access to various services outside of their LAN through a public IP address, such as FTP (File Transfer Protocol) or HTTPS (Secure Web). After configuring the Router for these features, the Router will redirect these external services to an appropriate server on the users LAN. The Router has 13 pre-configured external services already set, but the user may add alternate services using the window below. The Virtual Servers listed in the following window are:

- FTP – **F**ile **T**ransfer **P**rotocol, used to transfer large files over the Internet
- HTTP – **H**yper**T**ext **T**ransfer **P**rotocol, the basic protocol of the World Wide Web
- HTTPS – **H**yper**T**ext **T**ransfer **P**rotocol Secure, the basic protocol of the World Wide Web with added security provided by the Secure Shell feature (SSH)
- DNS – **D**omain **N**ame **S**erver, a server that translates website addresses into IP addresses

- SMTP – **S**imple **M**ail **T**ransfer **P**rotocol, used to transmit e-mail messages between parties
- POP3 – **P**ost **O**ffice **P**rotocol version 3, used to retrieve e-mail from a mail server
- Telnet – A terminal emulation program used for remote configuration
- IPSec – **IP Sec**urity, used for a secure transfer of information over the network. If one end of the transmission is using IPSec, so must the other end
- PPTP – **P**oint to **P**oint **T**unneling **P**rotocol, used to transfer information securely between VPNs (Virtual Private Routers)
- NetMeeting – An application that allows teleconferences over the Internet
- DCS –1000 – A D-Link internet camera used for security monitoring
- DCS –2000 – A D-Link internet camera used for security monitoring
- DVC –1000 – A D-Link VideoPhone used for video conferencing

These external services may be modified by clicking its corresponding edit icon, or they may be deleted by clicking the corresponding delete icon. Though there are seven fields available to configure the Virtual Server, in most cases, only the IP address of the Virtual Server will be needed for implementation. To enable an already existing Virtual Server, click its corresponding edit button, configure the appropriate fields listed below and set the **Status** fields to **Enabled** by clicking the radio button. To configure other virtual servers for the Router, configure the following fields and click **Apply**.

Virtual Server
Click the radio button to enable or disable the selected Virtual Server.

Name
Enter the name of the Virtual Server. If you have chosen a pre-configured Virtual Server from the list, its name will appear in this field.

Private IP
Enter the IP address of the Virtual Server.

Protocol Type
The protocol type used for the Virtual Server. The user may select **TCP**, **UDP** or **Both**, depending on the type of Virtual Server implemented.

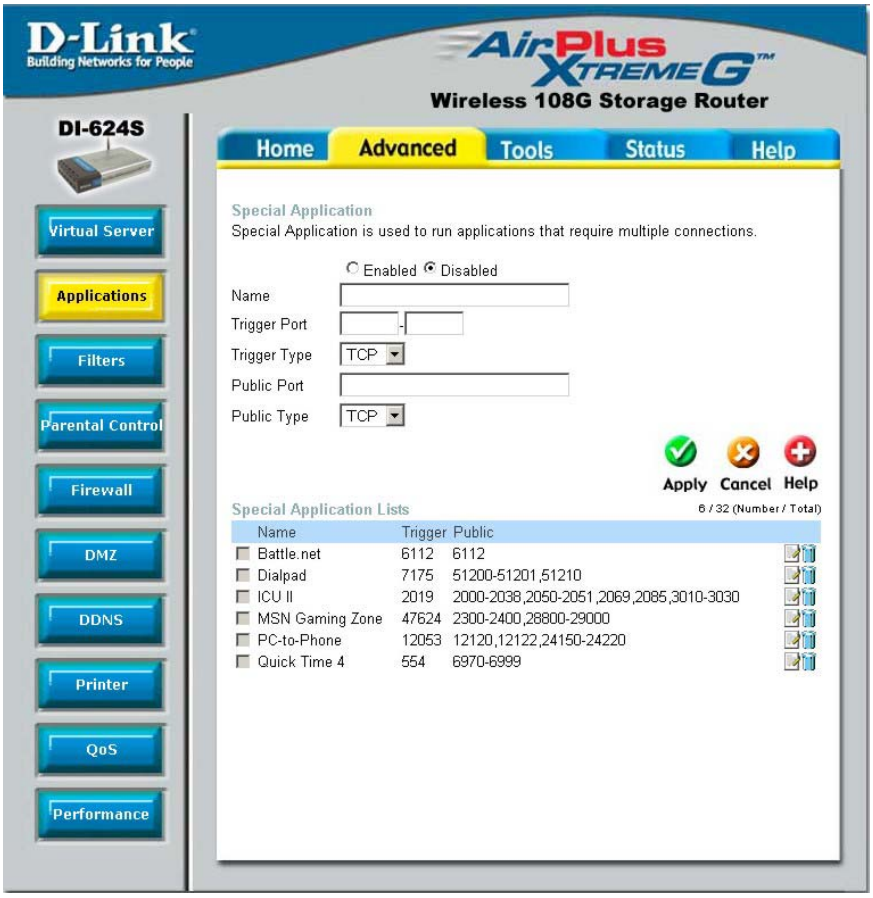
Private Port
Enter the port number of the Virtual Server's computer. Existing Virtual Servers listed already have their well-known port number listed yet this may need to be changed in certain circumstances.

Public Port
Enter the port number of the device on the WAN side of the network that will be accessing the Virtual Server currently being configured. Commonly, this port number is identical to the Private Port number. Existing Virtual Servers listed already have their well-known port number listed yet this may need to be changed in certain circumstances.

Schedule
Configure the time schedule you wish these Virtual Servers to be accessed. Clicking the **Always** radio button will allow access to these servers at any time. The user may set a strict time period by clicking the **From** radio button and configuring a time period for access.

Advanced > Applications

The **Applications** window is used to configure applications that require multiple connections, such as Internet Telephony, video conferencing and Internet gaming. The following window lists six Special Applications that commonly use more than one connection. To configure one of these applications, click its corresponding edit icon and then modify the fields listed below the following figure and then clicking the **Enabled** radio button. The user may add a new application by modifying the fields listed and then clicking the **Enabled** radio button. New entries will be listed at the bottom of the page in the **Special Application List**. To delete a particular application, click its corresponding delete icon.



Special Application

Special Application is used to run applications that require multiple connections.

○ Enabled ● Disabled

Name

Trigger Port -

Trigger Type TCP

Public Port

Public Type TCP

Special Application Lists

6 / 32 (Number / Total)

	Name	Trigger	Public
□	Battle.net	6112	6112
□	Dialpad	7175	51200-51201,51210
□	ICU II	2019	2000-2038,2050-2051,2069,2085,3010-3030
□	MSN Gaming Zone	47624	2300-2400,28800-29000
□	PC-to-Phone	12053	12120,12122,24150-24220
□	Quick Time 4	554	6970-6999

Applications

Click the appropriate corresponding radio button to enable or disable the Applications feature.

Trigger Port

Enter the port associated with the **Name** entered above. This is the port that will "trigger" this application to accept multiple connections.

Trigger Type

Choose the protocol type of the Special Application from the pull-down menu. The choices available to the user are **TCP**, **UDP** or **Both**.

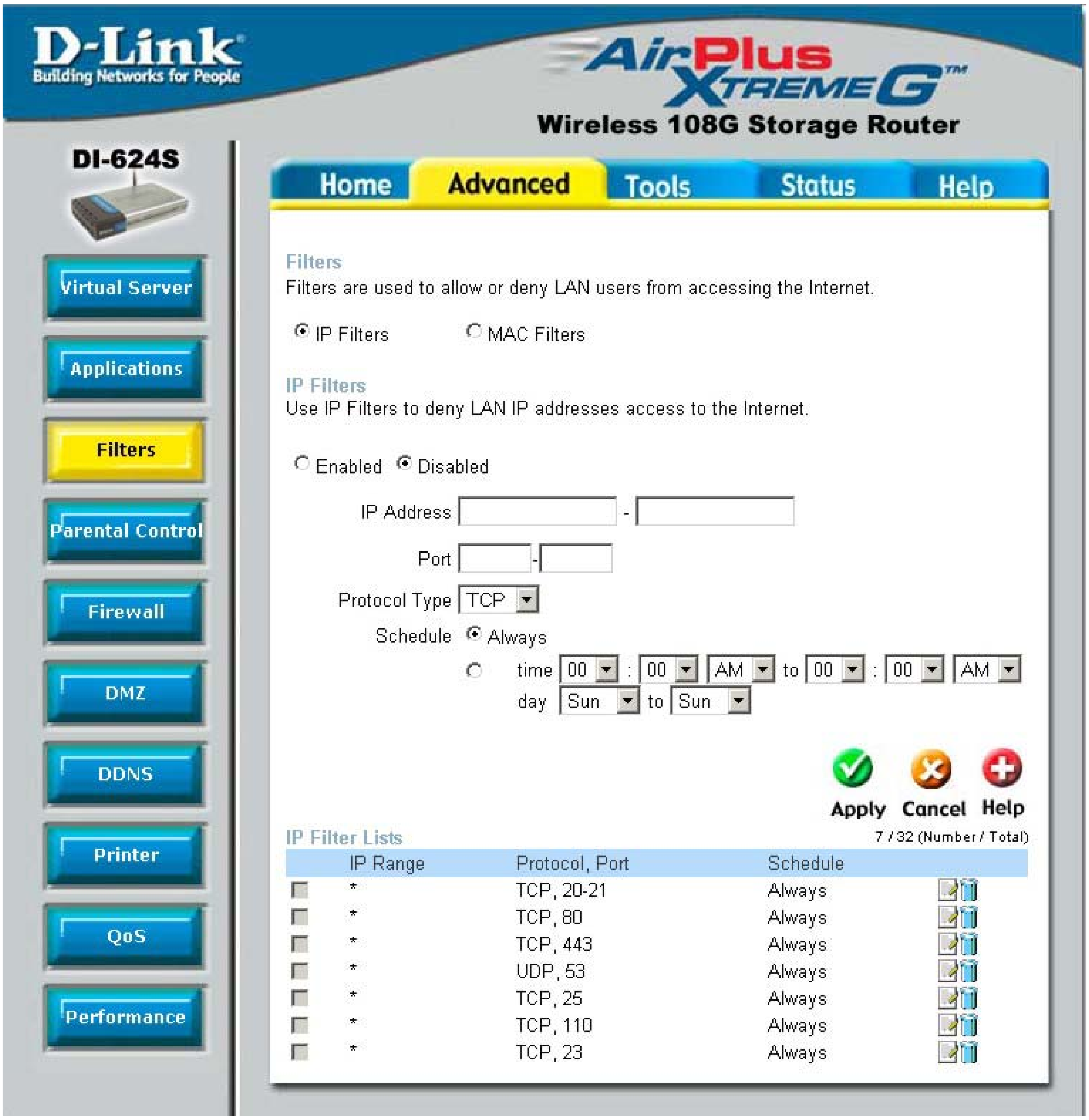
Public Port

Enter the port number on the WAN side of the connection that will access the Special Application. This field will accept a port, multiple ports which are to be separated by a comma upon entry, or a range of ports, which are to be separated by a dash.

Public Type

This entry will trigger the public port on the WAN side of the connection for the specified application. The choices available to the user are **TCP**, **UDP** or **Both**.

Advanced > Filters



Filters

Filters are used to allow or deny LAN users from accessing the Internet.

● IP Filters ○ MAC Filters

IP Filters

Use IP Filters to deny LAN IP addresses access to the Internet.

○ Enabled ● Disabled

IP Address ____ - ____

Port ____ - ____

Protocol Type TCP

Schedule ● Always

○ time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

IP Filter Lists 7 / 32 (Number / Total)

	IP Range	Protocol, Port	Schedule
□	*	TCP, 20-21	Always
□	*	TCP, 80	Always
□	*	TCP, 443	Always
□	*	UDP, 53	Always
□	*	TCP, 25	Always
□	*	TCP, 110	Always
□	*	TCP, 23	Always

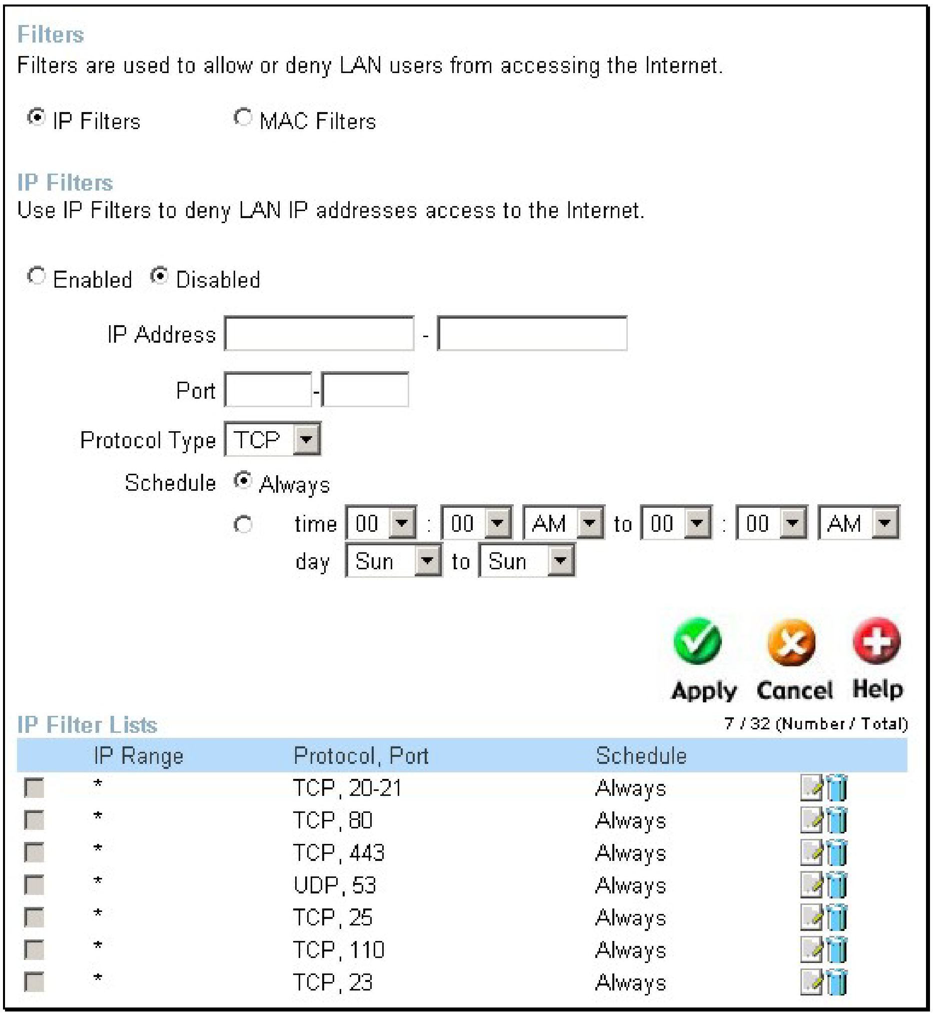
Packet filtering is a basic security measure that should be used on any network that is exposed to a security risk. A packet filter system examines data packets and scrutinizes them in order to control network access. Filtering rules determine whether packets are passed through the Router from either side of the gateway. The rules are created and controlled by the network administrator and can be precisely defined. These rules are used to block access to the LAN from outside the network and/or to deny access to the WAN from within the network. The Router uses filtering rules to examine data packet headers for specific information. Packets passing through the Router that do not meet the criteria specified by the rule set are dropped.

Effective implementation of packet filtering requires detailed knowledge of network services and communication protocols. An overly complicated filtering scheme can adversely affect the Router’s performance, while an inadequate set of rules may needlessly compromise security.

This Router has two fields to configure for filtering which are **IP Filters** and **MAC Filters.**

Advanced > Filters > IP Filters

This window will aid the use in configuring filters for IP addresses. This will deny specified LAN IP addresses or specific ports associated with these LAN IP address from accessing the Internet. Well known ports have already been previously set in the **IP Filters List** and can be modified by clicking their corresponding edit icon, and simple adding an IP address to the configuration. To access this screen, click the **Advanced** tab along the top of the configuration window and then the **Filters** tab to the left hand side.



Filters

Filters are used to allow or deny LAN users from accessing the Internet.

● IP Filters ○ MAC Filters

IP Filters

Use IP Filters to deny LAN IP addresses access to the Internet.

○ Enabled ● Disabled

IP Address ____ - ____

Port ____ - ____

Protocol Type: TCP

Schedule: ● Always

○ time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

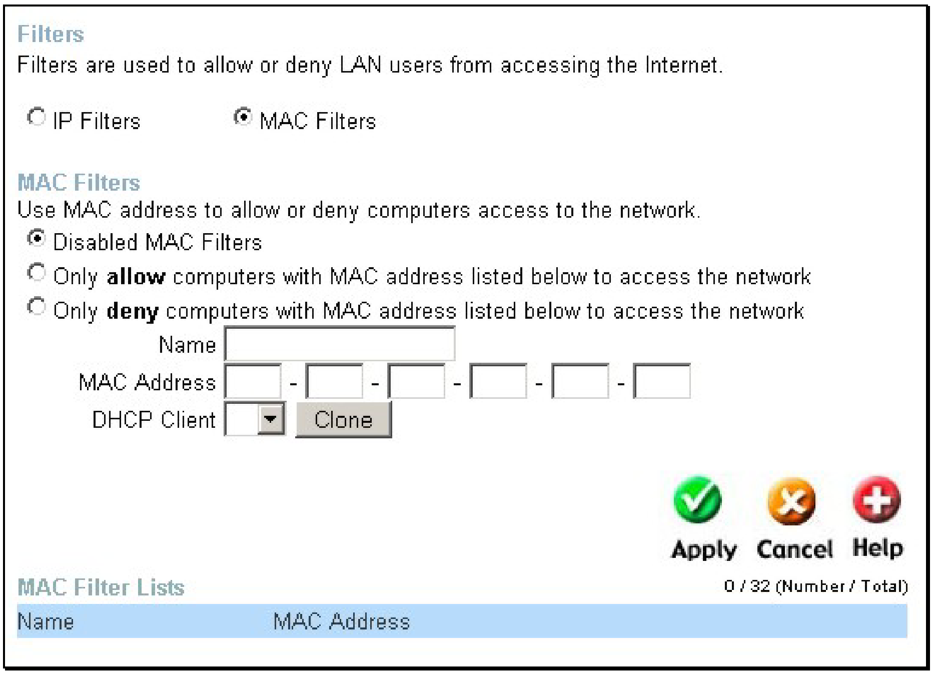
IP Filter Lists — 7 / 32 (Number / Total)

	IP Range	Protocol, Port	Schedule	
□	*	TCP, 20-21	Always	
□	*	TCP, 80	Always	
□	*	TCP, 443	Always	
□	*	UDP, 53	Always	
□	*	TCP, 25	Always	
□	*	TCP, 110	Always	
□	*	TCP, 23	Always	

IP Filters	Choose whether to enable or disable this configuration for IP filtering.
IP Address	An IP address or range of IP addresses that will be denied access to the Internet.
Port	A port or range of ports that will be denied access to the Internet. If no port is entered, all ports in this IP range will be denied access to the Internet.
Protocol Type	The protocol associated with this IP filter. The user may choose between **TCP**, **UDP** or **Both**.
Schedule	The user may configure time intervals that these IP filters will become active. Clicking the **Always** radio button will not allow access to these IP filters at any time. The user may set a strict time period by clicking the **From** radio button and configuring a time period to deny these IP addresses from accessing the Internet.

Advanced > Filters > MAC Filters

All computers are uniquely identified by their MAC (Media Access Control) address. The following window will allow users to deny computers access to the Internet or only allow certain computers access to the Internet, based on their MAC address. To access this screen, click the **Advanced** tab along the top of the configuration window, then the **Filters** tab to the left hand side and finally click the corresponding radio button for **MAC Filters**.



Filters

Filters are used to allow or deny LAN users from accessing the Internet.

○ IP Filters ● MAC Filters

MAC Filters

Use MAC address to allow or deny computers access to the network.

● Disabled 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

MAC Address - - - - -

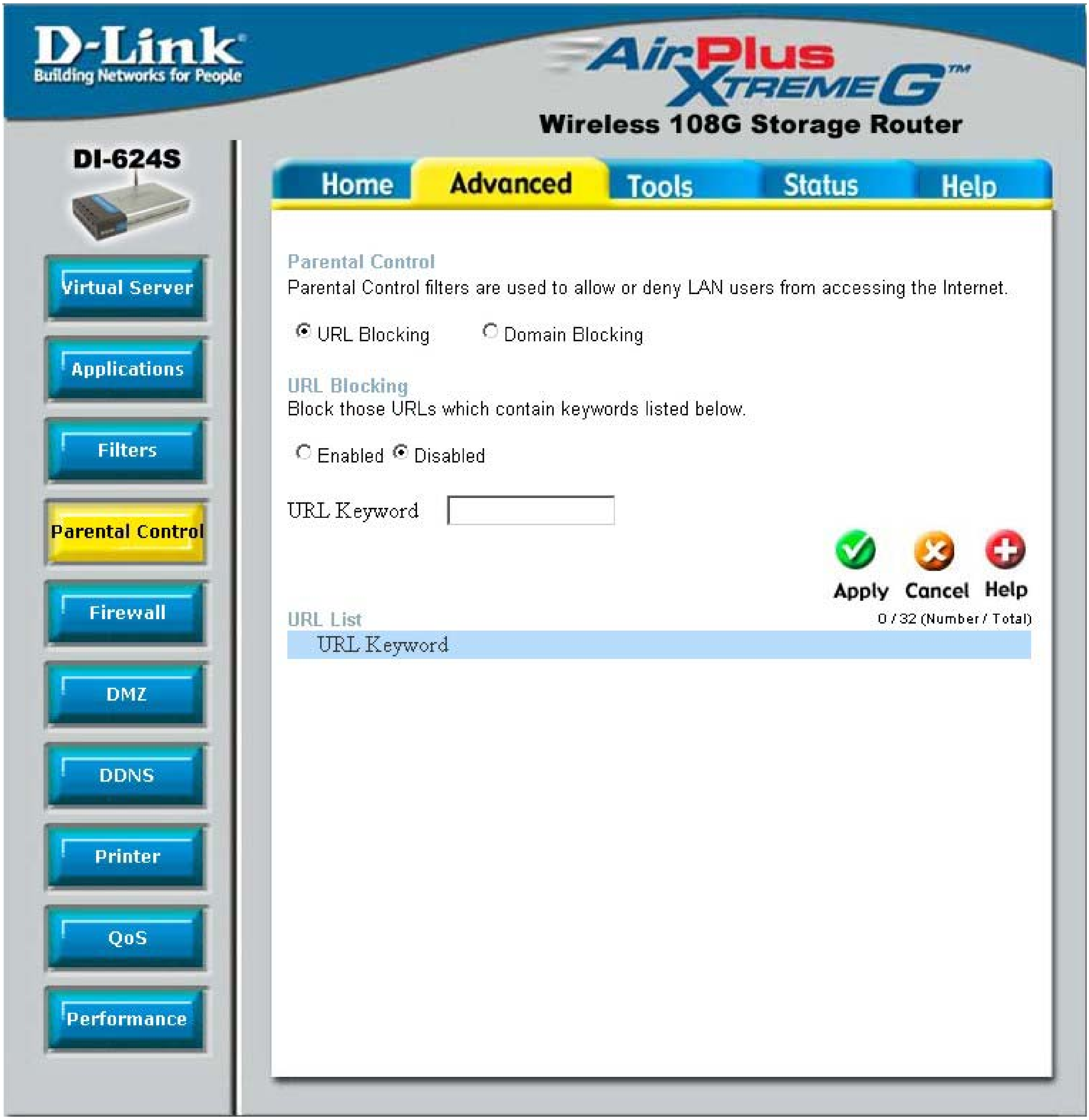
DHCP Client

MAC Filter Lists 0 / 32 (Number / Total)

Name	MAC Address

Disabled MAC Filters	Click this radio button to disable MAC filtering on the Router.
Only Allow	Click this radio button if you wish to allow specific computers access to the network, based on MAC address.
Only Deny	Click this radio button if you wish to deny specific computers access to the network, based on MAC address.
Name	A Name defined by the user to identify this MAC address filter setting.
MAC Address	Enter the MAC address to be filtered.
DHCP Client	This field will display the DHCP client's host name and MAC address here. You may clone this MAC address by simply clicking the **Clone** button. The cloned entry will be displayed in the **MAC Filters List**.

Advanced > Parental Control



Parental Control

Parental Control filters are used to allow or deny LAN users from accessing the Internet.

● URL Blocking ○ Domain Blocking

URL Blocking

Block those URLs which contain keywords listed below.

○ Enabled ● Disabled

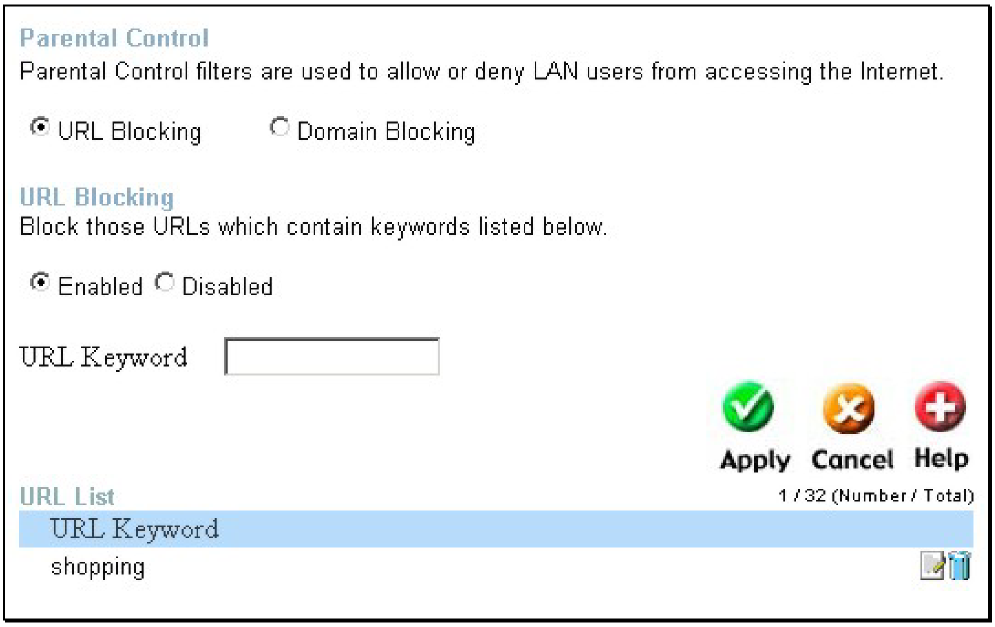
URL Keyword

URL List 0 / 32 (Number / Total)

URL Keyword

Parental Control is used to deny access to certain websites and domains on the Internet. This is beneficial for users who want to deny computers on the LAN entry to websites, especially for parents who want to guard against questionable content for their children's computers. The administrator has two choices in this screen, URL blocking (websites) and Domain Blocking. See the following for more information on Parental control and its implementation.

Advanced > Parental Control > URL Blocking



Parental Control

Parental Control filters are used to allow or deny LAN users from accessing the Internet.

● URL Blocking ○ Domain Blocking

URL Blocking

Block those URLs which contain keywords listed below.

● Enabled ○ Disabled

URL Keyword

URL List

1 / 32 (Number / Total)

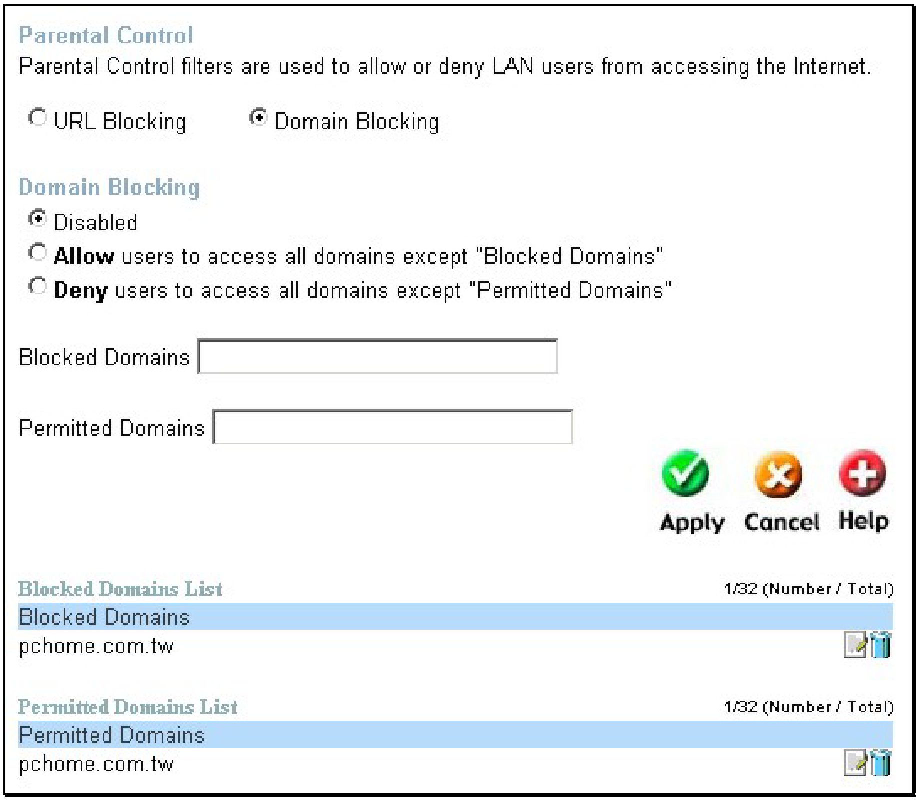
URL Keyword
shopping

URL or Uniform Resource Locator is a specially formatted text string that uniquely defines an Internet website. This window will allow users to block computers on the LAN from accessing certain URLs. This may be accomplished by simply entering the URL to be blocked in the **URL Address** field. The user may also use this field to block certain websites by entering a keyword into the **URL Address** field. So, if any website's URL contains this word, it will automatically be denied access to users on the LAN.

For example, if you wish to block users from accessing shopping websites, enter the keyword "shopping into the URL Address field. Then website having "shopping" in their URL (such as http://www.yahoo.com/shopping/stores.html or http://www.msn/search/shopping-spree.html) will be denied from computers on the LAN. This feature may be beneficial to parents wanting to stop their kids from accessing certain websites or for companies who want their employees to stop surfing the Internet on company time.

To configure this screen for URL blocking, enter the website's address or a keyword into the **URL Address** field and click the radio button for **Enabled URL Blocking** and then click **Apply** to save this configuration into the Routers memory. Configured URL blocking entries will be displayed in the URLs Blocking List at the bottom of the screen. To modify a URL blocking entry in the list, click its corresponding edit icon. To delete a URL blocking entry in the list, click its corresponding delete icon.

Advanced > Parental Control > Domain Blocking



Parental Control

Parental Control filters are used to allow or deny LAN users from accessing the Internet.

○ URL Blocking ● Domain Blocking

Domain Blocking

● Disabled

○ **Allow** users to access all domains except "Blocked Domains"

○ **Deny** users to access all domains except "Permitted Domains"

Blocked Domains

Permitted Domains

Blocked Domains List 1/32 (Number / Total)

Blocked Domains
pchome.com.tw

Permitted Domains List 1/32 (Number / Total)

Permitted Domains
pchome.com.tw

Domain blocking is a method of denying or allowing computers on the LAN access to specific domains on the Internet. There are two available methods available to the user to institute Domain blocking on the router. Under the **Domain Blocking** header in the screen pictured above, the user has three choices, one of which is to disable Domain blocking. The second choice is **Allow users to access all domains except "Blocked Domains"**. This option is for users who wish to block certain domains from being accessed by local users on the LAN, but leave the rest open for use. To specify which Domains you wish to exclude from use by computers on the LAN, enter the Domain's URL (ex. yahoo.com, google.com) into the **Blocked Domains** field and then click **Apply**. The blocked entry will appear in the **Blocked Domains List** at the bottom of the screen. To modify an entry in this list, click its corresponding edit icon. To delete an entry from this list, click its corresponding delete icon.

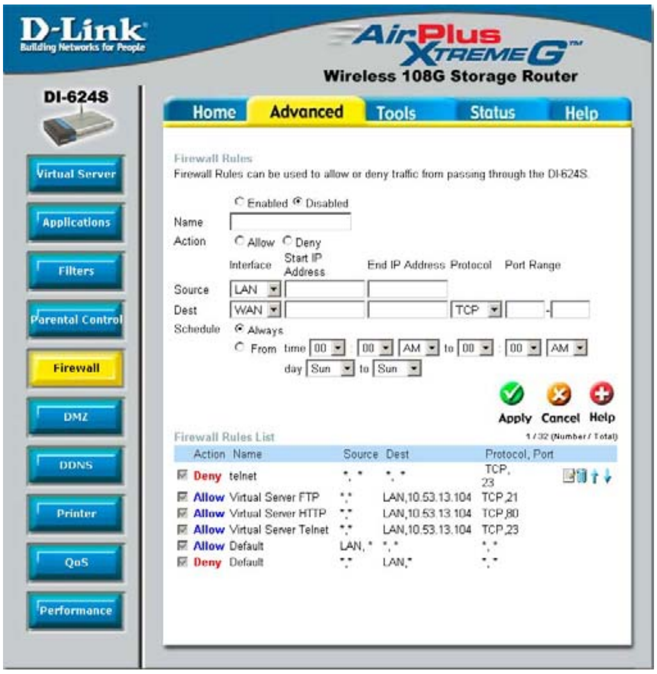
For users wishing to allow computers on the LAN access to only specified domains, choose option three under the Domain Blocking heading, **Deny users to access all domains except "Permitted Domains"**. To specify which domains you wish to include for this option, enter the Domain's URL (ex. yahoo.com, google.com) into the **Permitted Domains** field and then click **Apply**. The permitted entry will appear in the **Permitted Domains List** at the bottom of the screen. To modify an entry in this list, click its corresponding edit icon. To delete an entry from this list, click its corresponding delete icon.

NOTE: *Choosing the* ***Deny users to access all domains except "Permitted Domains"*** *option will block access to all other Internet traffic except the Domains specified. Be careful not to misuse this option or users on the LAN will have difficulty accessing network resources.*

Advanced > Firewall

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

To configure rules for the firewall, modify the following fields and click **Apply** to set the rule in the Routers memory. Newly configured firewall rules will be displayed in the **Firewall Rules List** at the bottom of the page. To modify an entry in this list, click its corresponding edit icon. To delete an entry from this list, click its corresponding delete icon.



Firewall Rules

Firewall Rules can be used to allow or deny traffic from passing through the DI-624S.

○ Enabled ● Disabled

Name

Action ○ Allow ○ Deny

	Interface	Start IP Address	End IP Address	Protocol	Port Range
Source	LAN				
Dest	WAN			TCP	-

Schedule ● Always

○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

Firewall Rules List

1 / 32 (Number / Total)

	Action	Name	Source	Dest	Protocol, Port
☑	Deny	telnet	*, *	*, *	TCP, 23
☑	Allow	Virtual Server FTP	*,*	LAN,10.53.13.104	TCP,21
☑	Allow	Virtual Server HTTP	*,*	LAN,10.53.13.104	TCP,80
☑	Allow	Virtual Server Telnet	*,*	LAN,10.53.13.104	TCP,23
☑	Allow	Default	LAN, *	*, *	*, *
☑	Deny	Default	*,*	LAN,*	*, *

Firewall

Click the corresponding radio button if you wish to enable or disable the firewall function on the Router.

Name

Enter a name that will define the firewall rule to be configured. This entry is dependant on how the user wishes to classify this rule.

Action

Click whether to Allow or Deny traffic to pass through the Router by checking the corresponding radio button. Users may configure only specific traffic to pass through the router by checking **Allow** or users may stop specific traffic from passing through the Router by checking **Deny**.

Source

Enter the IP address or range of IP addresses that you wish to block or allow to pass through the router. The Source may be identified on the LAN side, the WAN side or both by using the pull-down menu for the Interface heading.

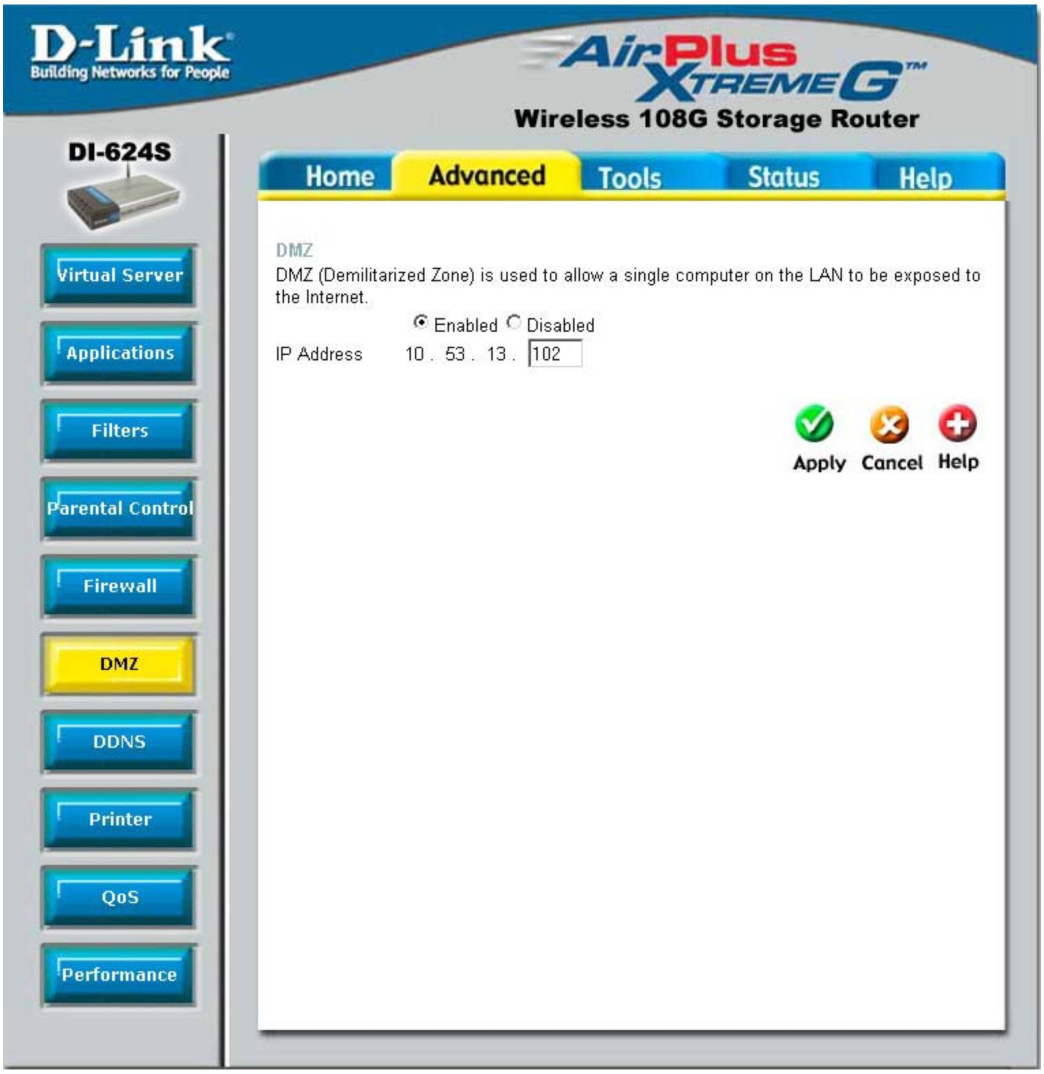
Destination

Enter the IP address or range of IP addresses that you wish to deny or allow access to the Internet. The **Destination** may be identified on the **LAN** side, the **WAN** side or **Both** by using the pull-down menu for the Interface heading. The type of protocol may also be chosen by using the pull-down menu. The user may choose between **TCP**, **UDP, ICMP** or (*) **Any**. The user may also select a range of ports of the destination IP addresses by entering the range under the **Port Range** heading.

Schedule

Clicking **Always** will set the firewall permanently, unless changed by the user. Alternately, the user may set up a time schedule to implement the firewall, on a week-to-week basis by clicking the **From** radio button and setting the appropriate times to begin and end the firewall function.

Advanced > DMZ



DMZ

DMZ (Demilitarized Zone) is used to allow a single computer on the LAN to be exposed to the Internet.

● Enabled ○ Disabled

IP Address 10 . 53 . 13 . 102

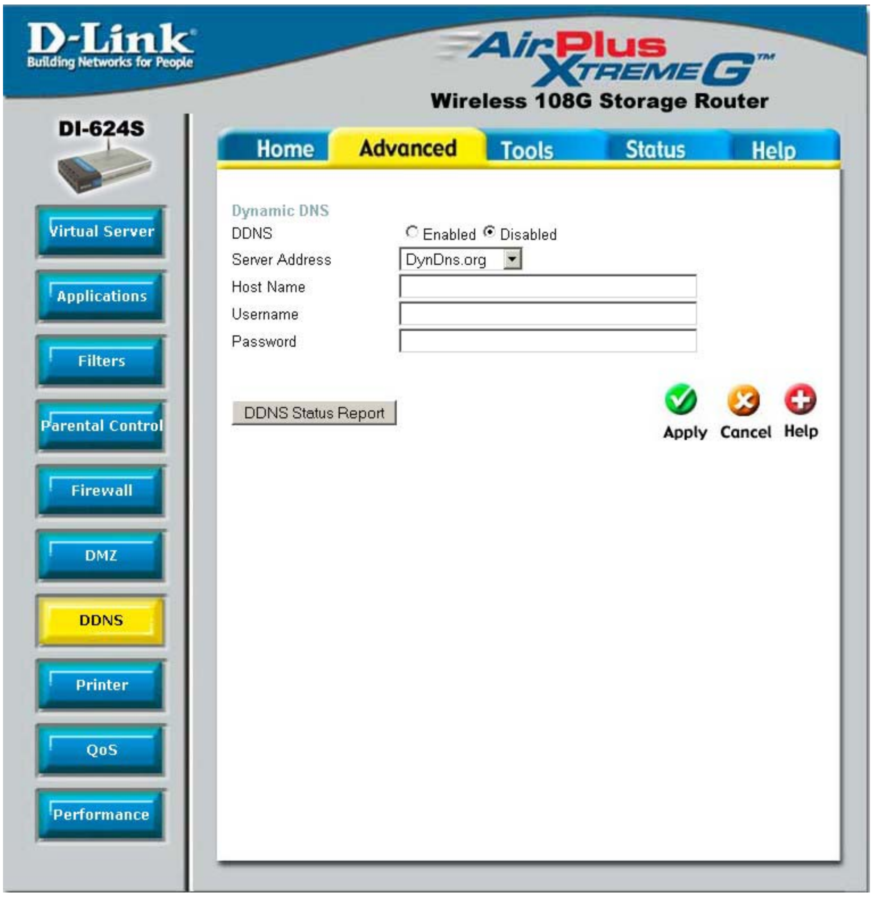
Firewalls may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a firewall bypass can be set up using a DMZ IP address. The DMZ IP address is a “visible” address and does not benefit from the full protection of the firewall function. Therefore it is advisable that other security precautions be enabled to protect the other computers and devices on the LAN. It may be wise to use isolate the device with the DMZ IP address from the rest of the LAN.

For example, if you want to use video conferencing and still use a firewall, you can use the DMZ IP address function. In this case, you must have a PC or server through which video conferencing will take place. The IP address of this PC or server will then be the DMZ IP address. You can designate the server’s IP address as the DMZ by typing in the IP address in the **IP Address** space provided and then enabling its status by clicking the **Status Enabled** radio button and then click **Apply**.

For the system that uses the DMZ IP address, you may want to manually assign an IP address to it and adjust your DHCP server addresses so that the DMZ IP address is not included in the DHCP server range. This way you avoid possible IP address problems if you reboot the DMZ system. To configure the Router’s DMZ IP address, click the **Advanced** tab at the top of the screen and then the **DMZ** tab to the left.

Advanced > DDNS

The DI-624S supports **DDNS** or Dynamic Domain Name Service. Dynamic DNS allows a dynamic public IP address to be associated with a static host name in any of the many domains, allowing access to a specific host from various locations on the Internet. With this function enabled, remote access to a host will be allowed by choosing a URL by using the pull-down menu. Because many ISPs assign public IP addresses using DHCP, it can be difficult to locate a specific host on the LAN using the standard DNS. For example, if you are running a public web server or VPN server on your LAN, DDNS ensures that the host can be located from the Internet if the public IP address changes.



Dynamic DNS

DDNS ○ Enabled ● Disabled

Server Address DynDns.org

Host Name

Username

Password

Note: DDNS requires that an account be setup with one of the supported DDNS servers prior to engaging it on the router. This function will not work without an accepted account with a DDNS server.

DDNS — Click the **Enabled** button to enable the DDNS feature on the router.

Server Address — Choose the DDNS server address from the pull down menu. Available servers include DynDns.org, No-IP.com, hn.org and zoneedit.com.

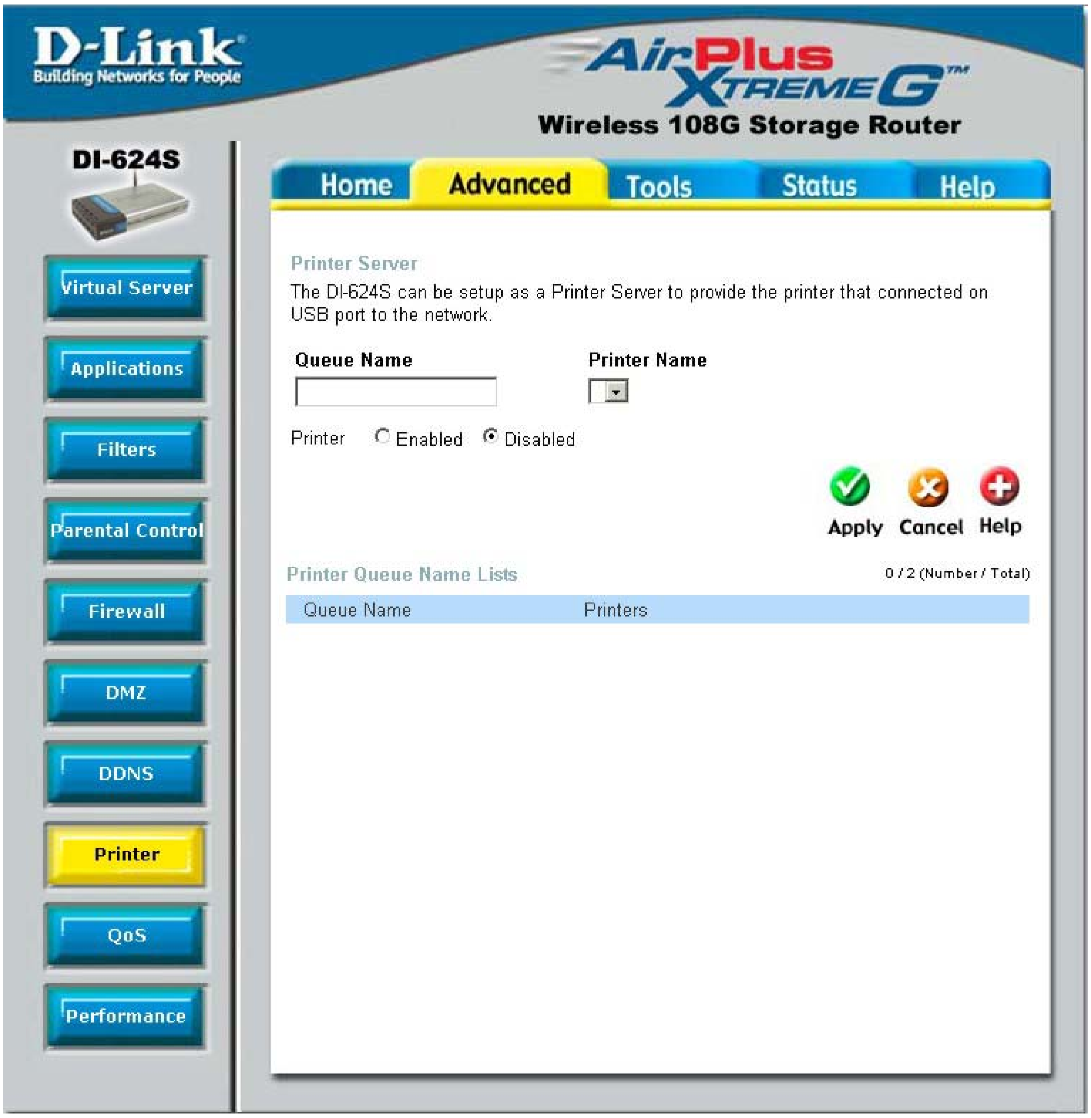
Host name — Enter the host name of the DDNS server.

Username — Enter the username given to you by your DDNS server.

Password — Enter the password given to you by your DDNS server.

Click **Apply** to set this information in the Router.

Advanced > Printer



Printer Server

The DI-624S can be setup as a Printer Server to provide the printer that connected on USB port to the network.

Queue Name

Printer Name

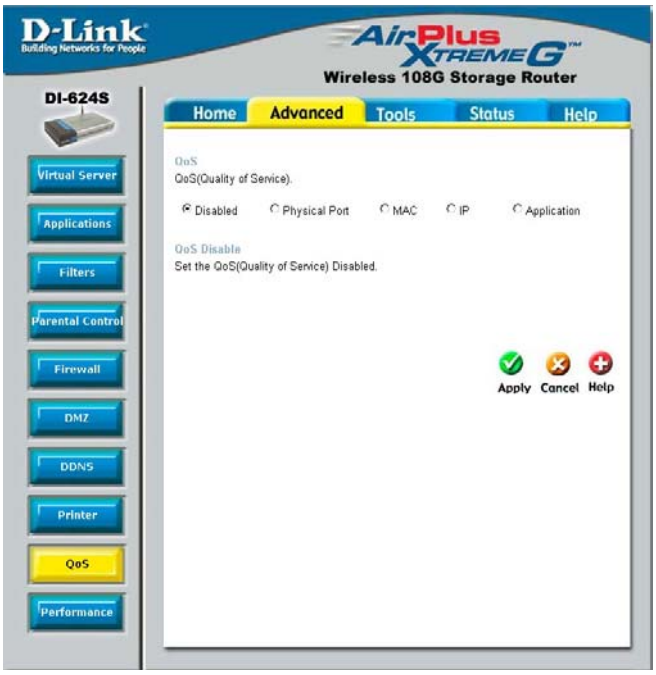
Printer ○ Enabled ● Disabled

Printer Queue Name Lists 0 / 2 (Number / Total)

Queue Name	Printers

The DI-624S has a special ability to serve as a print server when using a USB printer. After connected to the printer through one of the USB ports at the rear of the router, the user must enable the router to act as a print server by clicking the **Enabled** radio button. Once enabled, the router should recognize the connected printer and establish it in the queue as **lp1**. Adjacent to the **Queue Name** should appear the name of the printer, as assigned to it by its manufacturer. Once these names appear in the list, the user may set the printer into the routers memory by clicking **Apply**. Next, the user must enable the printer through a PC on the LAN. Ensure that the **Queue Name** on the router and the **Queue Name** on the PC are the same. For more information on setting up a printer on a PC, see the **Appendix** at the back of this manual.

Advanced > QoS



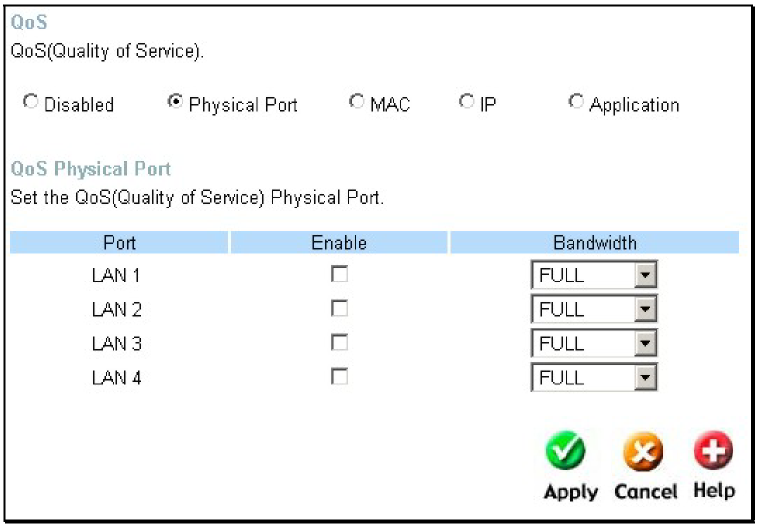
QoS
QoS(Quality of Service).

● Disabled ○ Physical Port ○ MAC ○ IP ○ Application

QoS Disable
Set the QoS(Quality of Service) Disabled.

QoS or Quality of Service is used to allot bandwidth and priority from the router. To allot bandwidth per port on the router, click the **QoS Bandwidth** radio button and configure the parameters. QoS may be configured per **Physical Port**, **MAC address**, **IP address** or specified application. See the following explanation for more detailed information on each type of QoS setting.

Advanced > QoS > Physical Port



QoS
QoS(Quality of Service).

○ Disabled ● Physical Port ○ MAC ○ IP ○ Application

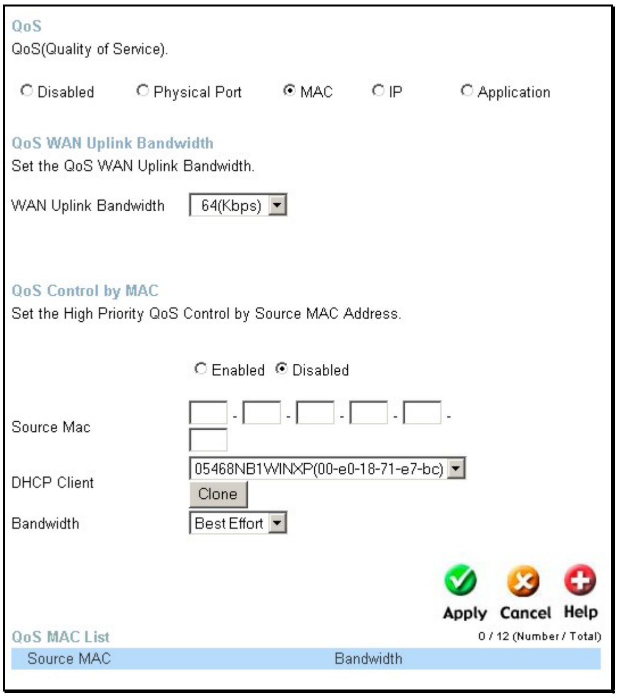
QoS Physical Port
Set the QoS(Quality of Service) Physical Port.

Port	Enable	Bandwidth
LAN 1	□	FULL
LAN 2	□	FULL
LAN 3	□	FULL
LAN 4	□	FULL

To enable QoS per port, first click the Physical Port radio button which will reveal the preceeding screen for the user to configure. Simply click the **Enable** check box of the corresponding port to enable for QoS. You may also set the bandwidth for that port by using that corresponding pull-down menu. The user may choose a bandwidth between 128 Kbps to 32 Mbps. **FULL** denotes that the port will have the maximum transfer speed allowed at any given time, up to 100Mbps. Click **Apply** to confirm your settings.

Advanced > QoS > MAC

The user may also set QoS by specific MAC address. To enable QoS per MAC address, first click the **MAC** radio button which will reveal the preceeding screen for the user to configure. Ensure that the Bandwidth configured does not exceed the incoming bandwidth from the ISP or it will cause other devices on the LAN to slow down due to decreased bandwidth. Check with your ISP for more information on the bandwidth allotted to your account.



QoS

QoS(Quality of Service).

○ Disabled ○ Physical Port ● MAC ○ IP ○ Application

QoS WAN Uplink Bandwidth

Set the QoS WAN Uplink Bandwidth.

WAN Uplink Bandwidth: 64(Kbps)

QoS Control by MAC

Set the High Priority QoS Control by Source MAC Address.

○ Enabled ● Disabled

Source Mac: [ ] - [ ] - [ ] - [ ] - [ ] - [ ]

DHCP Client: 05468NB1WINXP(00-e0-18-71-e7-bc)

Bandwidth: Best Effort

QoS MAC List 0 / 12 (Number / Total)

Source MAC	Bandwidth

WAN Uplink Bandwidth Use the pull down menu to set the **WAN Uplink Bandwidth**. The user may choose a speed from 64kbps to Full (100Mbps). Ensure that the Bandwidth does not exceed the incoming bandwidth from the ISP or it will cause other devices on the LAN to slow down due to decreased bandwidth. Check with your ISP for more information on the bandwidth allotted to your account.

QoS Control by MAC Click the **Enabled** radio button to enable QoS priority by MAC address. Information coming from this MAC address will have the highest priority on the LAN. This means that information originating from this device will be sent to other devices on the LAN requesting it, first. Other devices will have a lower priority in sending information through the router.

Source MAC Enter the source MAC address that will be set for high priority QoS in the router.

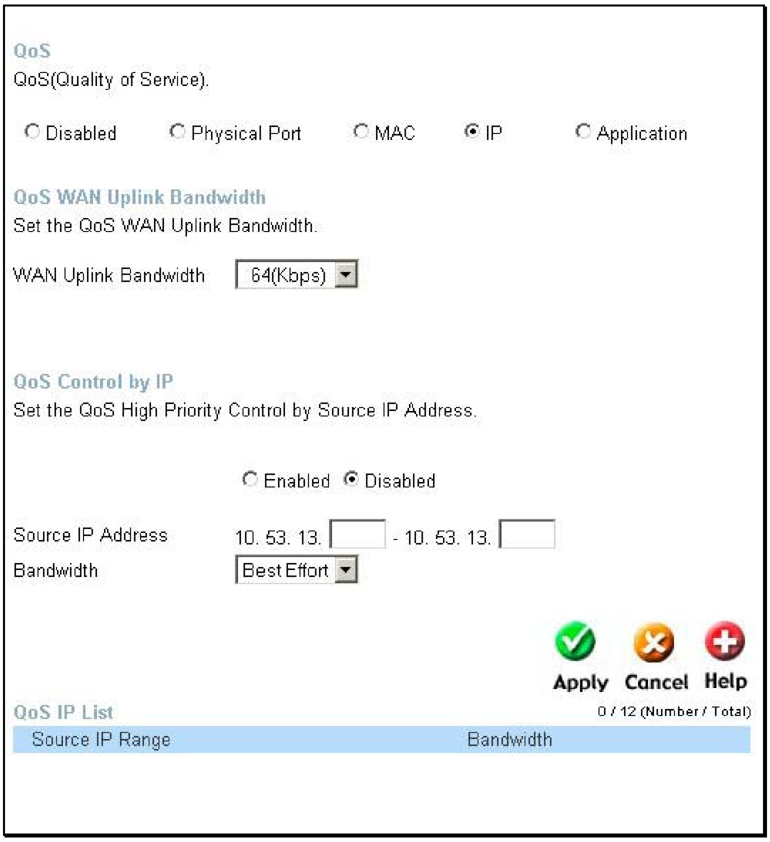
DHCP Client The user may use the DHCP client to aid in choosing the MAC address to be implemented for QoS. All devices connected to the router will be listed in the pull down menu. Simply choose the correct device and click the **Clone** button, which will produce that devices MAC address in the **Source MAC** field.

Bandwidth Use the pull-down menu to select the best bandwidth for the QoS Setting on this router. The user may set a bandwidth between 1Kbps to 32Mbps. Choosing **Best Effort** will set the router to allow the first user to access the source MAC address to have the total bandwidth needed for the file being transferred. Choosing **Full** will denote that the router will allot 100Mbps of bandwidth for the specified QoS implementation. Only one QoS implementation can be set at Full.

Click **Apply** to set the QoS for MAC.

Advanced > QoS > IP

The user may also set QoS by specific IP address. To enable QoS per IP address, first click the **IP** radio button which will reveal the preceeding screen for the user to configure. Ensure that the bandwidth does not exceed the incoming bandwidth from the ISP or it will cause other devices on the LAN to slow down due to decreased bandwidth. Check with your ISP for more information on the bandwidth allotted to your account.



QoS

QoS(Quality of Service).

○ Disabled ○ Physical Port ○ MAC ● IP ○ Application

QoS WAN Uplink Bandwidth

Set the QoS WAN Uplink Bandwidth.

WAN Uplink Bandwidth 64(Kbps)

QoS Control by IP

Set the QoS High Priority Control by Source IP Address.

○ Enabled ● Disabled

Source IP Address 10. 53. 13. [ ] - 10. 53. 13. [ ]

Bandwidth Best Effort

QoS IP List 0 / 12 (Number / Total)

Source IP Range	Bandwidth

WAN Uplink Bandwidth
Use the pull down menu to set the **WAN Uplink Bandwidth**. The user may choose a speed from 64kbps to Full (100Mbps). Ensure that the bandwidth does not exceed the incoming bandwidth from the ISP or it will cause other devices on the LAN to slow down due to decreased bandwidth. Check with your ISP for more information on the bandwidth allotted to your account.

QoS Control by IP
Click the enabled radio button to enable QoS priority by MAC address. Information coming from this IP address will have the highest priority on the LAN. This means that information originating from this device will be sent to other devices on the LAN requesting it, first. Other devices will have a lower priority in sending information through the router.

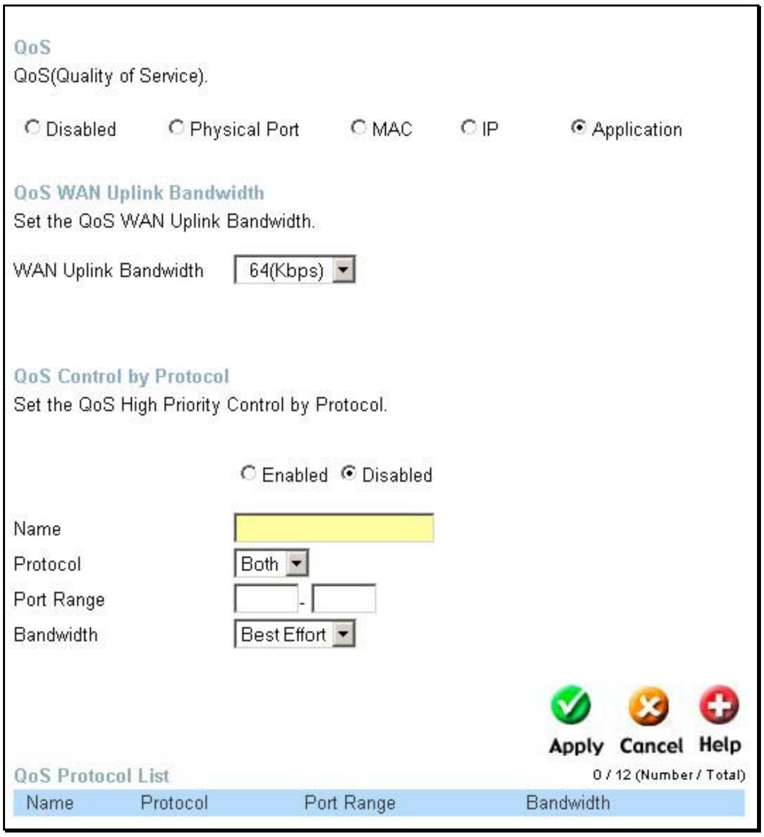
Source IP
Enter the source IP address or range of IP addresses that will be set for high priority QoS in the router.

Bandwidth
Use the pull-down menu to select the best bandwidth for the QoS setting on this router. The user may set a Bandwidth between 1Kbps to 32Mbps. Choosing **Best Effort** will set the router to allow the first user to access the source IP address to have the total bandwidth needed for the file being transferred. Choosing **Full** will denote that the router will allot 100Mbps of bandwidth for the specified QoS implementation. Only one QoS implementation can be set at **Full**.

Click Apply to set the QoS for IP.

Advanced > QoS > Application

The user may also set QoS by specific protocol. To enable QoS per protocol, first click the **Application** radio button which will reveal the preceeding screen for the user to configure. Ensure that the bandwidth does not exceed the incoming bandwidth from the ISP or it will cause other devices on the LAN to slow down due to decreased bandwidth. Check with your ISP for more information on the bandwidth allotted to your account.



QoS

QoS(Quality of Service).

○ Disabled ○ Physical Port ○ MAC ○ IP ● Application

QoS WAN Uplink Bandwidth

Set the QoS WAN Uplink Bandwidth.

WAN Uplink Bandwidth 64(Kbps)

QoS Control by Protocol

Set the QoS High Priority Control by Protocol.

○ Enabled ● Disabled

Name

Protocol Both

Port Range -

Bandwidth Best Effort

QoS Protocol List 0 / 12 (Number / Total)

Name	Protocol	Port Range	Bandwidth

QoS Control by IP

Click the **Enabled** radio button to enable QoS priority by application. Information coming from this application will have the highest priority on the LAN. This means that information originating from this device will be sent to other devices on the LAN requesting it, first. Other devices will have a lower priority in sending information through the router.

Name

Enter a user-defined name to define this application for users on the LAN.

Protocol

Choose the protocol to be enabled for QoS from the pull-down menu. The user may choose **TCP**, **UDP** or **Both**.

Port Range

Enter a virtual port range that will use this application. Remember these are virtual ports and not physical ports on the router.

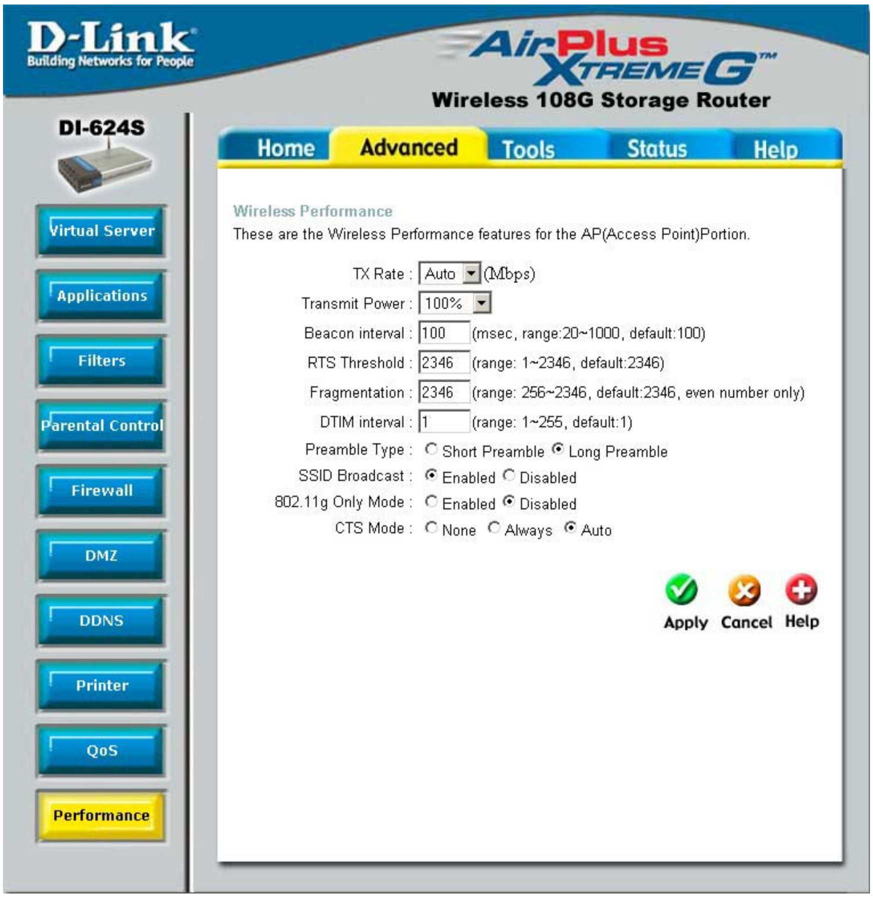
Bandwidth

Use the pull-down menu to select the best bandwidth for the QoS setting on this router. The user may set a bandwidth between 1Kbps to 32Mbps. Choosing **Best Effort** will set the router to allow the first user to access the set application to have the total bandwidth needed for the file being transferred. Choosing **Full** will denote that the router will allot 100Mbps of bandwidth for the specified QoS implementation. Only one QoS implementation can be set at **Full**.

Click A**pply** to set the QoS for IP.

Advanced > Performance

The **Performance** window is used to configure settings for the Access Point feature of this device. Configuring these settings may increase the performance of your router but if you are not familiar with networking devices and protocols, this section should be left at its default settings. Below is a list of the functions associated with the Access Point feature of the router. Click **Apply** when you have completed your changes.



Wireless Performance

These are the Wireless Performance features for the AP(Access Point)Portion.

TX Rate : Auto (Mbps)
Transmit Power : 100%
Beacon interval : 100 (msec, range:20~1000, default:100)
RTS Threshold : 2346 (range: 1~2346, default:2346)
Fragmentation : 2346 (range: 256~2346, default:2346, even number only)
DTIM interval : 1 (range: 1~255, default:1)
Preamble Type : ○ Short Preamble ● Long Preamble
SSID Broadcast : ● Enabled ○ Disabled
802.11g Only Mode : ○ Enabled ● Disabled
CTS Mode : ○ None ○ Always ● Auto

TX Rate

Use the pull down menu to select the transfer data rate, in Mbps. The default setting of **Auto** will automatically adjust the transfer rate to the highest possible rate allowed.

Transmit Power

Allows the user to adjust the transmit power of the router. A high transmit power allows a greater area range of accessibility to the router.

Beacon interval

Beacons are emitted from the router in order to synchronize the wireless network. You may set the range between 20-100 microseconds per beacon sent. The default is 100.

RTS Threshold

The RTS (Request to Send) Threshold controls the size of data packets issued to a RTS packet. A lower level will send packets more frequently which may consume a great amount of the available bandwidth. A high threshold will allow the router to recover from interference or collisions which is more prevalent in a network with high traffic or high electromagnetic interference. The default setting is 2346.

Fragmentation

The fragmentation threshold will determine if packets are to be fragmented. Packets over the 2346 byte limit will be fragmented before transmission. 2346 is the default setting.

DTIM Interval

DTIM (Delivery Traffic Indication Message) is a countdown informing clients of the next window for listening to broadcast and multicast messages. The default setting is 3.

Preamble Type

Select **Short** or **Long Preamble.** The Preamble defines the length of the CRC block (Cyclic Redundancy Check is a common technique for detecting data transmission errors) for communication between the wireless router and the roaming wireless network adapters. *Note: High network traffic areas should use the shorter preamble type.*

SSID Broadcast

Choose **Enabled** to broadcast the SSID across the network. All devices on a network must share the same SSID (Service Set Identifier) to establish communication. Choose **Disabled** if you do not wish to broadcast the SSID over the network.

802.11g Only Mode

Select this mode to restrict your network to only those devices that employ the 802.11g standard. Enabling this mode will ensure that you maintain the highest connectivity rate, unhampered by any connection to an 802.11b device.

CTS Mode

CTS (Clear To Send) is a function used to minimize collisions among wireless devices on a wireless local area network (LAN). CTS will make sure the wireless network is clear before a wireless client attempts to send wireless data. Enabling CTS will add overhead and may lower wireless throughput.

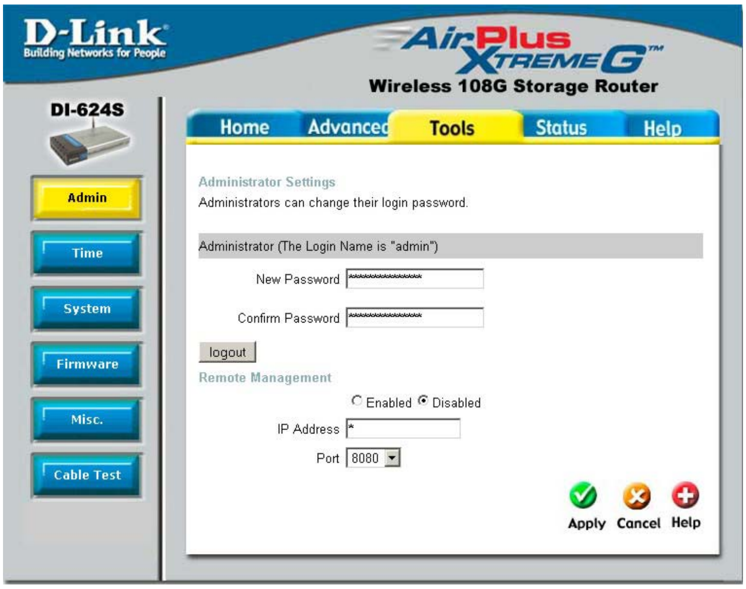
Auto- CTS will monitor the wireless network and automatically decide whether to implement CTS based on the amount of traffic and collisions that occurs on the wireless network.

Always- CTS will always be used to make sure the wireless LAN is clear before sending data.

None- CTS is typically used in a pure 802.11g environment. If CTS is set to “None” in a mixed mode environment populated by 802.11b clients, wireless collisions may

Tools > Admin

At this page, the DI-624S administrator can change the system password. There are two accounts that can access the Broadband Router's Web-Management interface. They are admin and user. Admin has read/write access while user has read-only access. User can only view the settings but cannot make any changes.



Administrator Settings

Administrators can change their login password.

Administrator (The Login Name is "admin")

New Password **************

Confirm Password **************

logout

Remote Management

○ Enabled ● Disabled

IP Address *

Port 8080

Administrator

admin is the **Administrator login name.**

Password

Enter the password here and the same password in the **Confirm Password** field. This will be the password that the administrator will use to gain access to the configuration menu of the device. There is no default password for this device.

User

user is the **User login name**

Password

Enter the password here and the same password in the **Confirm Password** field. This will be the password that the users will use to gain access to the configuration menu of the device. Users will have limited privileges on this device. There is no default password for this device.

Remote Management

Remote management allows the DI-624 to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform **Administrator** tasks. This feature enables you to perform Administrator tasks from the remote (Internet) host.

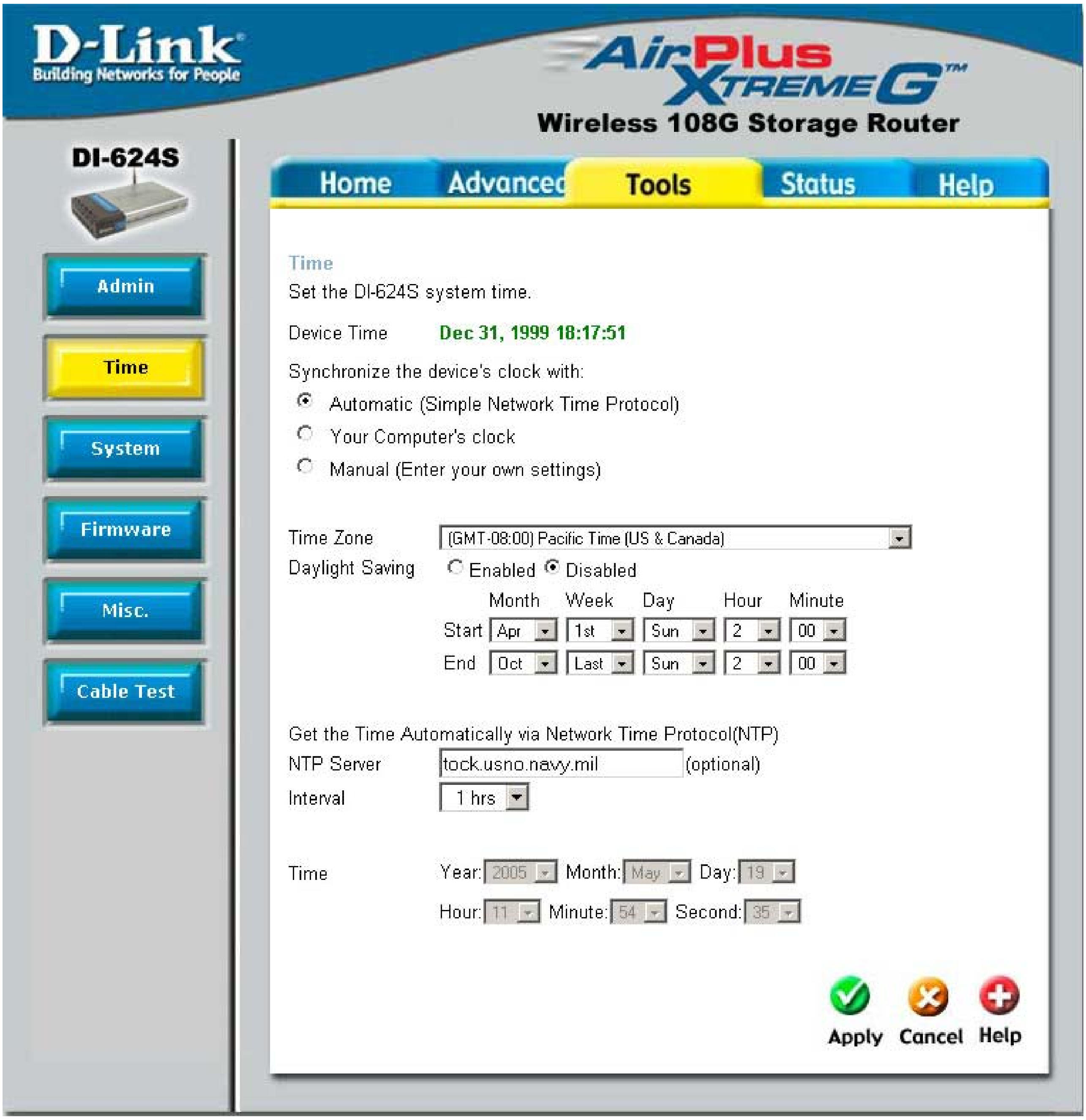
IP Address

The Internet IP address of the computer that has access to the Broadband Router. If you input an asterisk (*) into this field, then any computer will be able to access the Router. Putting an asterisk (*) into this field would present a security risk and is not recommended.

Port

The port number used to access the Broadband Router. The default port number for web management is 8080.

Tools > Time



Time

Set the DI-624S system time.

Device Time Dec 31, 1999 18:17:51

Synchronize the device's clock with:

● Automatic (Simple Network Time Protocol)

○ Your Computer's clock

○ Manual (Enter your own settings)

Time Zone (GMT-08:00) Pacific Time (US & Canada)

Daylight Saving ○ Enabled ● Disabled

	Month	Week	Day	Hour	Minute
Start	Apr	1st	Sun	2	00
End	Oct	Last	Sun	2	00

Get the Time Automatically via Network Time Protocol(NTP)

NTP Server tock.usno.navy.mil (optional)

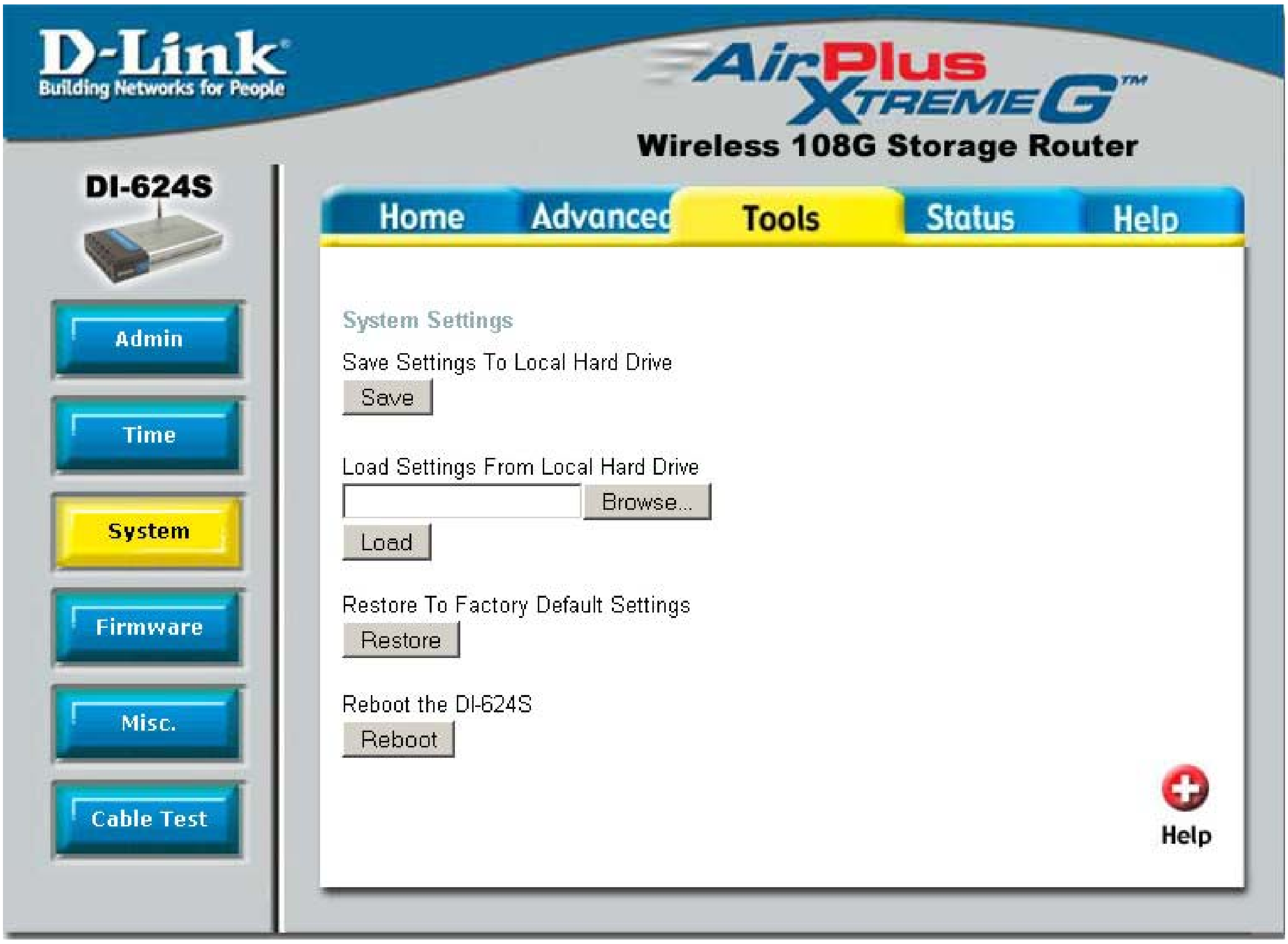
Interval 1 hrs

Time Year: 2005 Month: May Day: 19

Hour: 11 Minute: 54 Second: 35

The system time is the time used by the DI-624S for scheduling services. You can manually set the time, connect to a NTP (Network Time Protocol) server or synchronize the time on the router with your PC. If an NTP server is set, you will only need to set the time zone and the update Interval. You may also set the time from the clock on your computer by checking the corresponding radio button. To manually set the time, you will need to input the value into the fields provided. If you manually set the time, you may also set the Daylight Saving Time by clicking the corresponding **Enabled** radio button and the system time will automatically adjust on those dates. Click **Apply** to set changes made.

Tools > System



System Settings

Save Settings To Local Hard Drive

Load Settings From Local Hard Drive

Restore To Factory Default Settings

Reboot the DI-624S

The **System** window has three basic functions for the DI-624S administrator. Configuration settings can be saved to a local hard drive on your computer by clicking the Save button. This will produce a new window from your operating system inquiring you about the location where you would like to save your files. The administrator may also upload configuration settings saved to a local hard drive by entering the path into the open field or by clicking the browse button and searching for its location the computer. Once found, click **Load** to upload these settings to the DI-624S. The administrator may also restore the router back to its default configurations by clicking the **Restore** button.

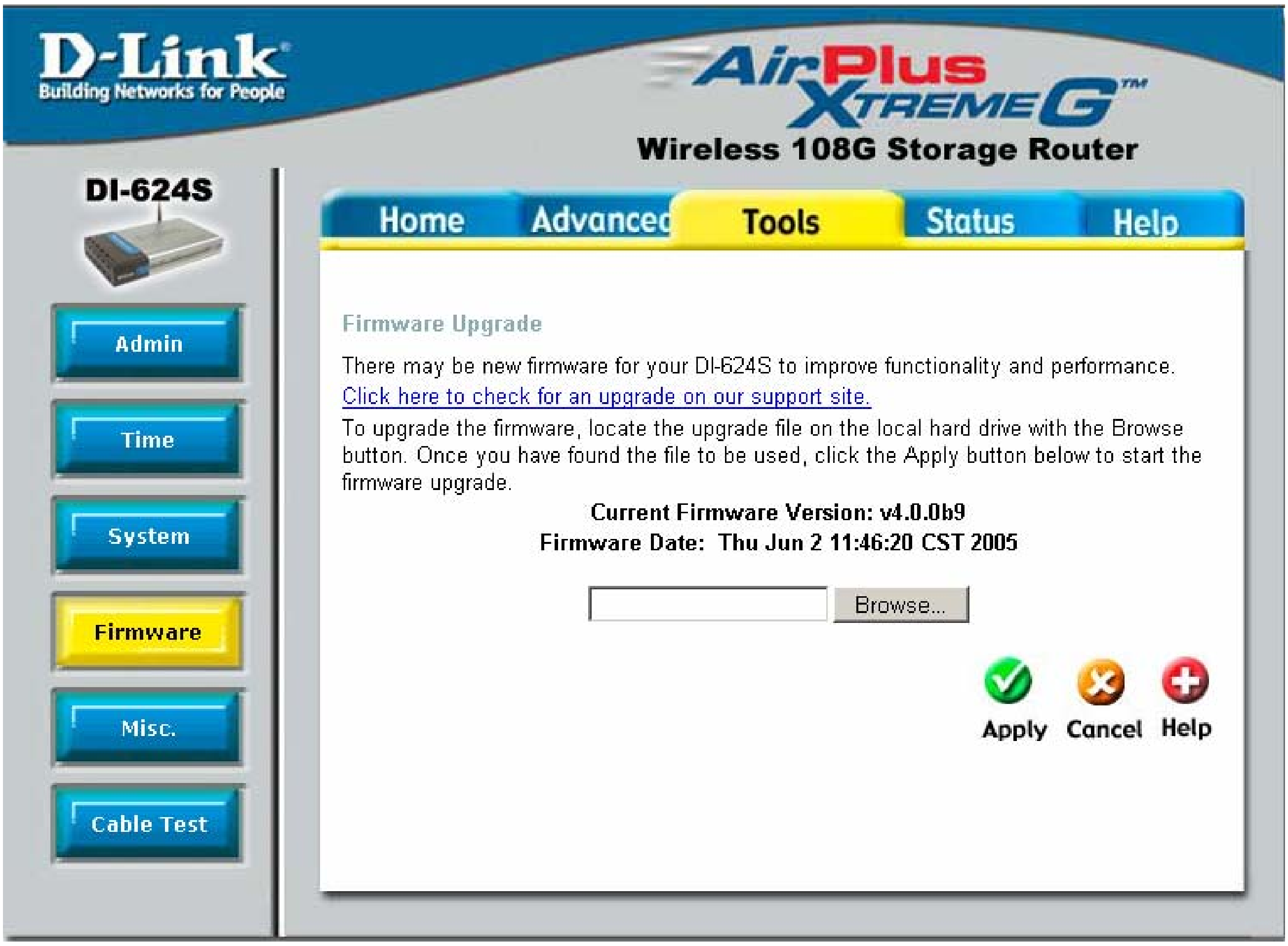
Save — Click **Save** to save the current settings to the local Drive

Browse / Load — Click **Browse** to find the settings, then click **Load**

Restore — Click **Restore** to restore the factory default settings

Reboot — Click **Reboot** to reboot the Router.

Tools > Firmware



Firmware Upgrade

There may be new firmware for your DI-624S to improve functionality and performance.
Click here to check for an upgrade on our support site.
To upgrade the firmware, locate the upgrade file on the local hard drive with the Browse button. Once you have found the file to be used, click the Apply button below to start the firmware upgrade.

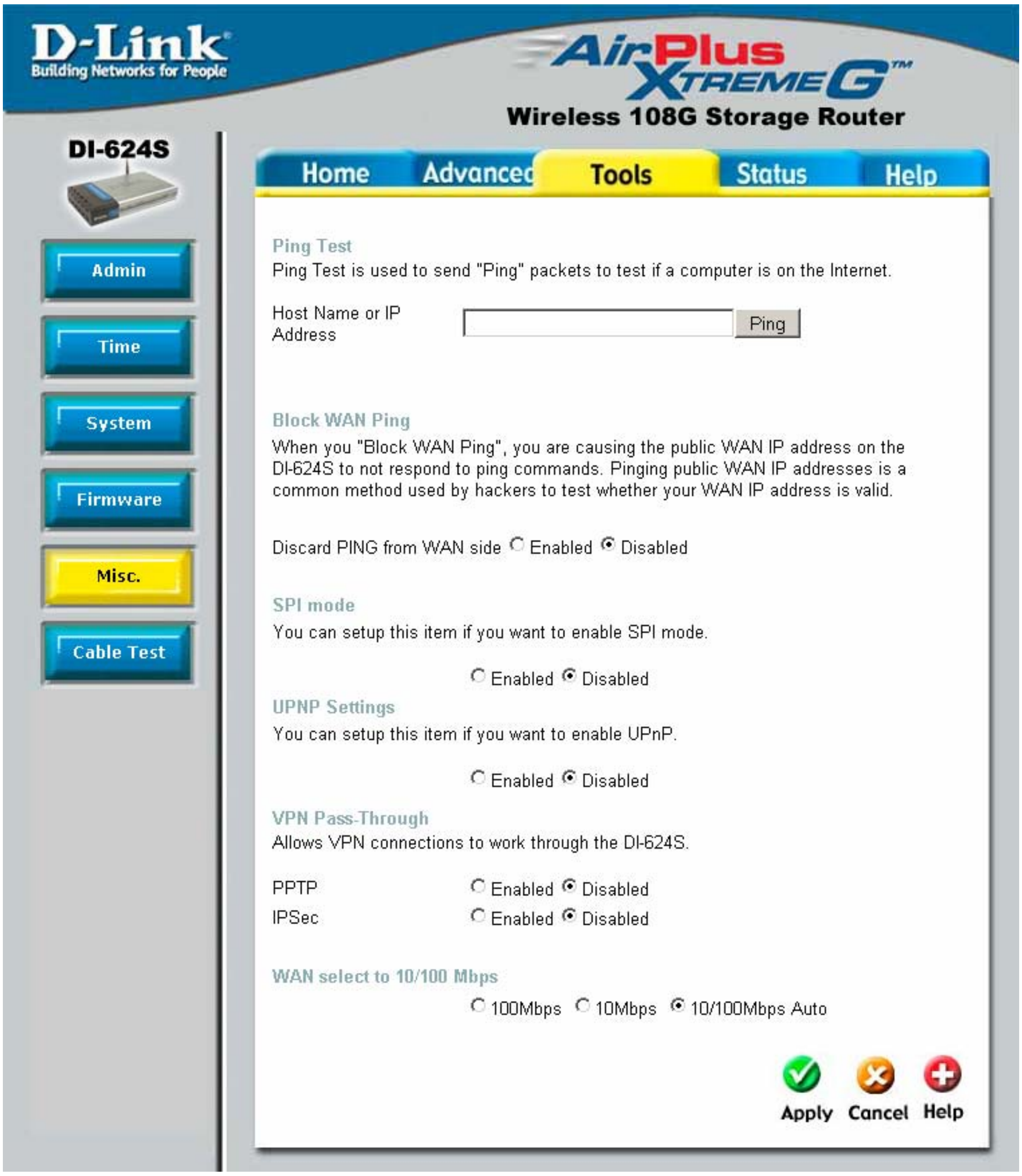
Current Firmware Version: v4.0.0b9
Firmware Date: Thu Jun 2 11:46:20 CST 2005

You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to browse the local hard drive and locate the firmware to be used for the update. Please check the D-Link Support site for firmware updates at http://support.dlink.com. You can download firmware upgrades to your hard drive from the D-Link support site.

Firmware Upgrade	Click on the link in this screen to find out if there is an updated firmware; if so, download the new firmware to your hard drive.
Browse	After you have downloaded the new firmware, click **Browse** in this window to locate the firmware update on your hard drive.

Click **Apply** to complete the firmware upgrade.

Tools > Misc.



Ping Test

Ping Test is used to send "Ping" packets to test if a computer is on the Internet.

Host Name or IP Address [ ] Ping

Block WAN Ping

When you "Block WAN Ping", you are causing the public WAN IP address on the DI-624S to not respond to ping commands. Pinging public WAN IP addresses is a common method used by hackers to test whether your WAN IP address is valid.

Discard PING from WAN side ○ Enabled ● Disabled

SPI mode

You can setup this item if you want to enable SPI mode.

○ Enabled ● Disabled

UPNP Settings

You can setup this item if you want to enable UPnP.

○ Enabled ● Disabled

VPN Pass-Through

Allows VPN connections to work through the DI-624S.

PPTP ○ Enabled ● Disabled

IPSec ○ Enabled ● Disabled

WAN select to 10/100 Mbps

○ 100Mbps ○ 10Mbps ● 10/100Mbps Auto

Ping Test

The Ping Test is used to send Ping packets to test if a computer is on the Internet. Enter the IP Address that you wish to Ping, and click **Ping**.

Block WAN Ping

Discard Ping from WAN side- If you choose to block WAN Ping, the WAN IP Address of the DI-624S will not respond to pings. Blocking the Ping may provide some extra security from hackers. Click **Enabled** to block the WAN ping.

SPI Mode

SPI or Stateful Packet Inspection is a type of firewall that protects your network against hacker attacks by analyzing packets to ensure that only authorized packets will be allowed to enter your network. To enable this function, click the Enabled radio button. This function is enabled by default.

VPN Pass Through

The DI-624S supports VPN (Virtual Private Network) pass-through for both PPTP (Point-to-Point Tunneling Protocol) and IPSec (IP Security). Once VPN pass-through is enabled, there is no need to open up virtual services. Multiple VPN connections can be made through the DI-624S. This is useful when you have many VPN clients on the LAN network.

PPTP select Enabled or Disabled.

IPSec select Enabled or Disabled.

UPNP Settings

You may enable the Universal Plug n' Play function here by clicking the **Enabled** radio button.

WAN select

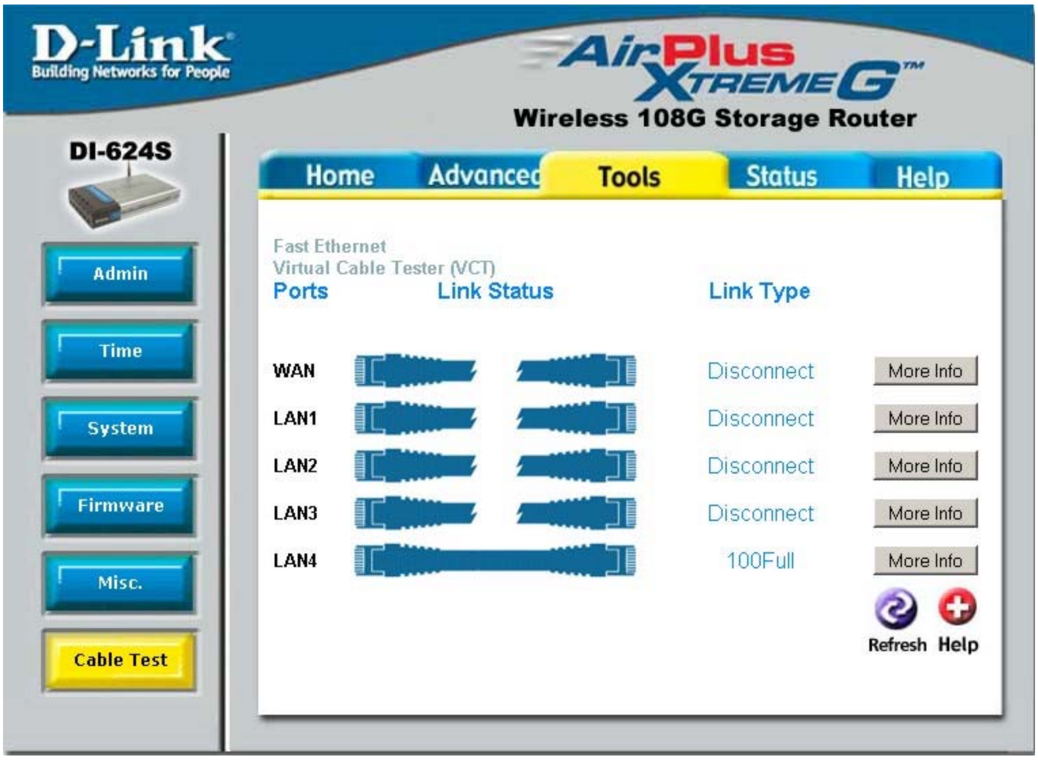
This section allows the user to set the wire speed over which the router will transmit packets. The user has three options:

100 Mbps – Clicking this radio button will set the wire speed at 100 megabytes per second.

10 Mbps – Clicking this radio button will set the wire speed at 10 megabytes per second.

10/100 Mbps Auto – Clicking this radio button will allow the wire speed to be automatically set by the router depending on the wire speed available at any given time.

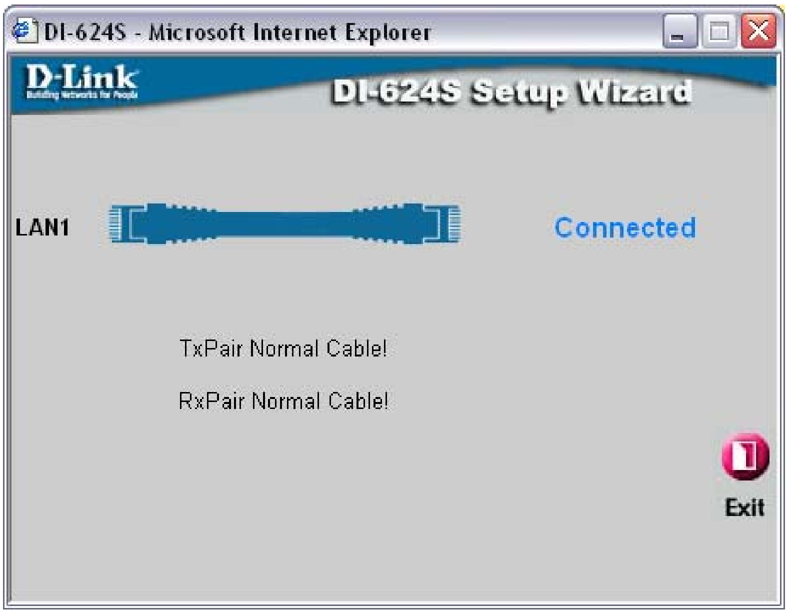
Tools > Cable Test



Fast Ethernet
Virtual Cable Tester (VCT)

Ports	Link Status	Link Type	
WAN		Disconnect	More Info
LAN1		Disconnect	More Info
LAN2		Disconnect	More Info
LAN3		Disconnect	More Info
LAN4		100Full	More Info

The above window is a **Vitrual Cable Tester** and it shows the user the current status of the ports of the Router. In this window, we can see that LAN4 port is connected at a speed of 100Mbps Full (duplex) and all the other connections do not have a valid link. Clicking the **More** Info button will open an additional window with more information about this connection, as shown below.


DI-624S - Microsoft Internet Explorer
D-Link
Building Networks for People
DI-624S Setup Wizard
Exit

LAN1 Connected

TxPair Normal Cable!

RxPair Normal Cable!

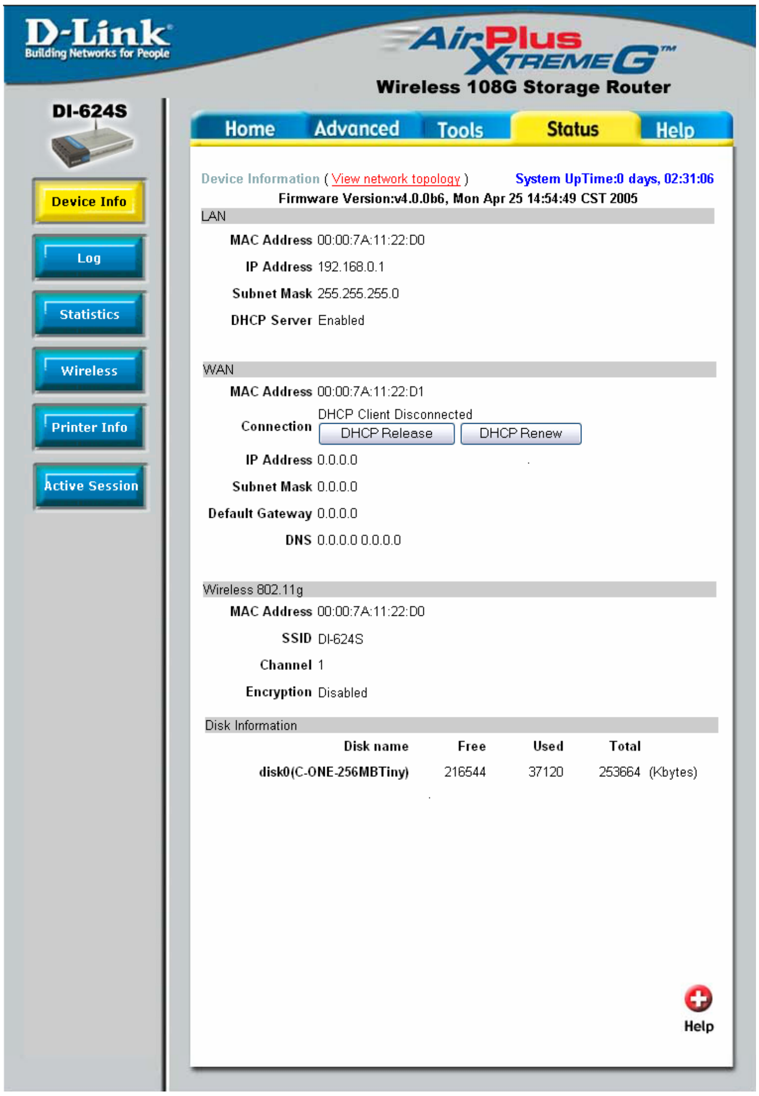
Status > Device Info

This page displays the current information for the DI-624S. It will display the LAN, WAN, Wireless 802.11g and Disk Information statistics.

If your WAN connection is set up for a Dynamic IP address then a Release button and a Renew button will be displayed. Use Release to disconnect from your ISP and use Renew to connect to your ISP.

If your WAN connection is set up for PPPoE, a Connect button and a Disconnect button will be displayed. Use Disconnect to drop the PPPoE connection and use Connect to establish the PPPoE connection.

This window will show the DI-624S's working status:



Device Information (View network topology) System UpTime:0 days, 02:31:06

Firmware Version:v4.0.0b6, Mon Apr 25 14:54:49 CST 2005

LAN

MAC Address 00:00:7A:11:22:D0

IP Address 192.168.0.1

Subnet Mask 255.255.255.0

DHCP Server Enabled

WAN

MAC Address 00:00:7A:11:22:D1

Connection DHCP Client Disconnected

IP Address 0.0.0.0

Subnet Mask 0.0.0.0

Default Gateway 0.0.0.0

DNS 0.0.0.0 0.0.0.0

Wireless 802.11g

MAC Address 00:00:7A:11:22:D0

SSID DI-624S

Channel 1

Encryption Disabled

Disk Information

Disk name	Free	Used	Total
disk0(C-ONE-256MBTiny)	216544	37120	253664 (Kbytes)

LAN

MAC Address: MAC address of the DI-624S

IP Address: LAN/Private IP Address of the DI-624S

Subnet Mask: LAN/Private Subnet Mask of the DI-624S

DHCP Server: DHCP Server Status

WAN

MAC Address: MAC address of the DI-624S

Connection: Displays the current connection for DHCP. This field also has two buttons for resetting the DHCP server on the Router. *DHCP Release* – Clicking this button will release and reset the DHCP server. All settings configured by DHCP will be lost. *DHCP Renew* – Clicking this button will allow the router to renew the DHCP server and automatically configure new DHCP settings for the connection.

IP Address: WAN/Public IP Address

Subnet Mask: WAN/Public Subnet Mask

Default Gateway: WAN/Public Gateway IP Address

Domain Name Server: WAN/Public DNS IP Address

Wireless 802.11g

MAC Address: MAC address of the DI-624S

SSID: Displays the current SSID

Channel: Displays the current wireless channel in use

Encryption: indicates whether wireless encryption is enabled or disabled

Disk Information

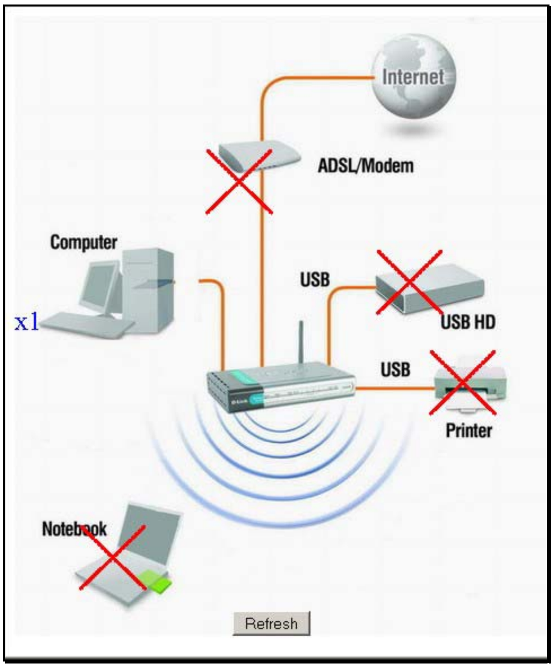
Disk name: Displays the name of a storage device currently connected to the router's USB port

Free: Displays the free memory space on the USB storage device

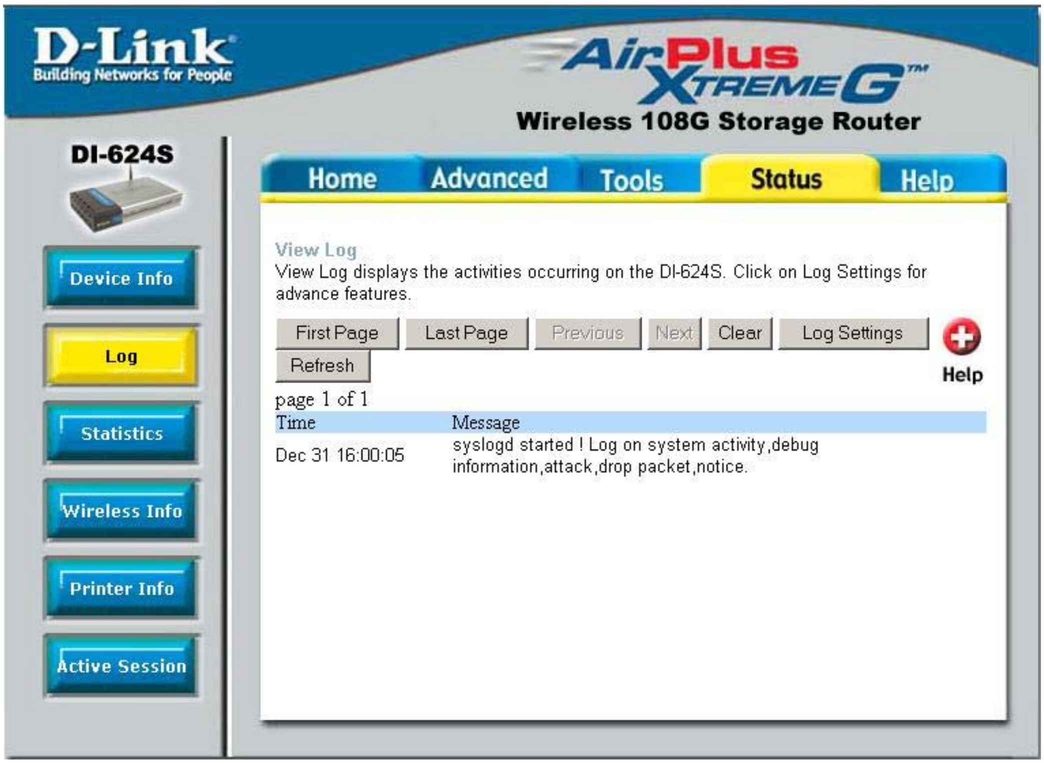
Used: Displays the used memory space on the USB storage device

Total: Displays the total memory space on the USB storage device

The user may also view the current topology currently configured on the router by clicking the View network topology link, which will reveal the following window. A red X through one of the pictures indicates that device is not in the current topology. To refresh this screen, click the **Refresh** button.



Status > Log



View Log

View Log displays the activities occurring on the DI-624S. Click on Log Settings for advance features.

page 1 of 1

Time	Message
Dec 31 16:00:05	syslogd started ! Log on system activity,debug information,attack,drop packet,notice.

The Router keeps a running log of events and activities occurring on the Router. If the device is rebooted, the logs are automatically cleared. You may save the log files under **Log Settings**.

View Log

First Page - The first page of the log

Last Page - The last page of the log

Previous - Moves back one log page

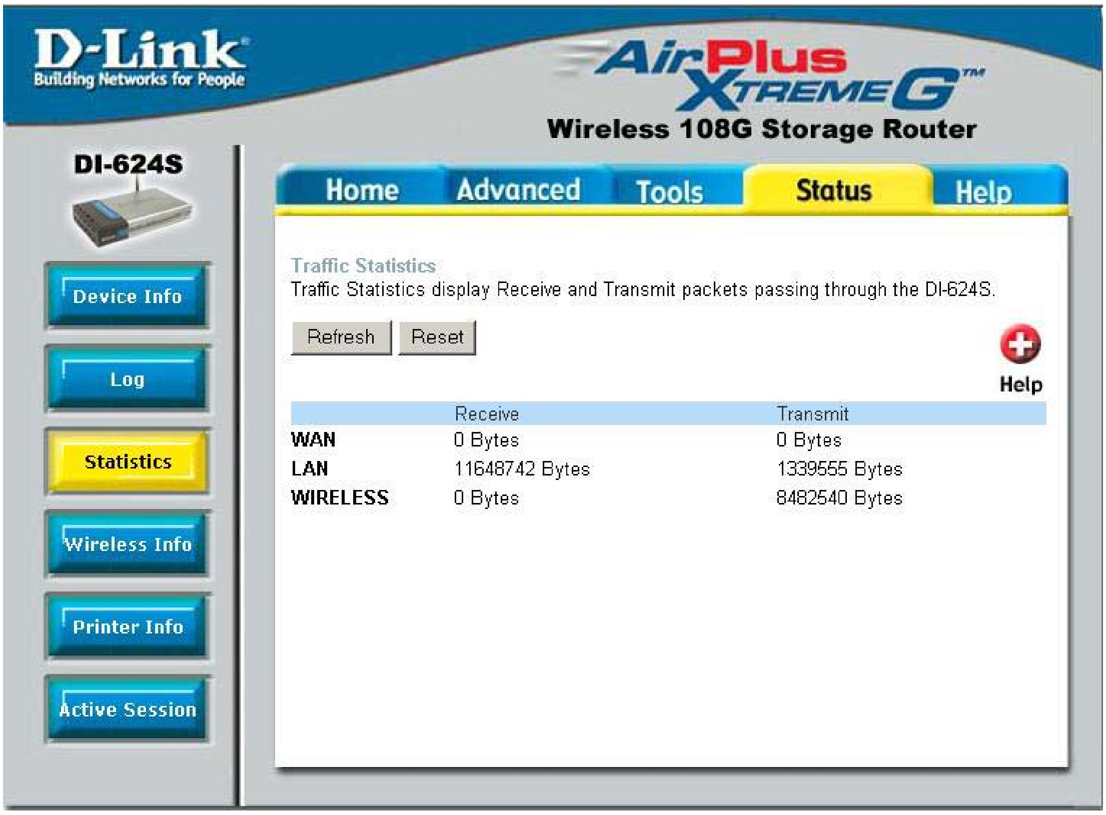
Next - Moves forward one log page

Clear - Clears the logs completely

Log Settings - Brings up the page to configure the log

Refresh – Refreshes the Log window

Status > Statistics



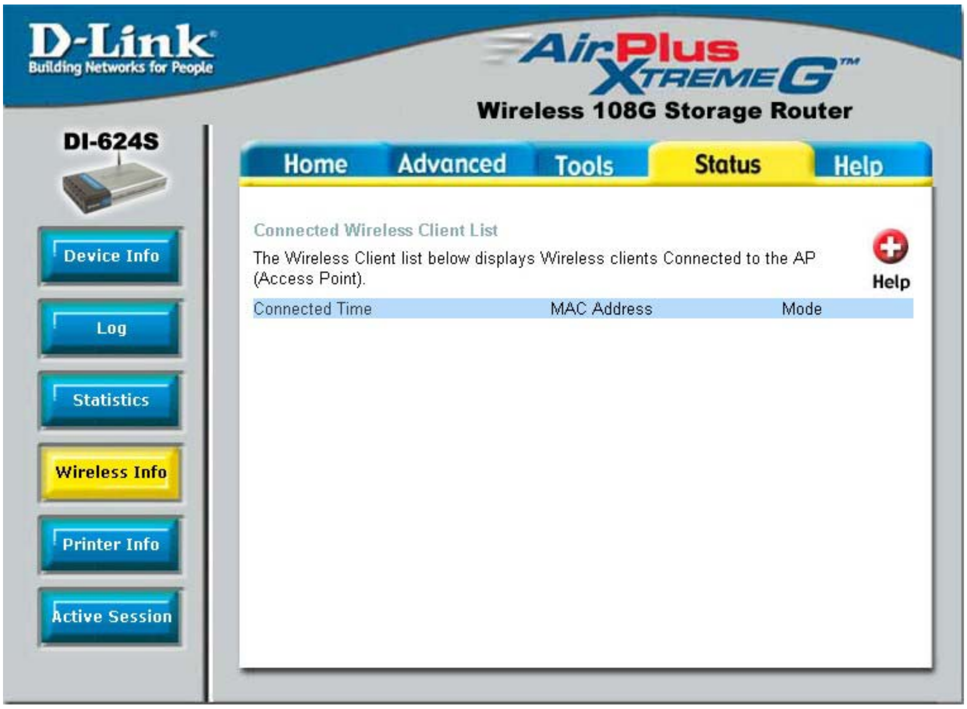
Traffic Statistics

Traffic Statistics display Receive and Transmit packets passing through the DI-624S.

	Receive	Transmit
WAN	0 Bytes	0 Bytes
LAN	11648742 Bytes	1339555 Bytes
WIRELESS	0 Bytes	8482540 Bytes

The screen above displays the Traffic Statistics. Here you can view the amount of packets that pass through the DI-624S on both the WAN and the LAN ports. The traffic counter will reset if the device is rebooted or can be reset by clicking the **Reset** button. To refresh current statistics, click the **Refresh** button.

Status > Wireless



Connected Wireless Client List

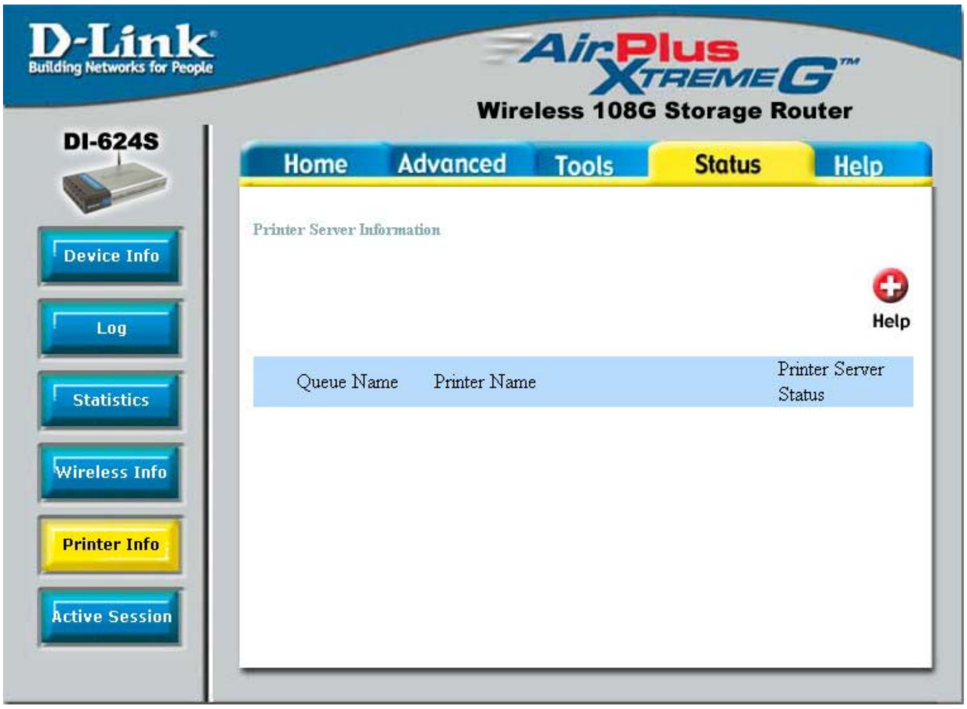
The Wireless Client list below displays Wireless clients Connected to the AP (Access Point).

Connected Time	MAC Address	Mode

The wireless client table displays a list of current connected wireless clients. This table also displays the MAC address and mode of the connected wireless client.

Click on **Help** at any time, for more information.

Status > Printer Info

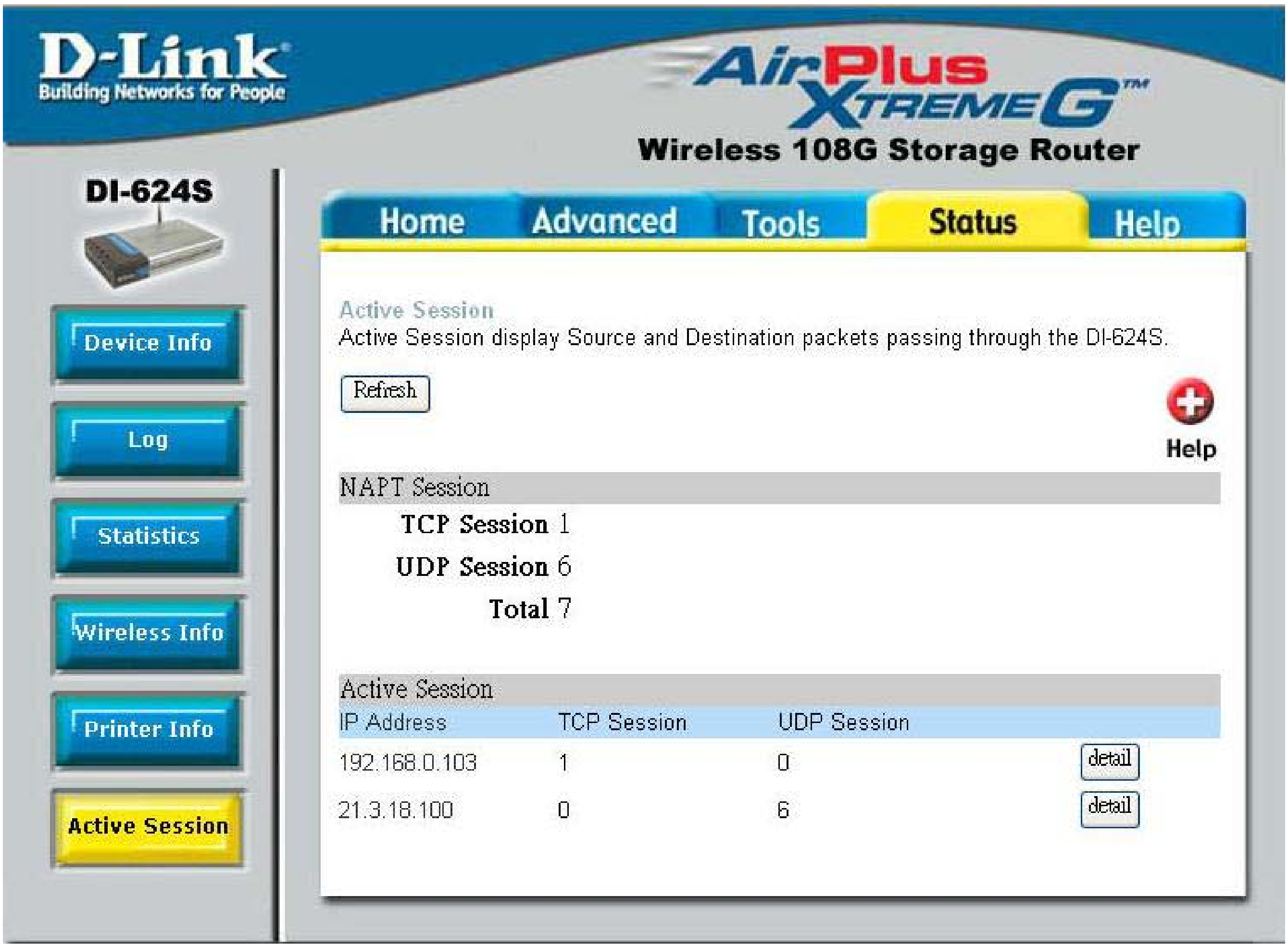


Printer Server Information

Queue Name	Printer Name	Printer Server Status

The **Printer Info** window displays a list of Printers that are using the DI-624S as a print server. These printers are defined by their **Queue Name** and **Printer Name**. The status of these printers is located to the right under the heading **Printer Server Status**.

Active Session



Active Session

Active Session display Source and Destination packets passing through the DI-624S.

NAPT Session

TCP Session 1

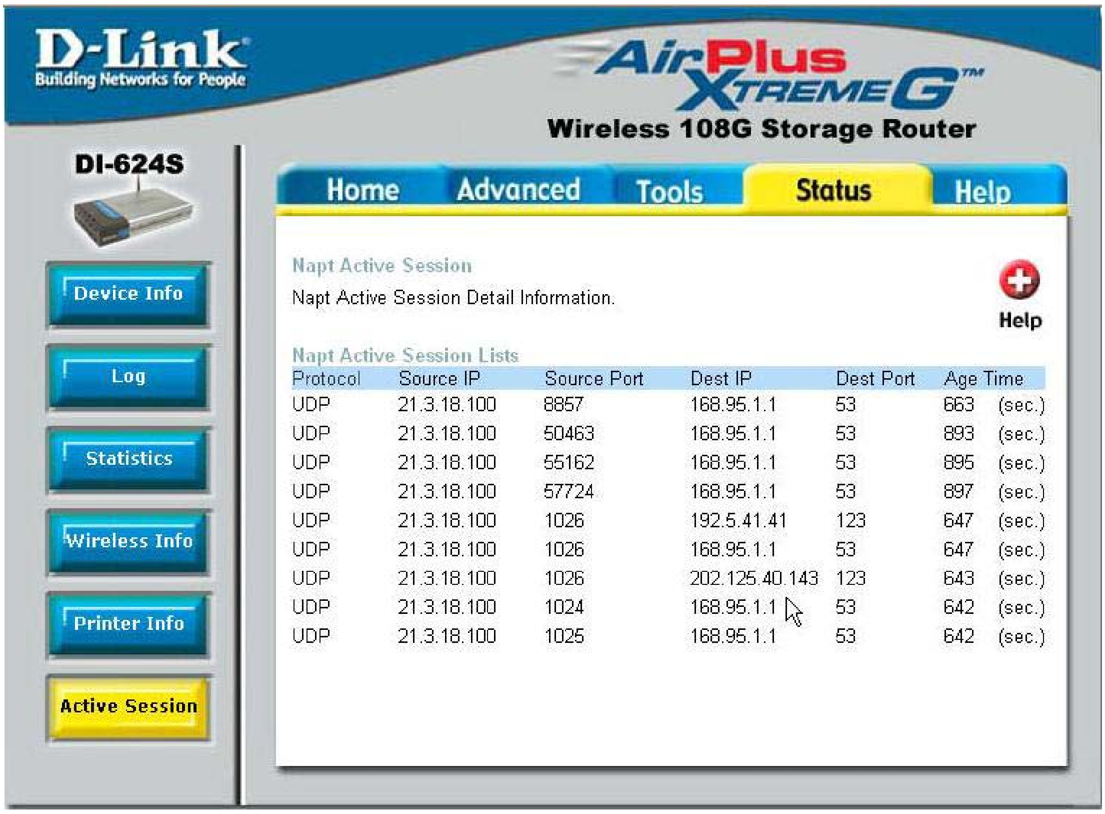
UDP Session 6

Total 7

Active Session

IP Address	TCP Session	UDP Session	
192.168.0.103	1	0	detail
21.3.18.100	0	6	detail

The **Active Session** window allows users to view the packets passing through the router, whether from the source or to the destination. This window displays the total TCP and UDP packets in the **NAPT Session** section. This is a total of the Active Session section on the bottom of the screen. The **Active Session** section will sub-divide the NAPT session section into separate IP addresses and their TCP and UDP packets. For more details regarding a separate IP address on the LAN, click the detail button of the corresponding IP address which will display the following window for the user to view.



Napt Active Session

Napt Active Session Detail Information.

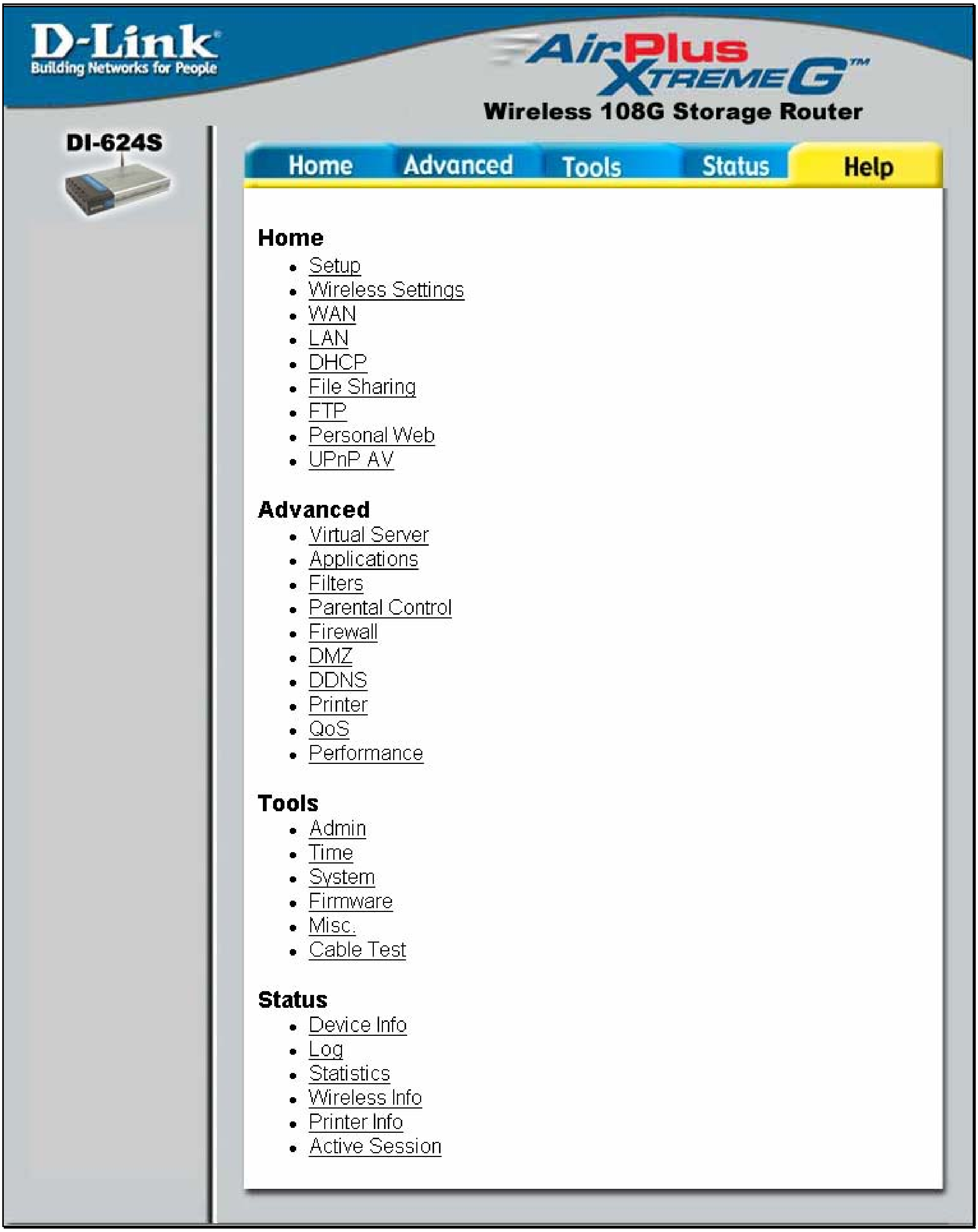
Napt Active Session Lists

Protocol	Source IP	Source Port	Dest IP	Dest Port	Age Time
UDP	21.3.18.100	8857	168.95.1.1	53	663 (sec.)
UDP	21.3.18.100	50463	168.95.1.1	53	893 (sec.)
UDP	21.3.18.100	55162	168.95.1.1	53	895 (sec.)
UDP	21.3.18.100	57724	168.95.1.1	53	897 (sec.)
UDP	21.3.18.100	1026	192.5.41.41	123	647 (sec.)
UDP	21.3.18.100	1026	168.95.1.1	53	647 (sec.)
UDP	21.3.18.100	1026	202.125.40.143	123	643 (sec.)
UDP	21.3.18.100	1024	168.95.1.1	53	642 (sec.)
UDP	21.3.18.100	1025	168.95.1.1	53	642 (sec.)

Sub-divided again, this window displays more detailed information on the TCP/UDP actions taken by the specific IP address, as stated below.

Protocol	Displays the protocol used by the corresponding IP address, whether it be TCP or UDP.
Source IP	Displays the IP address of the device sending information.
Source Port	Displays the virtual port used by the source IP address.
Dest IP	Displays the IP address of the destination of the packets sent from the Source IP.
Dest Port	Displays the virtual port receiving information for the Destination IP.
Age time	Displays the total time the particular UDP session was ongoing, in seconds.

Help



Home

- Setup
- Wireless Settings
- WAN
- LAN
- DHCP
- File Sharing
- FTP
- Personal Web
- UPnP AV

Advanced

- Virtual Server
- Applications
- Filters
- Parental Control
- Firewall
- DMZ
- DDNS
- Printer
- QoS
- Performance

Tools

- Admin
- Time
- System
- Firmware
- Misc.
- Cable Test

Status

- Device Info
- Log
- Statistics
- Wireless Info
- Printer Info
- Active Session

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

Technical Specifications

Standards

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

VPN Pass Through/ Multi-Sessions

- PPTP
- L2TP
- IPSec

Device Management

- Web-Based- Internet Explorer v6 or later; Netscape Navigator v6 or later
- DHCP Server and Client Advanced Firewall Features
- NAT with VPN Passthrough (Network Address Translation)
- MAC Filtering
- IP Filtering
- URL Filtering
- Domain Blocking
- Scheduling

Wireless Operating Range

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

Operating Temperature

- 32°F to 113 °F (0°C to 45°C)

Humidity:

- 95% maximum (non-condensing)

Safety and Emissions:

- EMI: FCC Class B, CE Class B, C-Tick, IC
- Safety: CSA International

Wireless Frequency Range:

- 2.4GHz to 2.462GHz

LEDs:

- Power
- WAN
- LAN (10/100)
- WLAN (Wireless Connection)

Status Physical Dimensions:

- L = 7.56 inches (192mm)
- W = 4.65 inches (118mm)
- H = 1.22 inches (31 mm)

Wireless Transmit Power:

- 11g: 14dBm Typical
- 11b: 16dBm Typical

Security:

- 802.1 x
- WPA - WiFi Protected Access
- WPA2 – WiFi Certified Security with AES encryption
- (64, 128-bit WEP with TKIP, MIC, IV Expansion, Shared Key Authentication)

External Antenna Type:

- Single detachable reverse SMA Modulation Technology:
- Orthogonal Frequency Division Multiplexing (OFDM)

Power Input:

- Ext. Power Supply DC 5V, 3.0A
- Weight: 10.8 oz. (0.3kg)

Technical Specifications (continued)

Warranty:

- 3 year (depends on D-Link global warranty policy)

Wireless Data Rates with Automatic Fallback:

- 54 Mbps
- 48 Mbps
- 36 Mbps
- 24 Mbps
- 22 Mbps
- 18 Mbps
- 12 Mbps
- 11 Mbps
- 9 Mbps
- 6 Mbps
- 5.5 Mbps
- 2 Mbps
- 1 Mbps

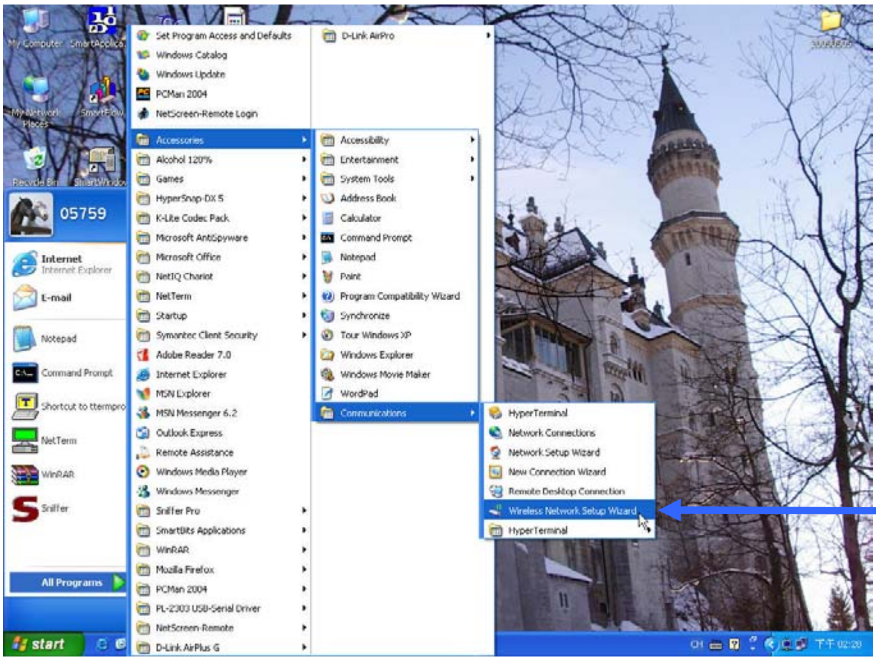
Receiver Sensitivity:

- 54Mbps OFDM, 10% PER, -68dBm
- 48Mbps OFDM, 10% PER, -68dBm
- 36Mbps OFDM, 10% PER, -75dBm
- 24Mbps OFDM, 10% PER, -79dBm
- 22Mbps PBCC, 8% PER, -80dBm
- 18Mbps OFDM, 10% PER, -82dBm
- 12Mbps OFDM, 10% PER, -84dBm
- 11Mbps CCK, 8% PER, -82dBm
- 9Mbps OFDM, 10% PER, -87dBm
- 6Mbps OFDM, 10% PER, -88dBm
- 5.5Mbps CCK, 8% PER, -85dBm
- 2Mbps QPSK, 8% PER, -86dBm
- 1Mbps BPSK, 8% PER, -89dBm

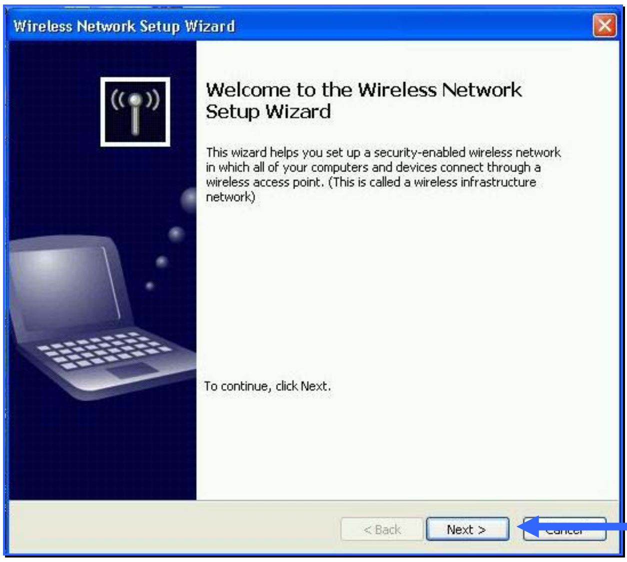
Appendix

WCN and the Wireless Setup Wizard

WCN or **W**indows **C**onnect **N**ow technology has been recently incorporated by D-Link to quickly aid the user in setting up a secure wireless environment. Combining the new WCN technology incorporated by Windows and only available through a PC that has a wireless NIC card and is running the Windows XP Operating System with Service Pack 2 installed, the user will configure the wireless settings only once and then save it to a USB flash drive. Once saved, the user may insert this flash drive into any device on the network that is running wirelessly and the settings will automatically upload to that device. No more configurations are necessary and all devices will have the identical access information and wireless information necessary to work smoothly over your internal LAN. See the explanation below for a better understanding of how to set up your WCN wireless function.



In Windows XP SP2, click **Start > All Programs > Accessories > Communications > Windows Network Setup Wizard** to open the wizard's front page, as seen below.



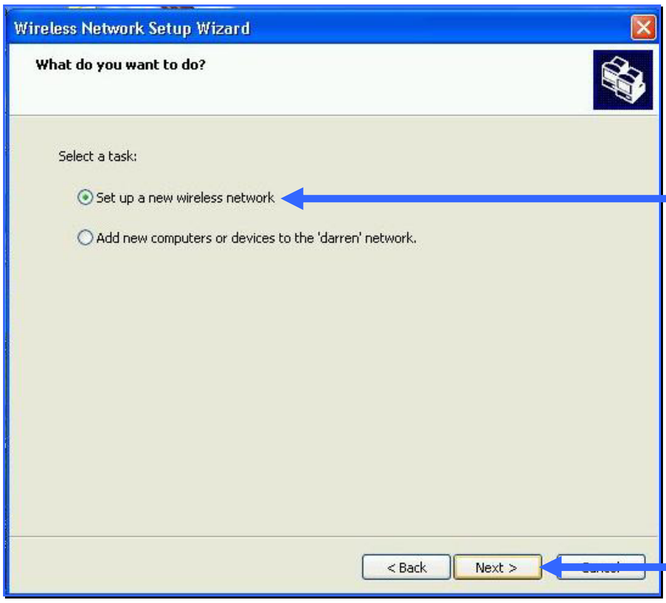
Wireless Network Setup Wizard

Welcome to the Wireless Network Setup Wizard

This wizard helps you set up a security-enabled wireless network in which all of your computers and devices connect through a wireless access point. (This is called a wireless infrastructure network)

To continue, click Next.

Click **Next**.



What do you want to do?

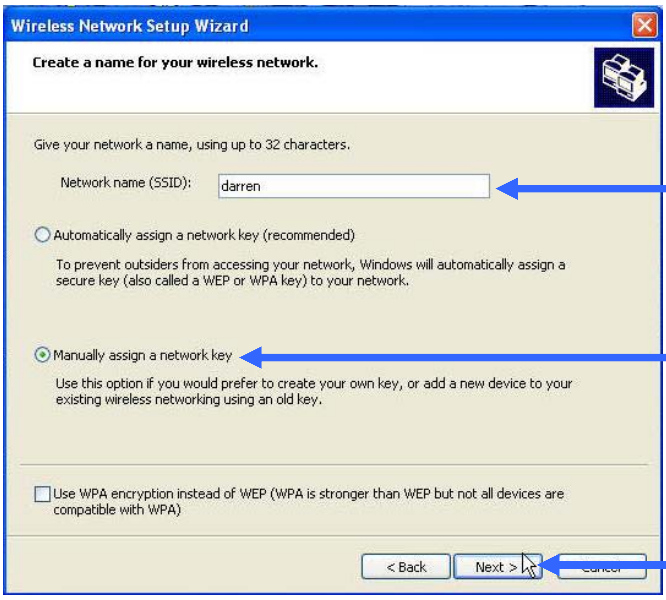
Select a task:

● Set up a new wireless network

○ Add new computers or devices to the 'darren' network.

Choose “**Set up a new wireless network**”.

Click **Next**.



Create a name for your wireless network.

Give your network a name, using up to 32 characters.

Network name (SSID): darren

○ Automatically assign a network key (recommended)

To prevent outsiders from accessing your network, Windows will automatically assign a secure key (also called a WEP or WPA key) to your network.

● Manually assign a network key

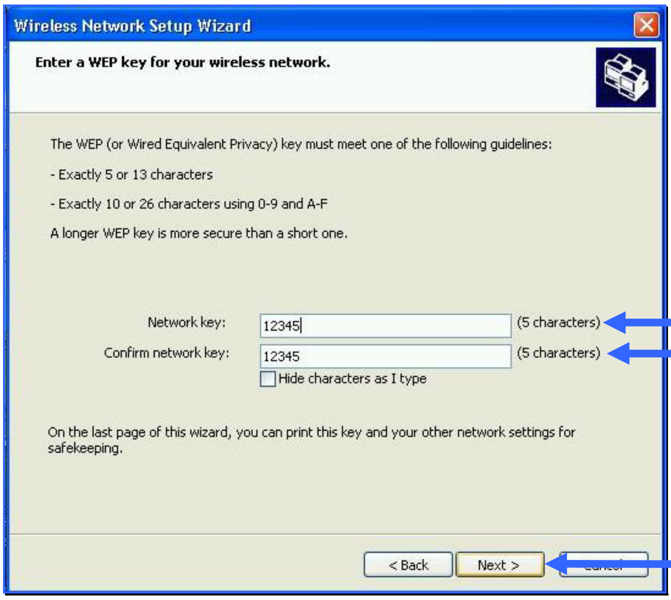
Use this option if you would prefer to create your own key, or add a new device to your existing wireless networking using an old key.

□ Use WPA encryption instead of WEP (WPA is stronger than WEP but not all devices are compatible with WPA)

Enter a network name of up to 32 characters to identify your wireless network. This name will be common to all users on the wireless LAN.

Choose “**Manually assign a network key**” which will be configured in the next window.

Click **Next**.



Enter a WEP key for your wireless network.

The WEP (or Wired Equivalent Privacy) key must meet one of the following guidelines:

- Exactly 5 or 13 characters
- Exactly 10 or 26 characters using 0-9 and A-F

A longer WEP key is more secure than a short one.

Network key: 12345 (5 characters)

Confirm network key: 12345 (5 characters)

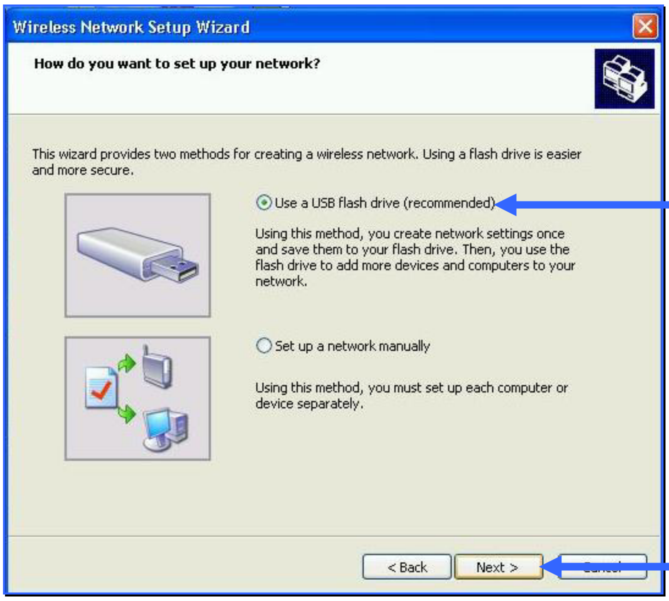
□ Hide characters as I type

On the last page of this wizard, you can print this key and your other network settings for safekeeping.

Choose a key that will be shared among users on your LAN. There are certain guidelines to choosing this key, as stated on the screen to the left.

Confirm the network key by retyping it in the following field.

Once entered, click **Next**.



Wireless Network Setup Wizard

How do you want to set up your network?

This wizard provides two methods for creating a wireless network. Using a flash drive is easier and more secure.

● Use a USB flash drive (recommended)

Using this method, you create network settings once and save them to your flash drive. Then, you use the flash drive to add more devices and computers to your network.

○ Set up a network manually

Using this method, you must set up each computer or device separately.

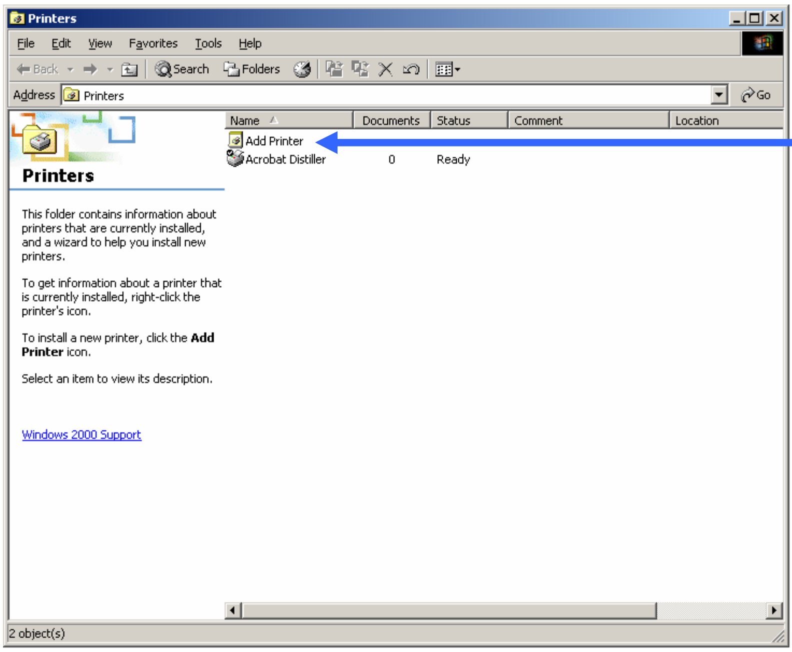
Insert the USB drive into a USB port on the computer, choose “**Use a USB flash drive**”.

Click **Next**.

The settings will the automatically be uploaded to your USB flash drive. Once saved the user is to unplug the device, in the proper method, and then plug that USB flash drive into all devices that will be accessing the wireless LAN. Each device will upload the configurations automatically and be instantly accessible on the wireless LAN.

Installing a Printer on your DI-624S

The Di-624S can be used as a print server for devices on your LAN. Once you have installed the USB printer through the router, the user must set up the computer on the LAN for the printer as well. The following explanation will guide you through the steps needed to do this. Remember to enter the same **Queue Name** on the PC as your router displays or the printer will not function properly. To begin the process, open the Printer window on your PC by clicking **Start > Settings > Printers,** which will open the following window.



Printers

This folder contains information about printers that are currently installed, and a wizard to help you install new printers.

To get information about a printer that is currently installed, right-click the printer's icon.

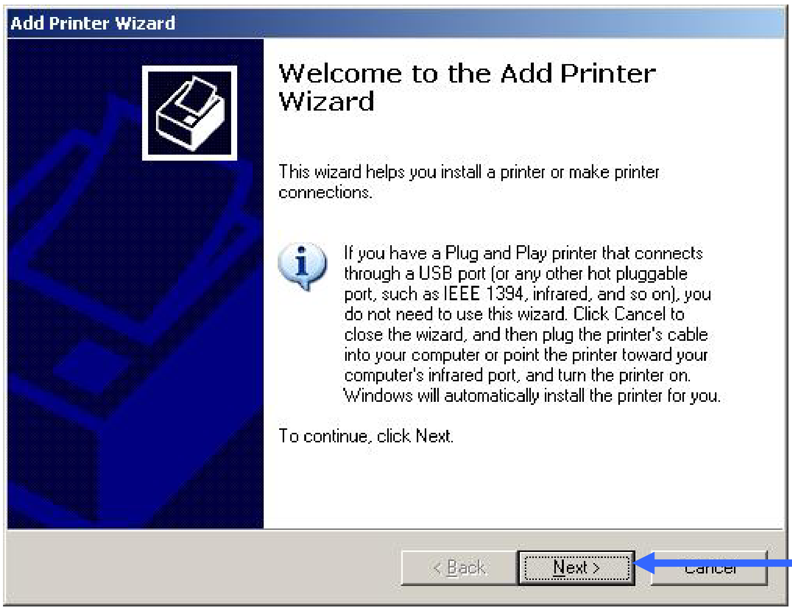
To install a new printer, click the **Add Printer** icon.

Select an item to view its description.

Windows 2000 Support

Name	Documents	Status	Comment	Location
Add Printer				
Acrobat Distiller	0	Ready		

Double click "**Add Printer**" which will open the "**Welcome to the Add Printer Wizard**".



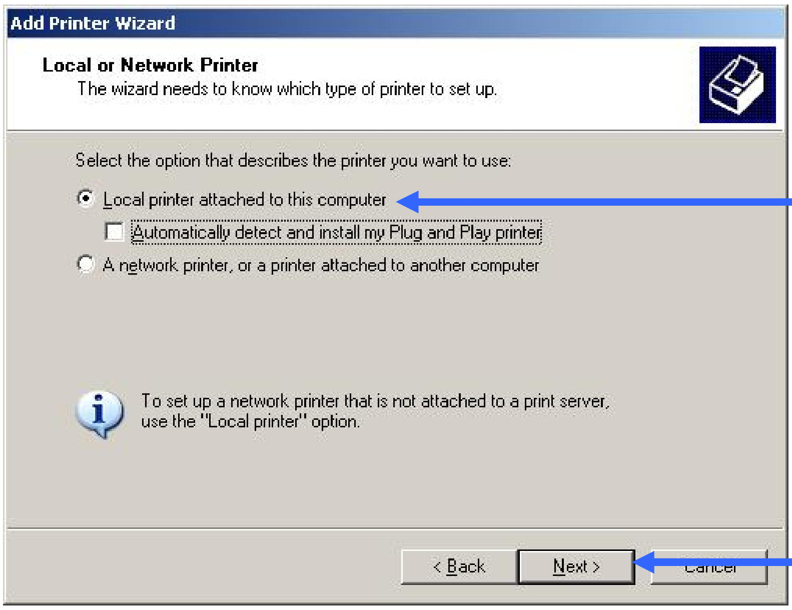
Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

Click **Next**.



Local or Network Printer
The wizard needs to know which type of printer to set up.

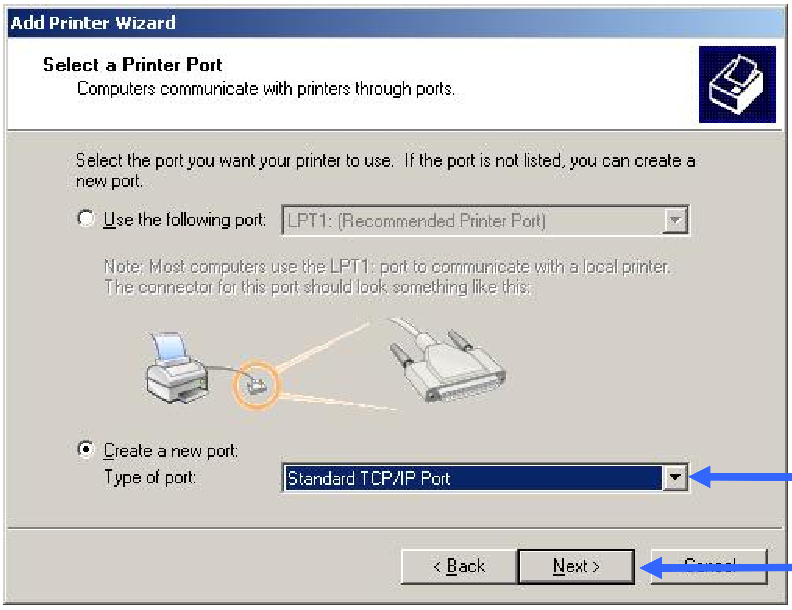
Select the option that describes the printer you want to use:

● Local printer attached to this computer
□ Automatically detect and install my Plug and Play printer
○ A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

In the **Local or Network Printer** window, choose "**Local printer attached to this computer**".

Click **Next.**



Select a Printer Port
Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

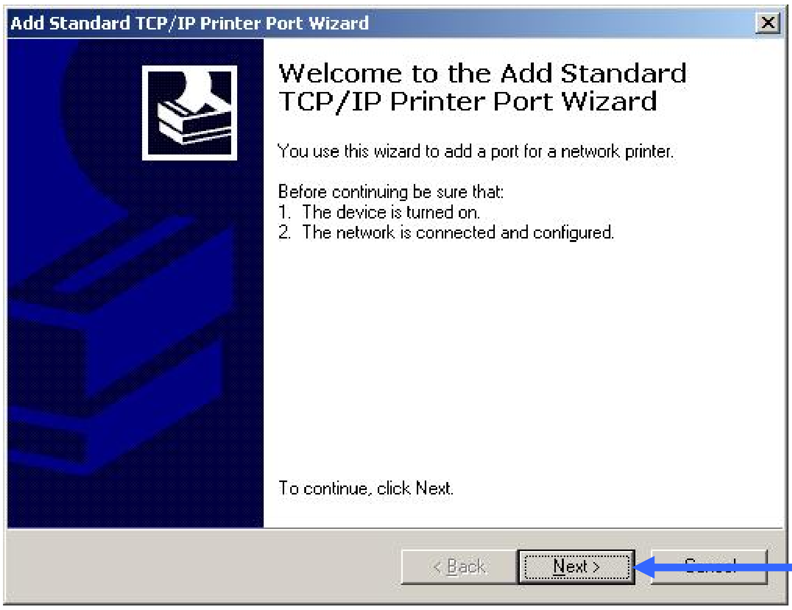
○ Use the following port: LPT1: (Recommended Printer Port)

Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

● Create a new port:
Type of port: Standard TCP/IP Port

Then the user must choose the type of installation for the wizard. Choose "**Create a new port**" and use the pull-down menu to select "**Standard TCP/IP Port**".

Click **Next.**



Welcome to the Add Standard TCP/IP Printer Port Wizard

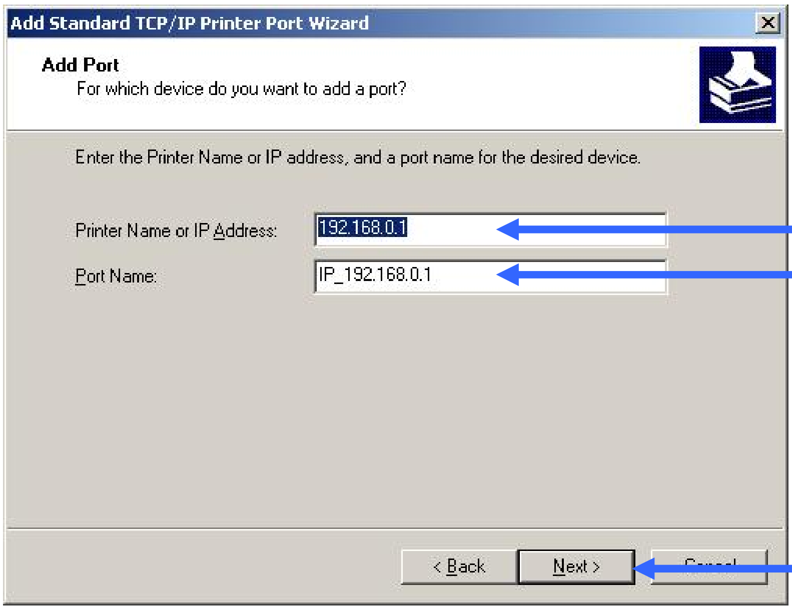
You use this wizard to add a port for a network printer.

Before continuing be sure that:
1. The device is turned on.
2. The network is connected and configured.

To continue, click Next.

The next screen to appear is the "**Welcome to the Add Standard TCP/IP Printer Port Wizard**". Make sure that the printer is turned on and the network is properly configured.

Click **Next.**



Add Standard TCP/IP Printer Port Wizard

Add Port

For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

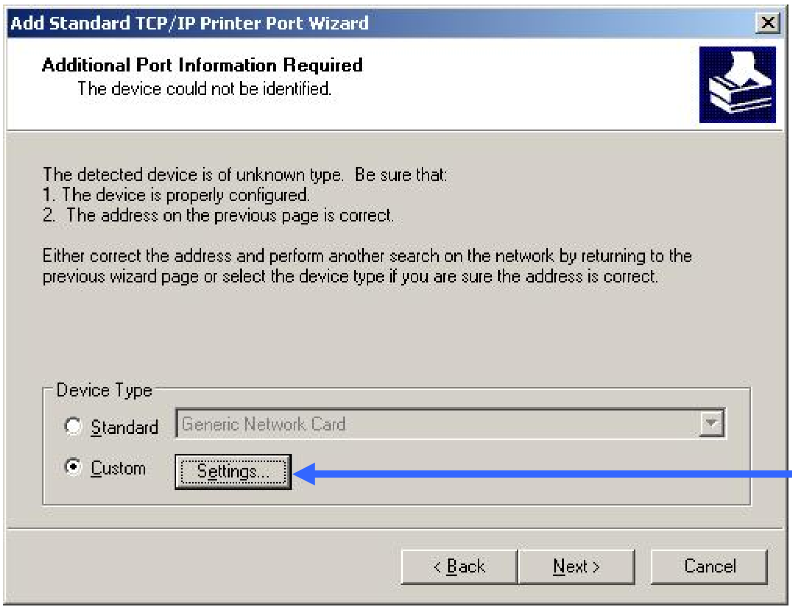
Printer Name or IP Address: 192.168.0.1

Port Name: IP_192.168.0.1

Enter the IP address (default: 192.168.0.1) of the DI-624S to the "**Printer Name or IP Address**" field.

In the **Port Name** field, be sure add a name to the router IP address to differentiate it from other devices.(ex: IP_192.168.0.1dlink)

Click **Next**.



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The detected device is of unknown type. Be sure that:
1. The device is properly configured.
2. The address on the previous page is correct.

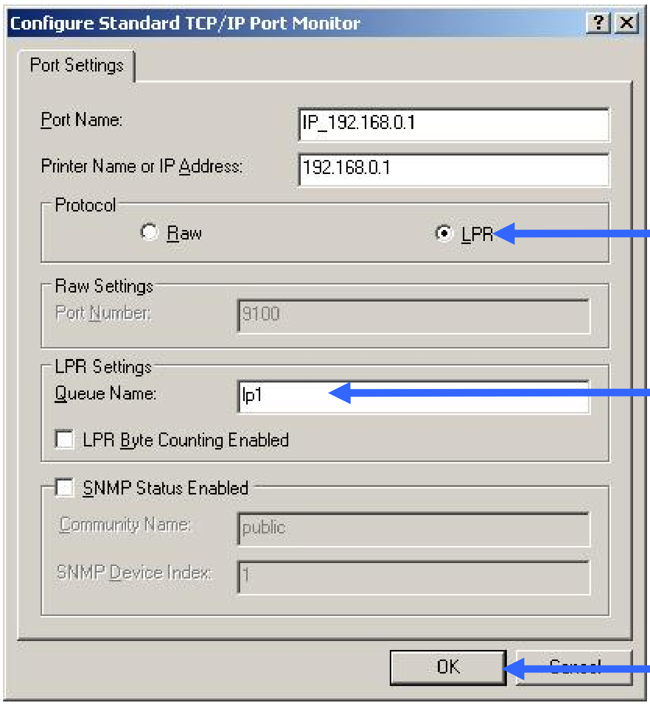
Either correct the address and perform another search on the network by returning to the previous wizard page or select the device type if you are sure the address is correct.

Device Type

○ Standard Generic Network Card

● Custom Settings...

After clicking **Next**, the Wizard requires additional information to complete the process. In the **Additional Port Information Required** window, click **Custom > Settings**. In the following window, the user will add the **Queue Name**.



Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.0.1

Printer Name or IP Address: 192.168.0.1

Protocol

○ Raw ● LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name: lp1

□ LPR Byte Counting Enabled

□ SNMP Status Enabled

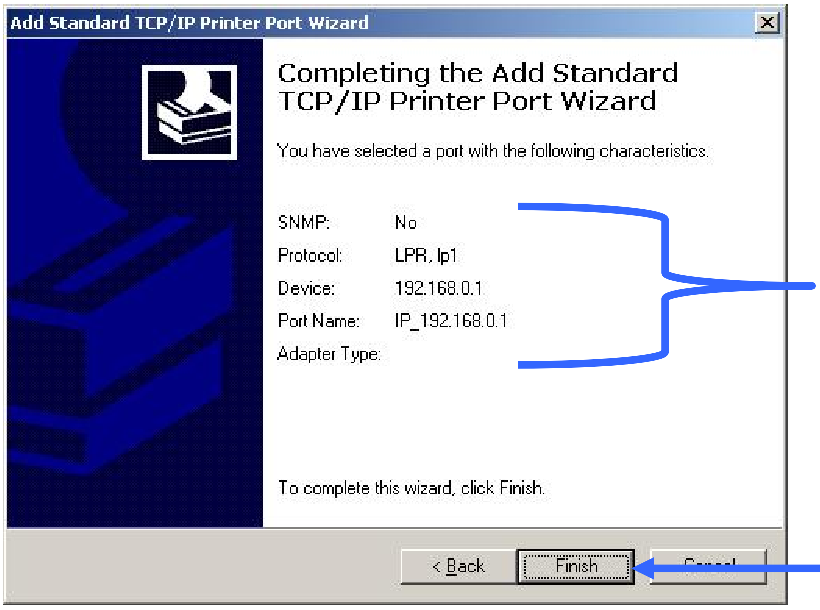
Community Name: public

SNMP Device Index: 1

In the "**Configure Standard TCP/IP Port Monitor**" window, first Choose **LPR** in the **Protocol** field.

Next, add the **Queue Name** that was automatically generated for you by your DI-624S (in this case, lp1).

Click **OK** to continue.



Completing the Add Standard TCP/IP Printer Port Wizard

You have selected a port with the following characteristics.

SNMP:	No
Protocol:	LPR, lp1
Device:	192.168.0.1
Port Name:	IP_192.168.0.1
Adapter Type:	

To complete this wizard, click Finish.

The final window will be the "**Completing the Add Standard TCP/IP Printer Port Wizard**" window, as shown to the left. Here you can view the properties of the added printer, including the IP address, protocol and queue name.

Click **Finish** to complete the wizard.

Warranty and Registration
(USA only)

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

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

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

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

- Hardware (excluding power supplies and fans) Three (3) Years
- Power Supplies and Fans One (1) Year
- Spare parts and spare kits Ninety (90) days

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

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

Non-Applicability of Warranty: The Limited Warranty provided hereunder for hardware and software of D-Link's products will not be applied to and does not cover any refurbished product and any product purchased through the inventory clearance or liquidation sale or other sales in which D-Link, the sellers, or the liquidators expressly disclaim their warranty obligation pertaining to the product and in that case, the product is being sold "As-Is" without any warranty whatsoever including, without limitation, the Limited Warranty as described herein, notwithstanding anything stated herein to the contrary.

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

- The customer must submit with the product as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.

- The original product owner must obtain a Return Material Authorization ("RMA") number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

- After an RMA number is issued, the defective product must be packaged securely in the original or other suitable shipping package to ensure that it will not be damaged in transit, and the RMA number must be prominently marked on the outside of the package. Do not include any manuals or accessories in the shipping package. D-Link will only replace the defective portion of the Product and will not ship back any accessories.

- The customer is responsible for all in-bound shipping charges to D-Link. No Cash on Delivery ("COD") is allowed. Products sent COD will either be rejected by D-Link or become the property of D-Link. Products shall be fully insured by the customer. D-Link will not be held responsible for any packages that are lost in transit to D-Link. The repaired or replaced packages will be shipped to the customer via UPS Ground or any common carrier selected by D-Link, with shipping charges prepaid. Expedited shipping is available if shipping charges are prepaid by the customer and upon request.

- Return Merchandise Ship-To Address

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

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

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

Disclaimer of Other Warranties: EXCEPT FOR THE LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND WHATSOEVER INCLUDING, WITHOUT LIMITATION, ANY WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IF ANY IMPLIED WARRANTY CANNOT BE DISCLAIMED IN ANY TERRITORY WHERE A PRODUCT IS SOLD, THE DURATION OF SUCH IMPLIED WARRANTY SHALL BE LIMITED TO NINETY (90) DAYS. EXCEPT AS EXPRESSLY COVERED UNDER THE LIMITED WARRANTY PROVIDED HEREIN, THE ENTIRE RISK AS TO THE QUALITY, SELECTION AND PERFORMANCE OF THE PRODUCT IS WITH THE PURCHASER OF THE PRODUCT.

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

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

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

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

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

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

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

IC Statement: The Class B digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulation.

For detailed warranty outside the United States, please contact corresponding local D-Link office.

Register your D-Link product online at http://support.dlink.com/register/

(07/04/2005)