D-Link®
Building Networks for People

Manual

Version 1.0

DI-624S

Wireless 108G USB Storage Router

Table of Contents

Package Contents 4
System Requirements 4
Introduction 5
Connections 6
LEDs 7
Features 8
Wireless Basics 9
Standards-Based Technology 10
Installation Considerations 11
Getting Started 12
Using the Configuration Menu 13
Home 13
Wireless 14
WPA-PSK 15
Wan 16
Dynamic IP Address 16
Static IP Address 17
PPPoE 18
LAN 21
DHCP 22
Advanced 23
Virtual Server 23
Applications 26
Filters 27
IP Filters 27
MAC Filter 28
TMSS Home 29
Parental Controls 30
General Parental Controls 30
Per-User Parental Controls 32
Add User 33
Firewall 34
DMZ 35
Performance 36
Folder 38
Tools 40
Admin 40
Time 41
System 42
Firmware 43
DDNS 44
Misc 45

Cable Test *46*
Device Info *47*
Status 48
Log *48*
Log Settings 49
Stats *50*
Wireless *50*
Networking Basics 51
Troubleshooting 66
Technical Specifications 73
Frequently Asked Questions 76
Contacting Technical Support 102
Warranty 103
Registration 106

Package Contents

D-Link *Air*Plus *Xtreme G™* DI-624S

- High-Speed 2.4GHz Wireless 108G Storage Router
- Power Adapter-DC 5V, 2.5A
- Manual and Warranty on CD-ROM
- Quick Installation Guide
- Ethernet Cable (All the Ethernet ports on the DI-624S 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

- Computers with Windows, Macintish, or Linux-based operating systems
  - 200MHz Processor
  - 64MB Memory
  - CD-ROM Drive
  - Ethernet Adapter with TCP/IP Protocol Installed
- Cable or DSL Modem with an Ethernet Port
- Internet Explorer Version 6.0 or Netscape Havigator Version 7.0 or above

Introduction

The D-Link *Air*Plus *Xtreme G*™ DI-624S High-Speed Wireless Storage Router is an 802.11g high-performance, wireless router that supports high-speed wireless networking at home, at work or in public places.

Unlike most routers, the DI-624S provides data transfers at up to 108 Mbps (compared to the standard 54Mbps) when used with other D-Link *Air*Plus *Xtreme G*™ products. The 802.11g standard is backwards compatible with 802.11b products. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 802.11g's speed when you mix 802.11b and 802.11g devices, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11b network. You may choose to slowly change your network by gradually replacing the 802.11b devices with 802.11g devices .

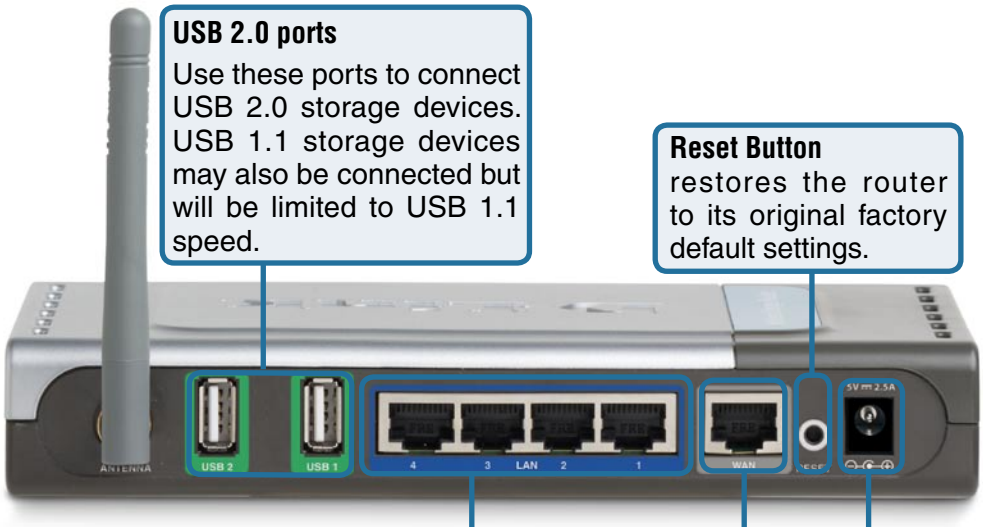
For home users that will not incorporate a RADIUS server in their network, the security for the DI-624S, used in conjunction with other 802.11g products, will still be much stronger than ever before. Utilizing the **Pre Shared Key mode** of WPA, the DI-624S will obtain a new security key every time it 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.

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 ports
Use these ports to connect USB 2.0 storage devices. USB 1.1 storage devices may also be connected but will be limited to USB 1.1 speed.

Reset Button
restores the router to its original factory default settings.

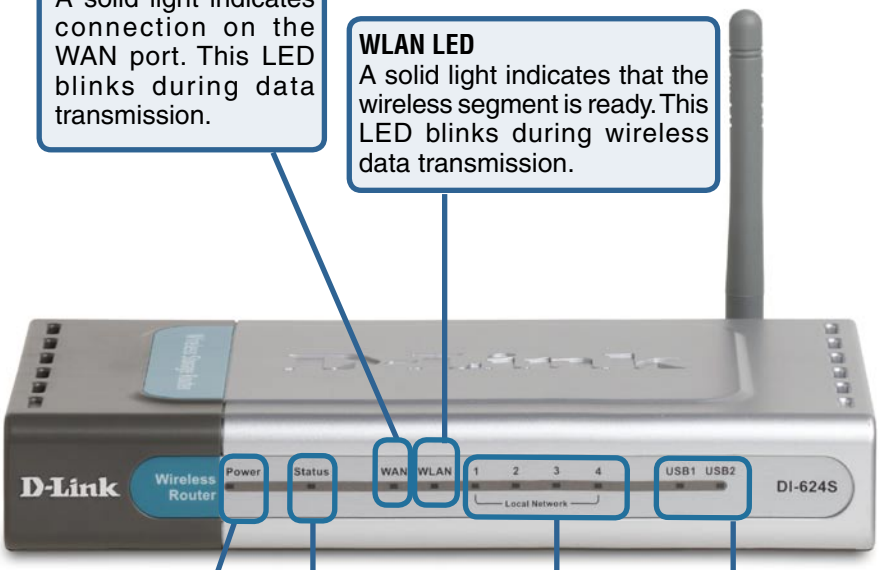


Auto MDI/MDIX LAN ports automatically sense the cable type when connecting to Ethernet-enabled computers.

Auto MDI/MDIX WAN port is the connection for the Ethernet cable to the Cable or DSL modem

Receptor for the **Power Adapter**

LEDs



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

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

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

STATUS
A blinking light indicates that the DI-624S is ready.

USB LED
A solid light indicates that a connection is enabled.

LOCAL NETWORK LED
A solid light indicates a connection to an Ethernet-enabled computer on ports 1-4. This LED blinks during data transmission.

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 11Mbps.
- **WPA** (Wi Fi Protected Access) authorizes and identifies users based on a secret key that changes automatically at a regular interval, for example:
  - **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.
- Utilizes **OFDM** technology (**O**rthogonal **F**requency **D**ivision **M**ultiplexing).
- User-friendly configuration and diagnostic utilities.
- Operates in the 2.4GHz to 2.462GHz frequency range.
- Connects multiple computers to a Broadband (Cable or DSL) modem to share the Internet connection.
  - Advanced Firewall features:
  - MAC Filtering
  - IP Filtering
  - Scheduling
- DHCP server enables all networked computers to automatically receive IP addresses.
- Web-based interface for Managing and Configuring.
- Access Control to manage users on the network.
- Supports special applications that require multiple connections.
- Equipped with 4 10/100 Ethernet ports, 2 USB ports, 1 WAN port, Auto MDI/MDIX.

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 108G Storage 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 54Mbps 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** (**O**rthogonal **F**requency **D**ivision **M**ultiplexing) 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 802.11b devices. This means that if you have an existing 802.11b network, the devices in that network will be compatible with 802.11g devices at speeds of up to 11Mbps in the 2.4GHz range.

Installation Considerations

The D-Link *Air*Plus *Xtreme G*™ 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.

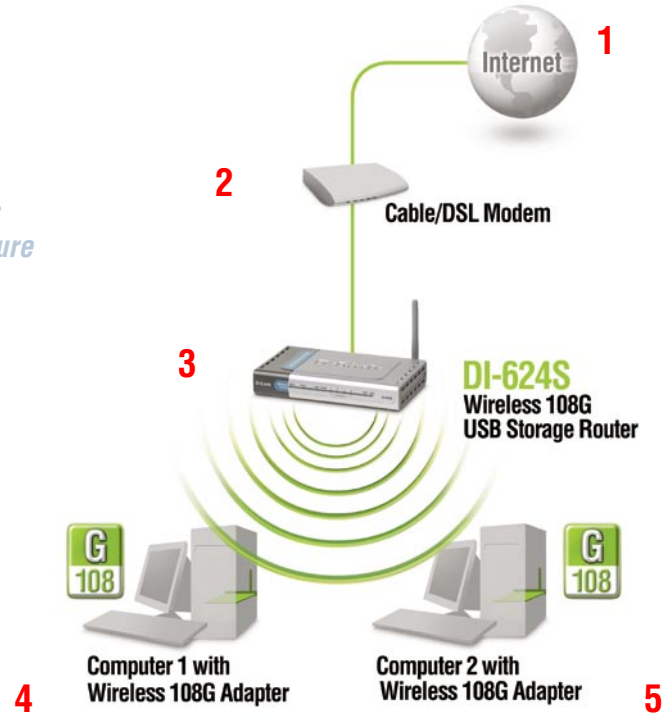
2. Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or 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* Xtreme 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 Broadband 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 *Air*Plus *Xtreme G* DWL-G520 wireless PCI adapter into an available PCI slot on your 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. You may also install the DWL-G510, or the DWL-AG530. *(See the printed Quick Installation Guide included with the network adapter.)*

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

Using the Configuration Menu

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 at right:

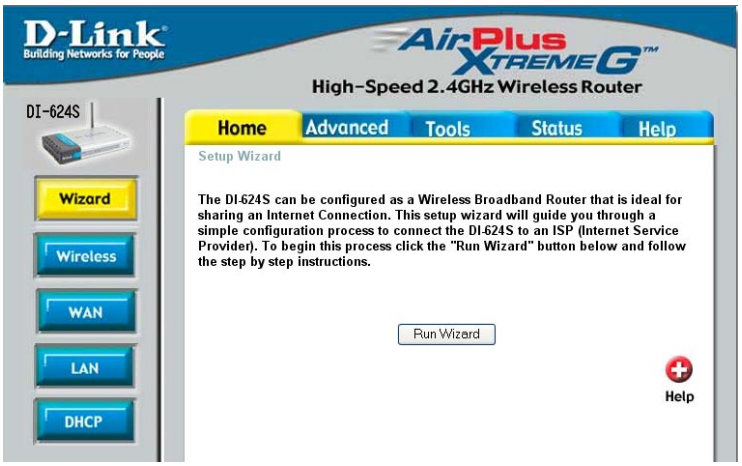
- Open the web browser
- Type in the **IP Address** of the Router (http://192.168.0.1)

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

- Type **admin** in the **User Name** field
- Leave the **Password** blank
- Click **OK**

Home > Wizard

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



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.

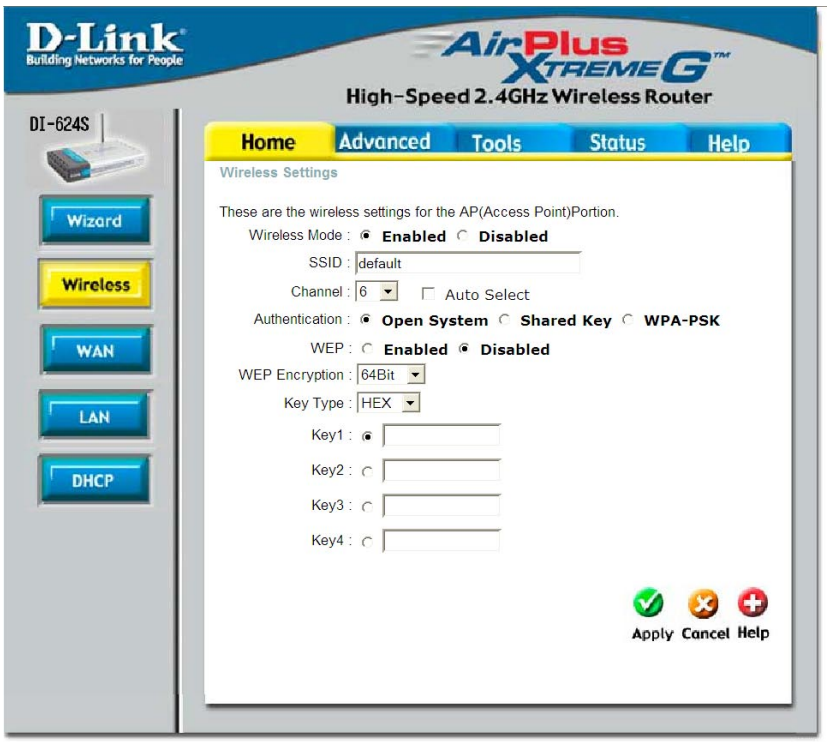
Apply — Clicking **Apply** will save changes made to the page

Cancel — Clicking **Cancel** will clear changes made to the page

Help — Clicking **Help** will bring up helpful information regarding the page

Restart — Clicking **Restart** will restart the router. (Necessary for some changes.)

Home > Wireless



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

Channel: **6** is the default channel. All devices on the network must share the same channel. *(Note: The wireless adapters will automatically scan and match the wireless setting.)*

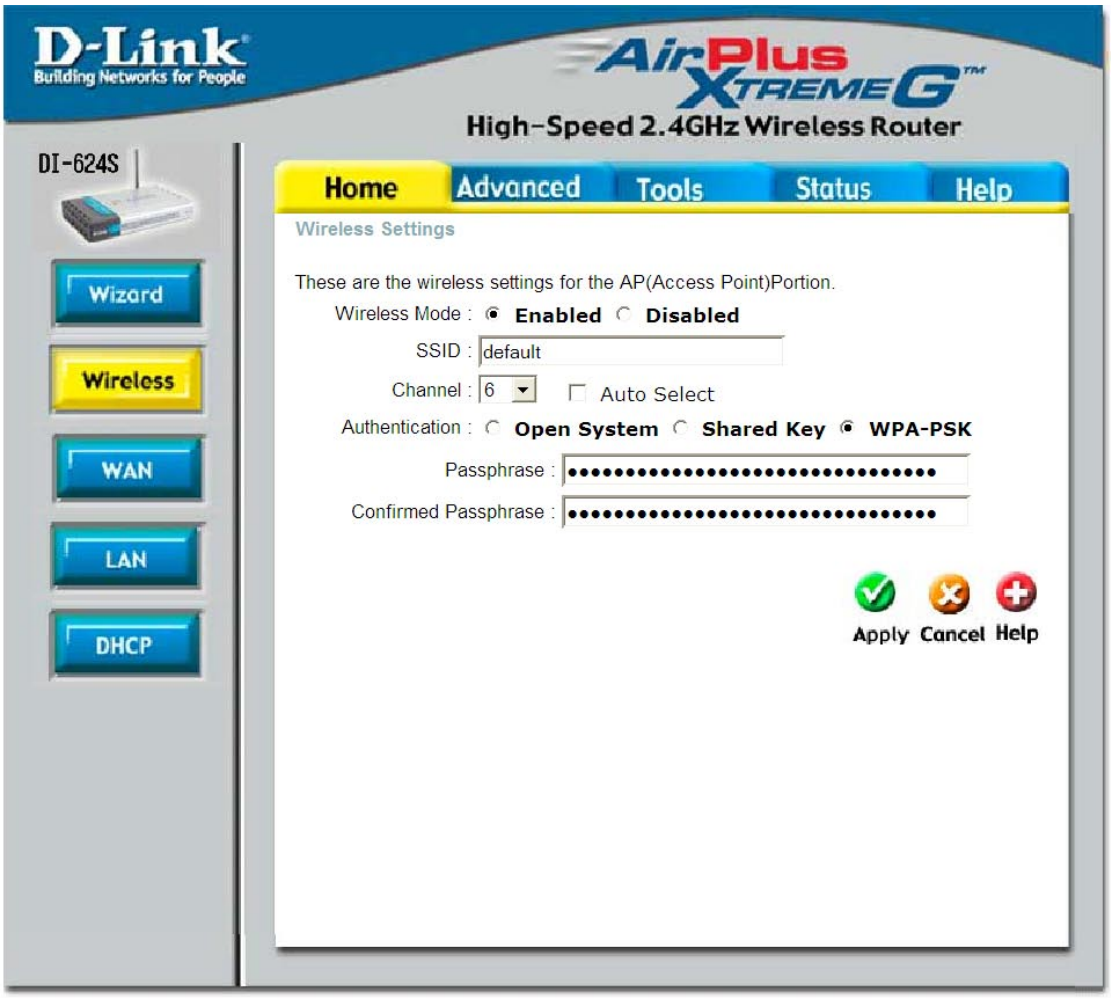
Authentication: Choose **Open System**, **Shared Key**, or **WPA-PSK**.

WEP Encryption: Select the level of encryption desired: 64-bit, or 128-bit.

Key Type: Select **HEX** or **ASCII**.

Keys 1-4: Input up to 4 WEP keys; select the one you wish to use.

Home > Wireless > WPA-PSK



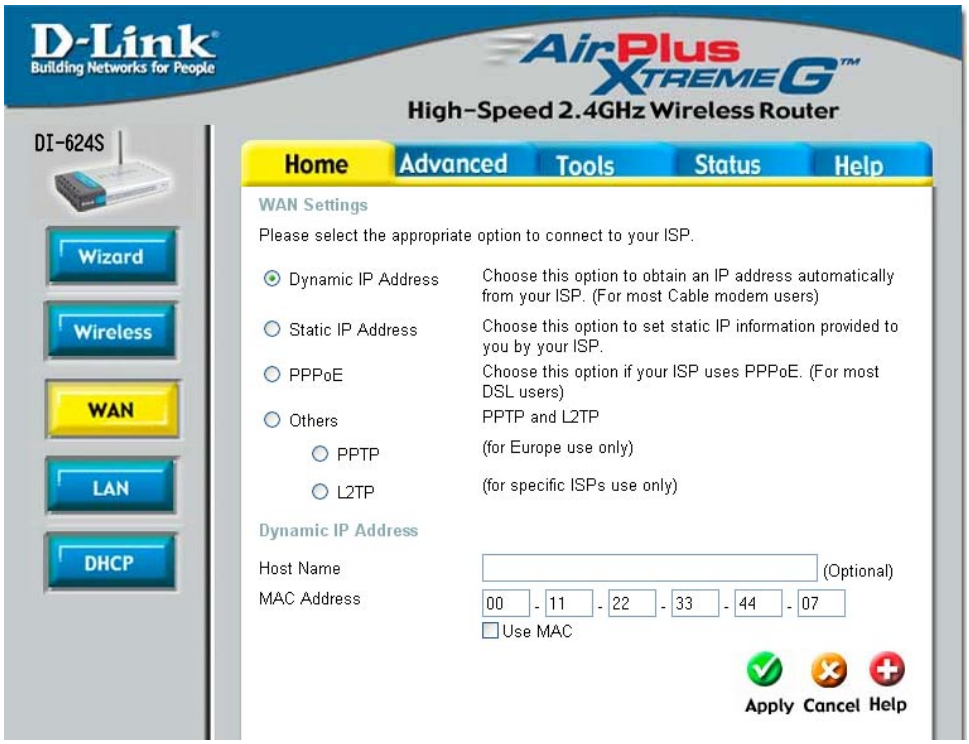
SSID: Service Set Identifier (SSID) is the name designated for a specific wireless local area network (WLAN). The SSID's factory default setting is **default.** The SSID can be easily changed to connect to an existing wireless network or to establish a new wireless network.

Channel: **6** is the default channel. All devices on the network must share the same channel. Select **Auto Select** to have the router automatically choose the best channel. *(Note: The wireless adapters will automatically scan and match the wireless setting.)*

Passphrase: Enter the passphrase to be used for the WPA-PSK Aunthentication.

Confirmed Passphrase: Reenter the passphrase to be used for the WPA-PSK Aunthentication.

Home > WAN > Dynamic IP Address



Dynamic IP Address: Choose Dynamic IP Address to obtain IP Address information automatically from your ISP. Select this option if your ISP does not give you any IP numbers to use. This option is commonly used for Cable modem services.

Host Name: The Host Name may be required by some ISPs.

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.

Use MAC: Checking this checkbox will allow you to enter the MAC address of the Ethernet Card installed by your ISP, and replace the WAN MAC address of the router. It is not recommended that you change the default MAC address unless required by your ISP.

Home > WAN > Static IP Address

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: Enter the gateway IP Address provided by your ISP.

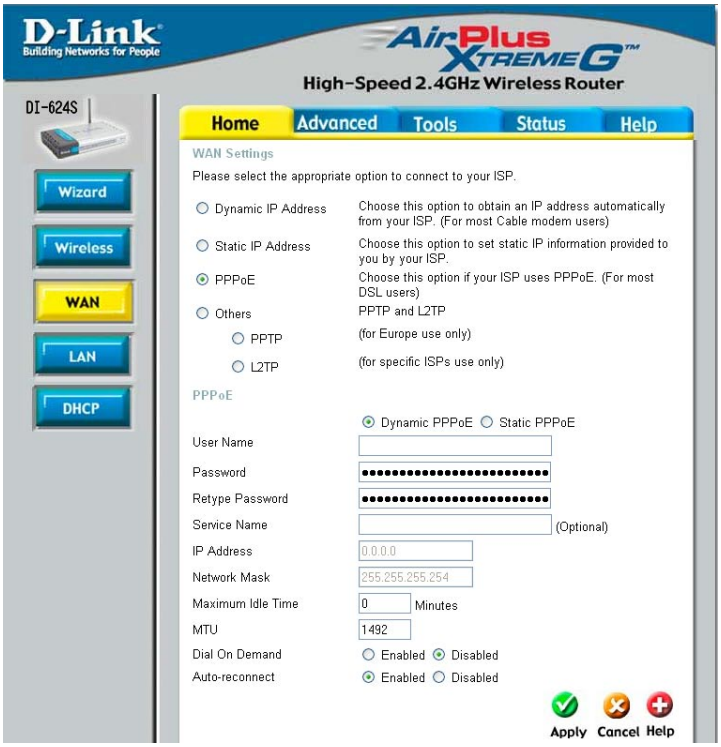
Primary DNS Address: Input the primary DNS (Domain Name Server) IP address provided by your ISP.

Secondary DNS Address: This is optional.

Home > WAN > PPPoE

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

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

Dynamic PPPoE: receive an IP Address automatically from your ISP.

Static PPPoE: you have an assigned (static) IP Address.

User Name: Your PPPoE username provided by your ISP.

Password: Enter the PPPoE password.

Retype Password: Re-enter the PPPoE password.

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.

Network Mask: The network mask of the PPPoE interface.

Maximum Idle Time: Either set the value for idle time to zero or enable Auto-reconnect to disable this feature.

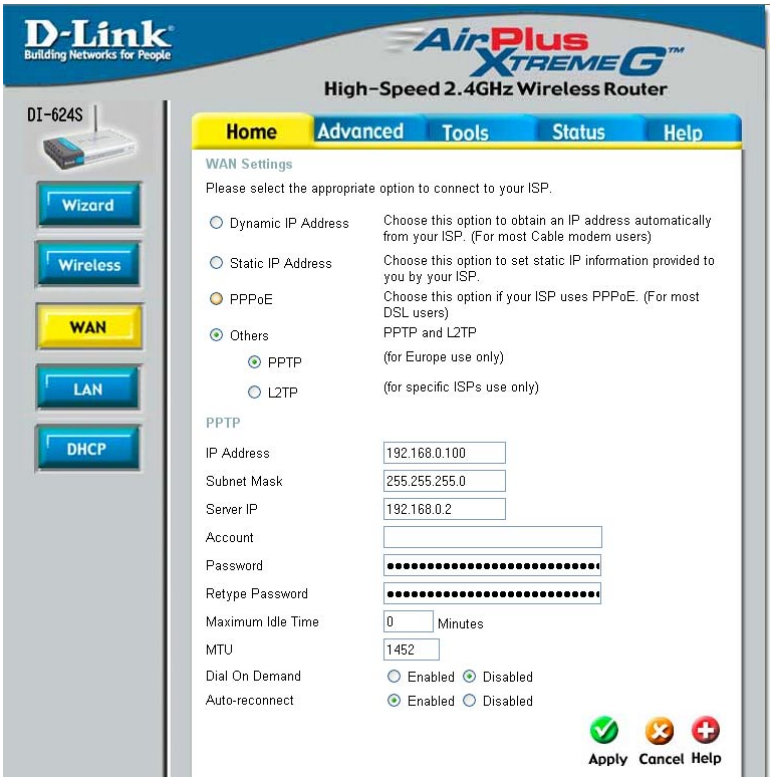
MTU: Maximum Transmission Unit-1492 is the default setting-you may need to change the MTU for optimal performance with your specific ISP.

Home > WAN > PPPoE *(continued)*

Dial on Demand: If **Enabled**, the DI-624S will connect to your ISP after you initiate an Internet connection, such as opening an Internet browser.

Auto-reconnect: If **Enabled**, the DI-624S will automatically connect to your ISP after your system is restarted or if the PPPoE connection is dropped.

Home > WAN > Others > PPTP



PPTP: Choose this option if your ISP uses PPTP (Point-to-Point Tunneling Protocol).

IP Address: Enter the static IP Address for the PPTP connection.

Subnet Mask: The subnet mask of the PPTP interface.

Server IP: Enter the Service Name provided by your ISP (optional).

Account: Your PPTP account name provided by your ISP.

Password: Enter the PPTP password.

Retype Password: Re-enter the PPTP password.

Maximum Idle Time: Either set the value for idle time to zero or enable Auto-reconnect to disable this feature.

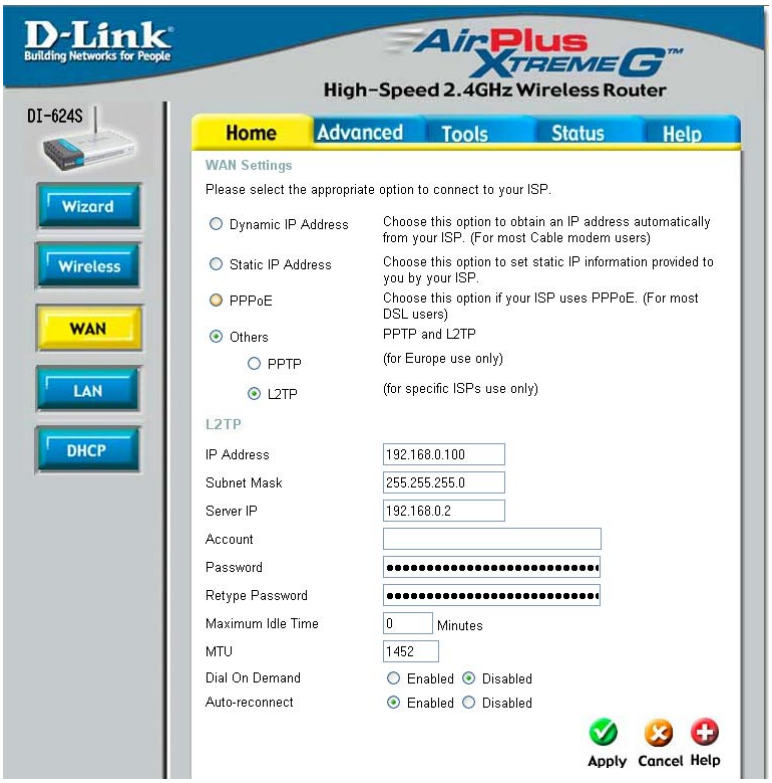
Home > WAN > Others > PPTP *(continued)*

MTU: Maximum Transmission Unit-1492 is the default setting-you may need to change the MTU for optimal performance with your specific ISP.

Dial on Demand: If **Enabled**, the DI-624S will connect to your ISP after you initiate an Internet connection, such as opening an Internet browser.

Auto-reconnect: If **Enabled**, the DI-624S will automatically connect to your ISP after your system is restarted or if the PPTP connection is dropped.

Home > WAN > Others > L2TP



L2TP: Choose this option if your ISP uses L2TP (Layer 2 Tunneling Protocol).

IP Address: Enter the static IP Address for the L2TP connection.

Subnet Mask: The subnet mask of the L2TP interface.

Server IP: Enter the Server IP provided by your ISP (optional).

Account: Your L2TP account name provided by your ISP.

Password: Enter the L2TP password.

Retype Password: Re-enter the L2TP password.

Maximum Idle Time: Either set the value for idle time to zero or enable Auto-reconnect to disable this feature.

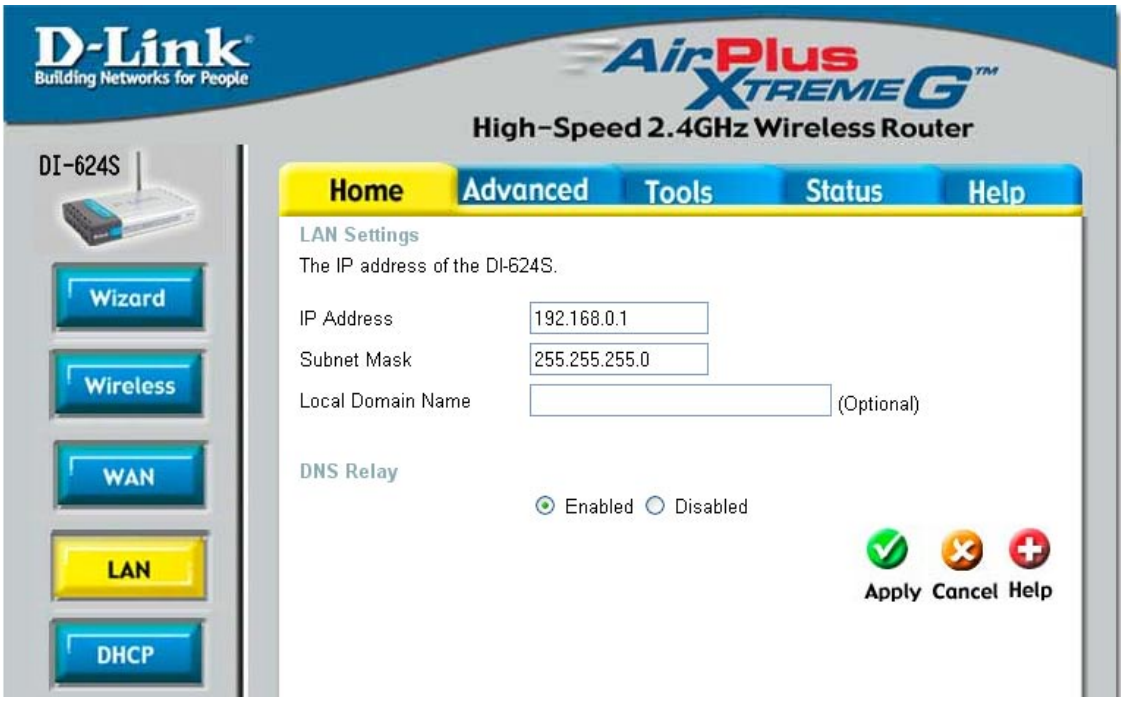
Home > WAN > Others > L2TP *(continued)*

MTU: Maximum Transmission Unit-1492 is the default setting-you may need to change the MTU for optimal performance with your specific ISP.

Dial on Demand: If **Enabled**, the DI-624S will connect to your ISP after you initiate an Internet connection, such as opening an Internet browser.

Auto-reconnect: If **Enabled**, the DI-624S will automatically connect to your ISP after your system is restarted or if the PPTP connection is dropped.

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. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

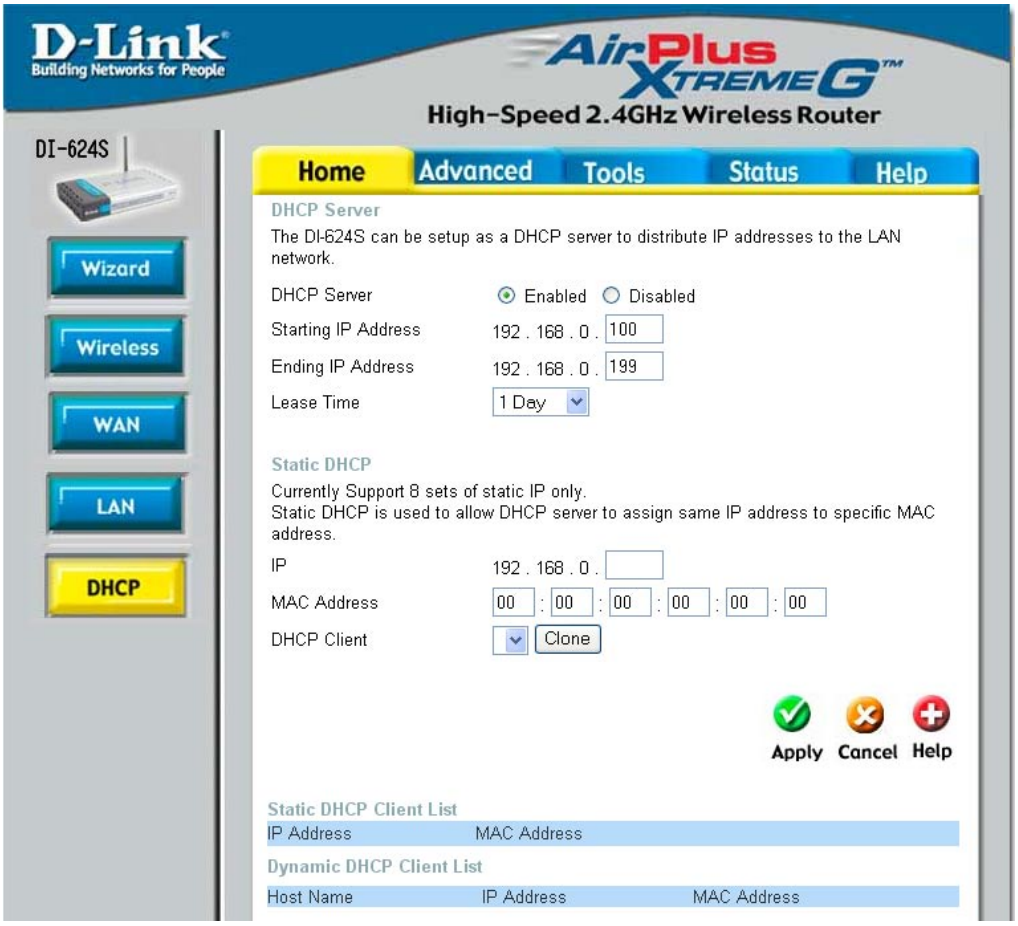
IP Address: The IP address of the LAN interface. The default IP address is: **192.168.0.1**

Subnet Mask: The subnet mask of the LAN interface.
The default subnet mask is **255.255.255.0**

Local Domain Name: This field is optional. Enter in the local domain name.

DNS Relay: If **Enabled**, the router will use its own IP afddress as the DNS server for the DHCP clients.

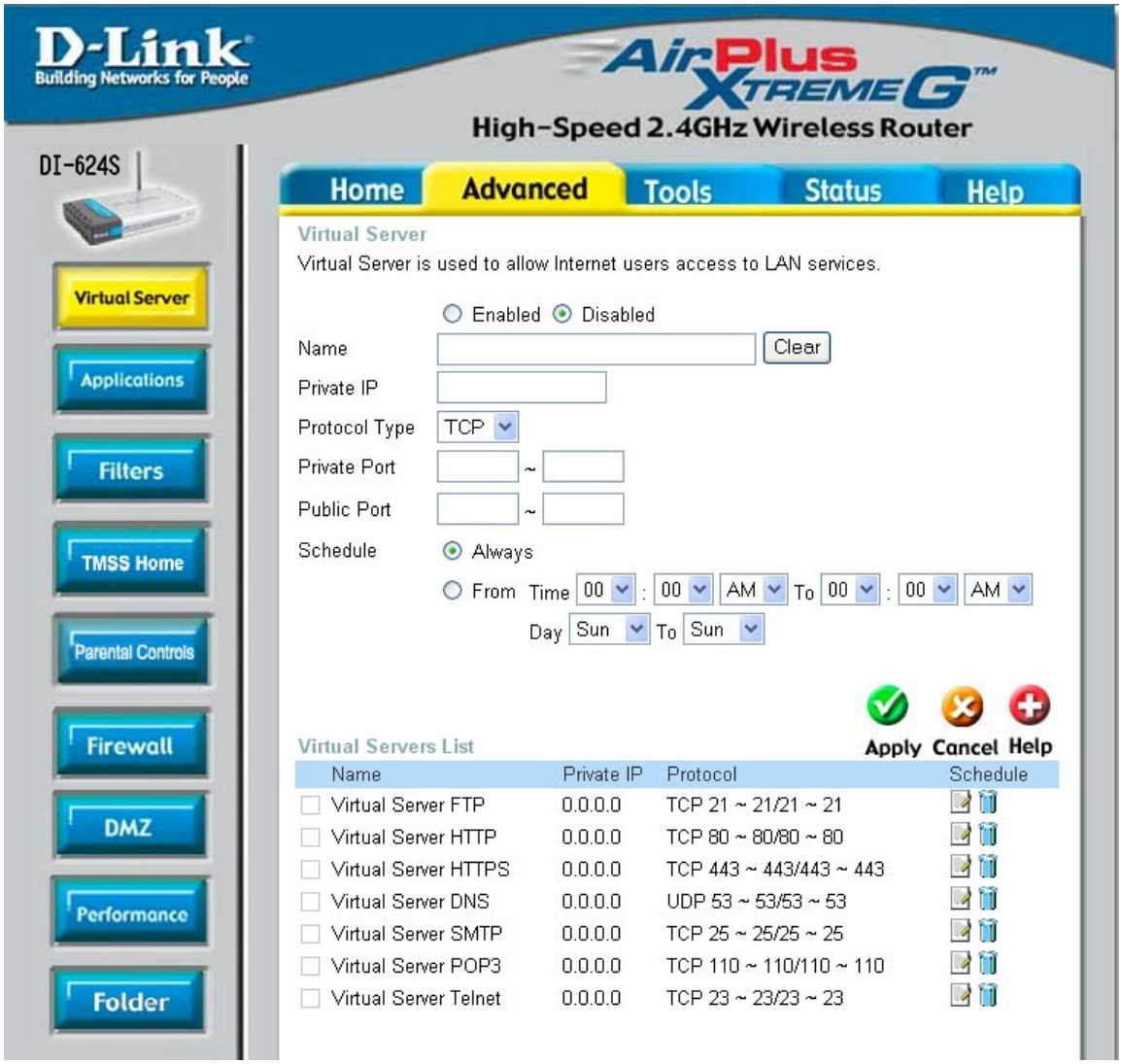
Home > DHCP



DHCP stands for *Dynamic Host Control Protocol*. The DI-624S has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically". When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DI-624S. The DHCP Server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting and ending address of the IP address pool.

DHCP Server:	Select **Enabled** or **Disabled.** The **default** setting is **Enabled.**
Starting IP Address:	The starting IP address for the DHCP server's IP assignment.
Ending IP Address:	The ending IP address for the DHCP server's IP assignment.
Lease Time:	The length of time for the IP lease. Enter the Lease time. The default setting is one hour.
Static DHCP:	Allows the DHCP server to assign the same IP address to a specific MAC address.
IP:	IP address specific to the client.
MAC Address:	Enter the MAC Address.
DHCP Client:	Select a DHCP client from the pull-down list; click **Clone** to copy that MAC Address.

Advanced > Virtual Server



The DI-624S can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DI-624S firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DI-624S are invisible to the outside world. If you wish, you can make some of the LAN computers accessible from the Internet by enabling *Virtual Server.* Depending on the requested service, the DI-624S redirects the external service request to the appropriate server within the LAN network.

The DI-624S is also capable of port-redirection, meaning incoming traffic to a particular port may be redirected to a different port on the server computer.

Each virtual service that is created will be listed at the bottom of the screen in the Virtual Servers List. There are pre-defined virtual services already in the table. You may use them by enabling them and assigning the server IP to use that particular virtual service.

Advanced > Virtual Server *(continued)*

Virtual Server: Select **Enabled** or **Disabled**.

Name: Enter the name referencing the virtual service.

Private IP: The server computer in the LAN (Local Area Network) that will be providing the virtual services.

Protocol Type: The protocol used for the virtual service.

Private Port: The port number of the service used by the Private IP computer.

Public Port: The port number on the WAN (Wide Area Network) side that will be used to access the virtual service.

Schedule: The schedule of time when the virtual service will be enabled. The schedule may be set to **Always**, which will allow the particular service to always be enabled. If it is set to **Time**, select the time frame for the service to be enabled. If the system time is outside of the scheduled time, the service will be disabled.

Example #1: If you have a Web server that you wanted Internet users to access at all times, you would need to enable it. Web (HTTP) server is on LAN (Local Area Network) computer 192.168.0.25. HTTP uses port 80, TCP.
Name: Web Server
Private IP: 192.168.0.25
Protocol Type: TCP
Private Port: 80
Public Port: 80
Schedule: always

Advanced > Virtual Server *(continued)*

Virtual Servers List

	Name	Private IP	Protocol	Schedule	
☒	Virtual Server HTTP	192.168.0.25	TCP 80/80	always	

Click on this icon to edit the virtual service

Click on this icon to delete the virtual service

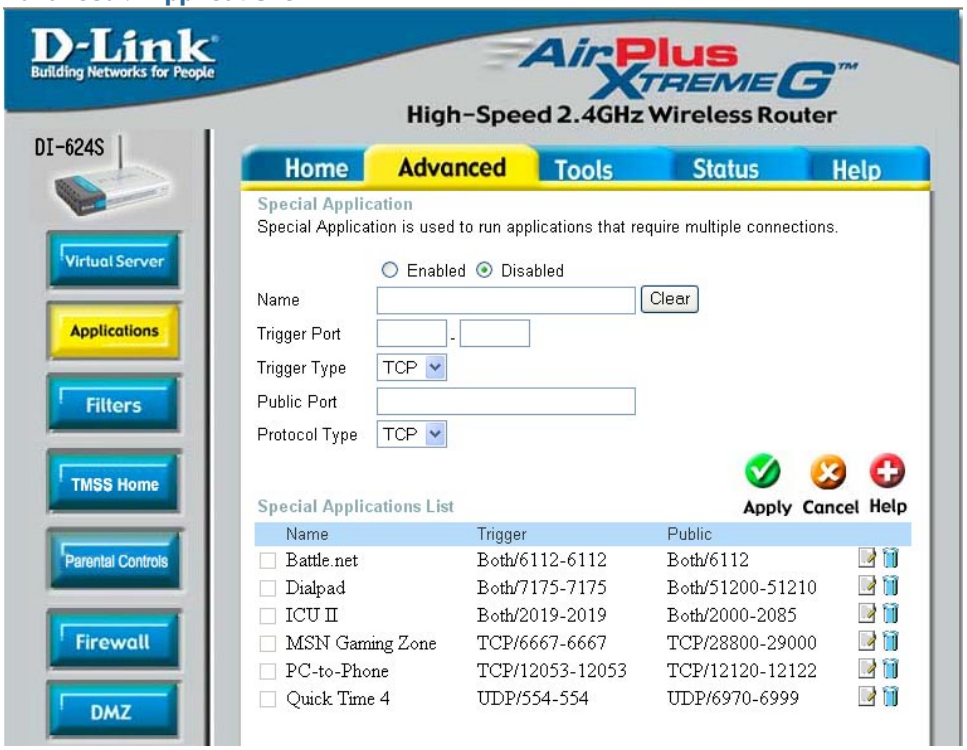
Example #2:
If you have an FTP server that you wanted Internet users to access by WAN port 2100 and only during the weekends, you would need to enable it as such. FTP server is on LAN computer 192.168.0.30. FTP uses port 21, TCP.

Name: FTP Server
Private IP: 192.168.0.30
Protocol Type: TCP
Private Port: 21
Public Port: 2100

Schedule: From: 01:00AM to 01:00AM, Sat to Sun

All Internet users who want to access this FTP Server must connect to it from port 2100. This is an example of port redirection and can be useful in cases where there are many of the same servers on the LAN network.

Advanced > Applications



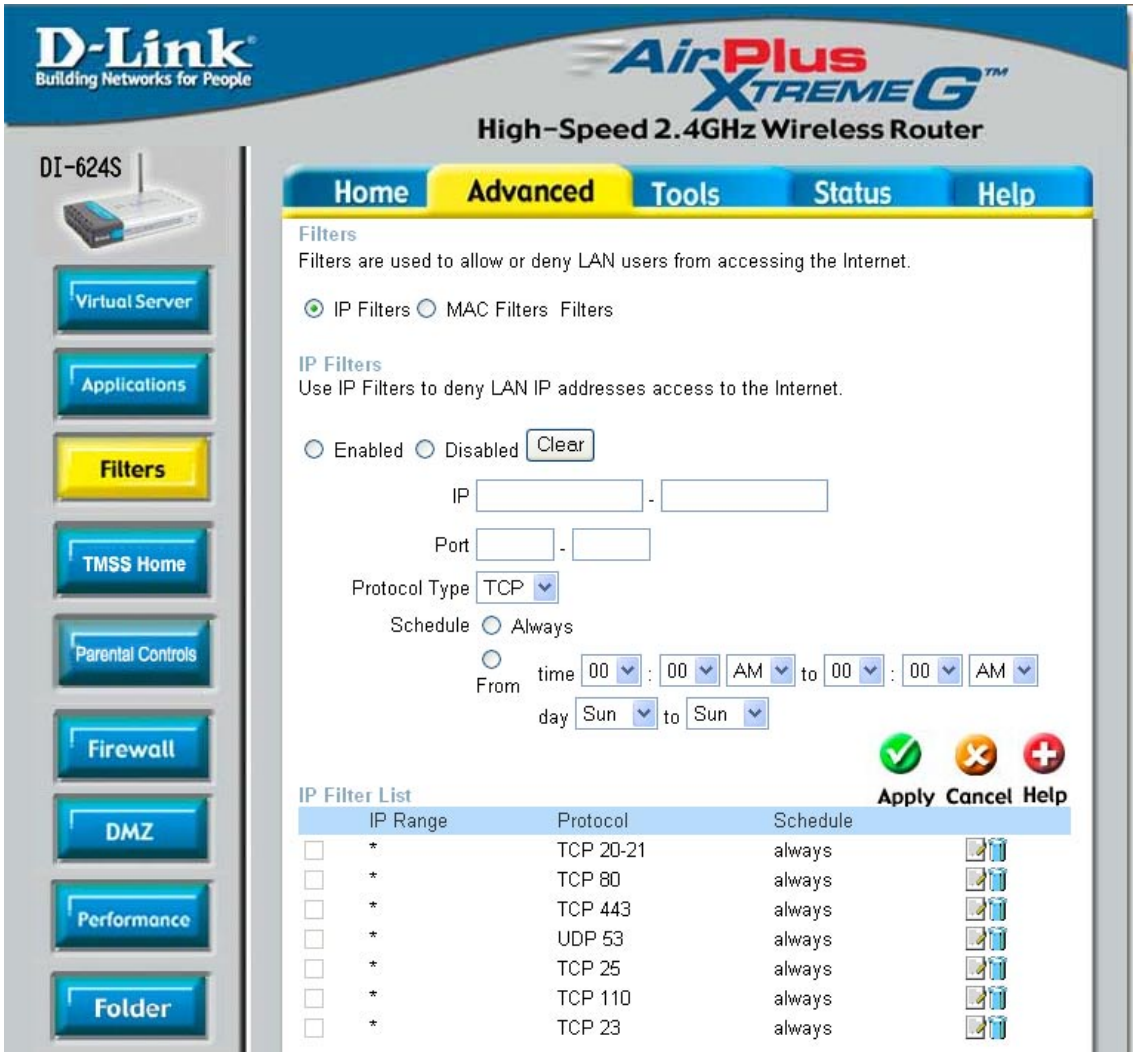
The DI-624S provides some predefined applications in the table on the bottom of the web page. Select the application you want to use and enable it.

Some applications require multiple connections, such as Internet gaming, video conferencing, Internet telephony and others. These applications have difficulties working through NAT (Network Address Translation). Special Applications makes some of these applications work with the DI-624S. If you need to run applications that require multiple connections, specify the port normally associated with an application in the "Trigger Port" field, select the protocol type as TCP or UDP, then enter the public ports associated with the trigger port to open them for inbound traffic.

Note! *Only one PC can use each Special Application tunnel.*

Name:	This is the name referencing the special application.
Trigger Port:	This is the port used to trigger the application. It can be either a single port or a range of ports.
Trigger Type:	This is the protocol used to trigger the special application.
Public Port:	This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.
Protocol Type:	This is the protocol used for the special application.

Advanced > Filters > IP Filters



Filters are used to deny or allow LAN (Local Area Network) computers from accessing the Internet. The DI-624S can be setup to deny internal computers by their IP or MAC addresses. The DI-624S can also block users from accessing restricted web sites.

Filters: Select the filter you wish to use; in this case, **IP Filters** was chosen.

IP Filters: Use IP Filters to deny LAN IP addresses from accessing the Internet. You can deny specific port numbers or all ports for the specific IP address.

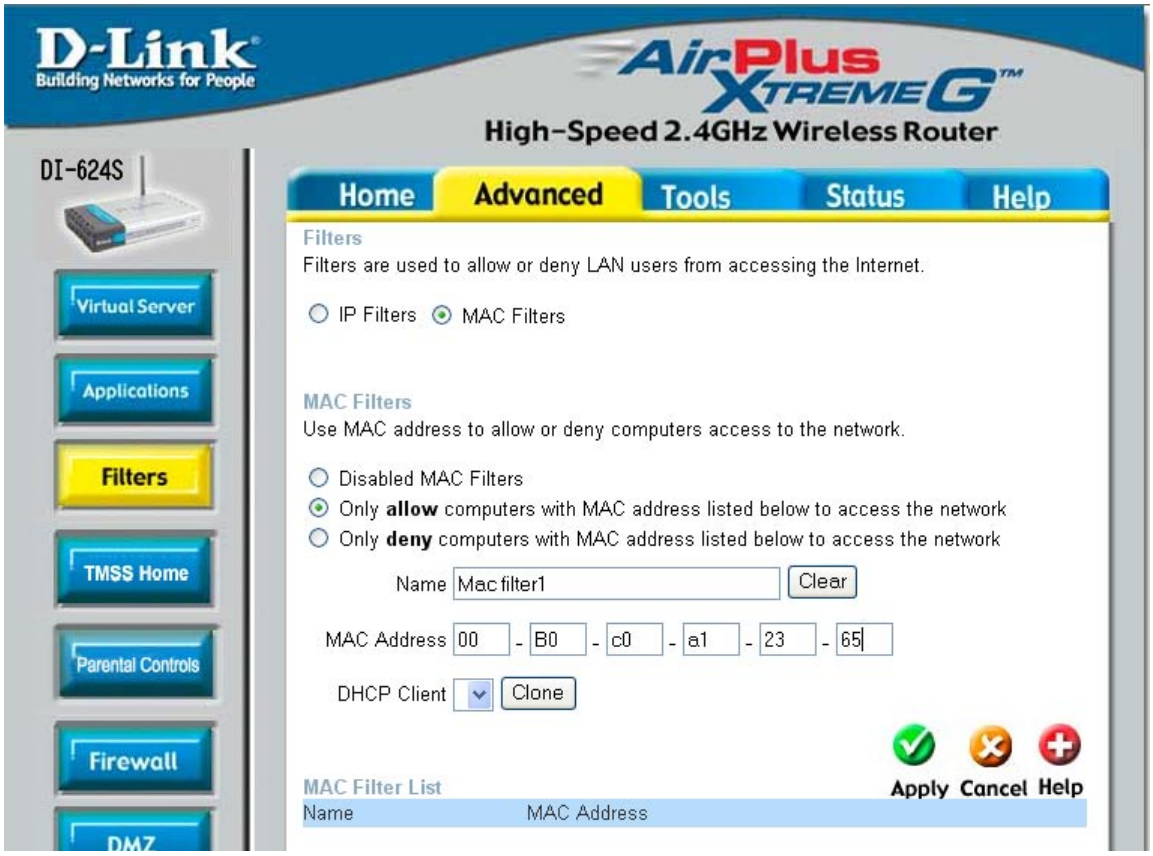
IP: The IP address of the LAN computer that will be denied access to the Internet.

Port: The single port or port range that the LAN computer specified in the IP field will be denied access.

Protocol Type: Choose the protocol type of the port you are blocking access to.

Schedule: This is the time when the IP Filter will be enabled.

Advanced > Filters > MAC Filters



Use MAC (Media Access Control) Filters to allow or deny LAN (Local Area Network) computers by their MAC addresses from accessing the Network. You can either manually add a MAC address or select the MAC address from the list of clients that are currently connected to the Broadband Router.

Filters:	Select the filter you wish to use; in this case, **MAC filters** was chosen.
MAC Filters:	Choose **Disable** MAC filters; **allow** MAC addresses listed below; or **deny** MAC addresses listed below.
Name:	Enter the name here.
MAC Address:	Enter the MAC Address.
DHCP Client:	Select a DHCP client from the pull-down list; click **Clone** to copy that MAC Address.

Advanced > TMSS Home

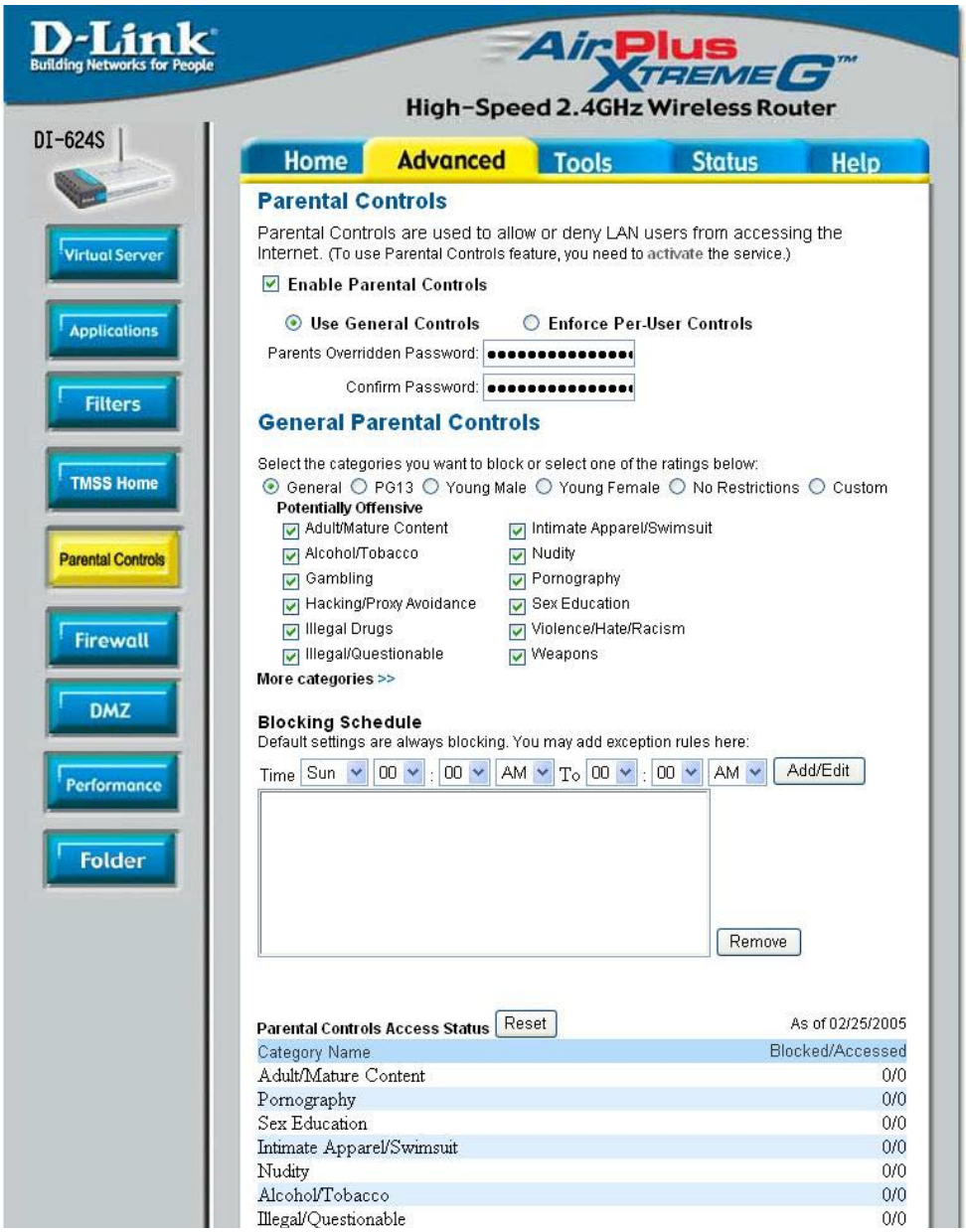
Enable Trend Micro Security Services: Select this checkbox to enable the Trend Micro Security Services. Note: This option must be enabled before you can enable Parental Controls.

Security Services Display Interval: Choose how often you would like the see the Security Services Dashboard.

Automatically check for Update Components: Select this checkbox if you would like the router to automatically check for updates for the Trend Micro Internet Security software. If enabled, you also will need to choose how often you would like the router to check for updates.

Client Virus Protection Status: Shows the status of the virus scanning software installed on the computers in your network.

Advanced > Parental Controls > General Parental Controls



Enable Parental Controls: Select this option to enable the Parental Control features provided by Trend Micro.

Use General Controls: Select this option to setup Parental Controls as a global setting. When using this option, the restrictions that you set affect every computer on the network.

Advanced > Parental Controls > General Parental Controls *(continued)*

Parents Override Password:	Enter a password that can be used to override blocked websites. You will have the option to enter this password and either temporarily or permanently allow access to the website being blocked.
Confirm Password:	Reenter the Parents Override Password.
Ratings:	Choose the rating that best matches the categories you would like to block.
Categories:	This shows the categories that are being blocked based on the Rating that you chose. If the Custom rating was chosen, you can select from the list of predefined Potentially Offensive categories to define the type of traffic you would like to block. Click on More Categories to see a larger list to choose from.
Blocking Schedule:	Specify the days and times that you would like the Parental Control feature to be active. To remove an entry in the schedule list, highlight the entry and click Remove.
Parental Controls Access Status:	This shows you the complete list of categories and also how many times traffic from each category has been Blocked or Accessed.

Advanced > Parental Controls > Per-User Parental Controls

Enable Parental Controls: Select this option to enable the Parental Control features provided by Trend Micro.

Use Per-User Controls: Select this option to setup Parental Controls in a per-user fashion. When using this option, the restrictions are setup based on usernames and passwords. This allows for more control of the content that each user on the network is allowed to access.

Parents Override Password: Enter a password that can be used to override blocked websites. You will have the option to enter this password and either temporarily or permanently allow access to the website being blocked.

Confirm Password: Reenter the Parents Override Password.

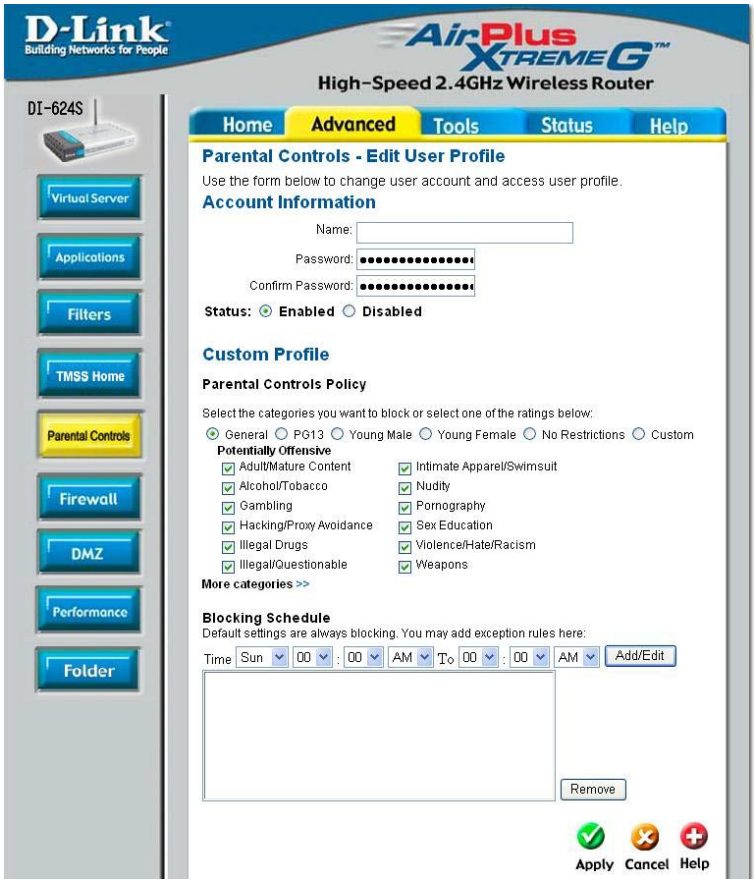
User List: Shows you the Name, Profile, and Status of each user that has been specified.

Add User: Click this button to add a new User account.

Advanced > Parental Controls > Per-User Parental Controls *(continued)*

Parental Controls Access Status: This shows you the complete list of categories and also how many times traffic from each category has been Blocked or Accessed.

Advanced > Parental Controls > Per-User Parental Controls > Add User



Name: Enter the name for your new User account.

Password: Enter the password for your new User account.

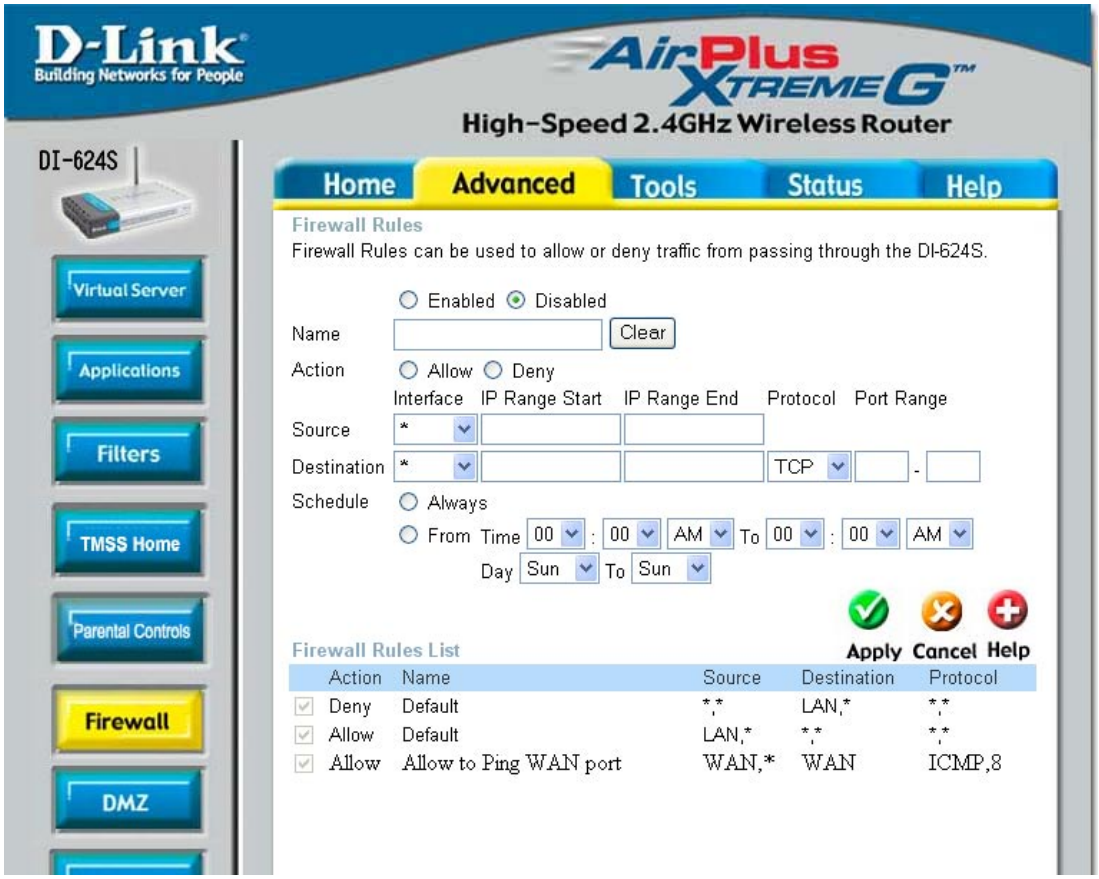
Status: Select Enabled to make this new account active, or Disabled to deactivate this account.

Ratings: Choose the rating that best matches the categories you would like to block for this user.

Categories: This shows the categories that are being blocked based on the Rating that you chose. If the Custom rating was chosen, you can select from the list of predefined Potentially Offensive categories to define the type of traffic you would like to block. Click on More Categories to see a larger list to choose from.

Blocking Schedule: Specify the days and times that you would like the Parental Control feature to be active for this user. To remove an entry in the schedule list, highlight the entry and click Remove.

Advanced > Firewall

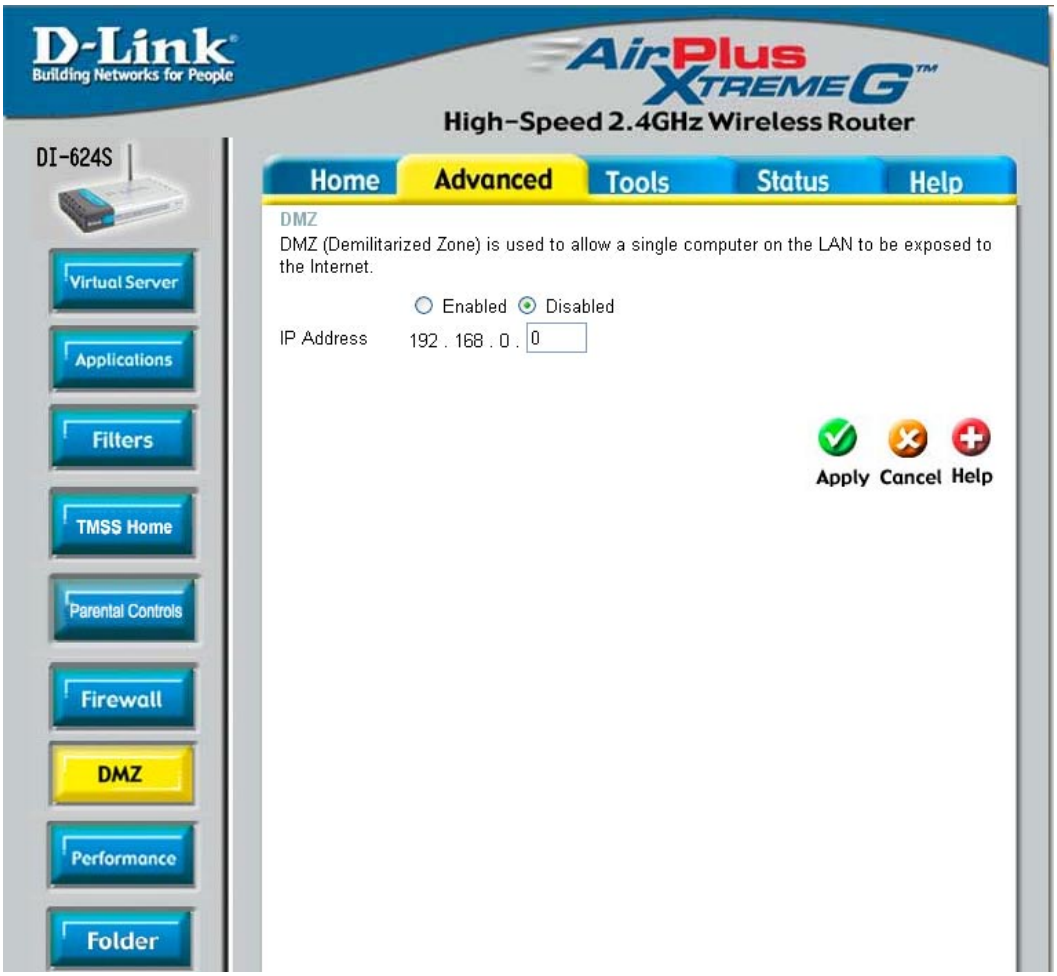


Firewall Rules is an advanced feature used to deny or allow traffic from passing through the DI-624S. It works in the same way as IP Filters with additional settings. You can create more detailed access rules for the DI-624S. When virtual services are created and enabled, it will also display in Firewall Rules. Firewall Rules contain all network firewall rules pertaining to IP (Internet Protocol).

In the Firewall Rules List at the bottom of the screen, the priorities of the rules are from top (highest priority) to bottom (lowest priority.)

Firewall Rules:	**Enable** or **disable** the Firewall.
Name:	Enter the name.
Action:	**Allow** or **Deny.**
Source:	Enter the **IP Address range.**
Destination:	Enter the **IP Address range**; the **Protocol**; and the **Port Range.**
Schedule:	Select **Always** or enter the **Time Range**.

Advanced > DMZ

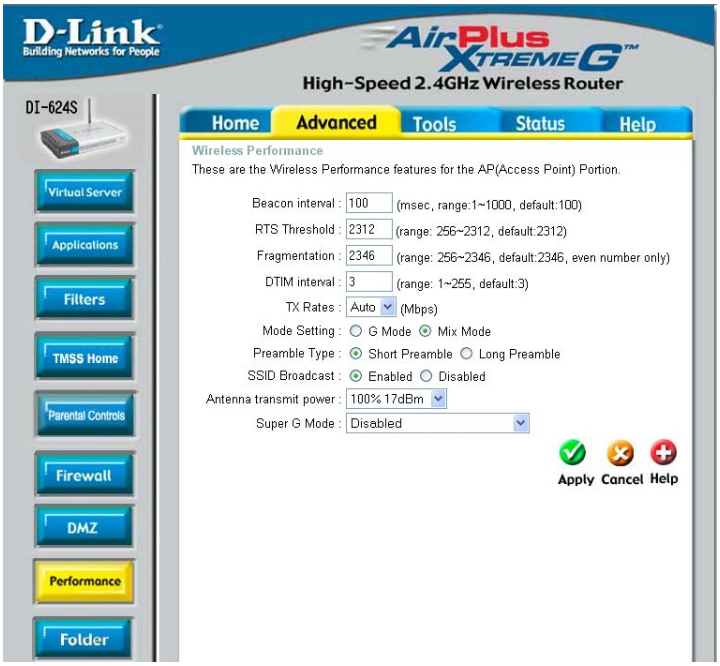


If you have a client PC that cannot run Internet applications properly from behind the DI-624S, then you can set the client up for unrestricted Internet access. It allows a computer to be exposed to the Internet. This feature is useful for gaming purposes. Enter the IP address of the internal computer that will be the DMZ host. Adding a client to the DMZ (Demilitarized Zone) may expose your local network to a variety of security risks, so only use this option as a last resort.

DMZ: **Enable** or **Disable** the DMZ. The DMZ (Demilitarized Zone) allows a single computer to be exposed to the internet. By **default** the DMZ is **disabled**.

IP Address: Enter the **IP Address** of the computer to be in the **DMZ**.

Advanced > Performance



Wireless Performance: Displayed in this window are the Wireless Performance features for the Access Point portion of the DI-624S.

Beacon Interval: Beacons are packets sent by an Access Point to synchronize a wireless network. Specify a value. 100 is the default setting and is recommended.

RTS Threshold: This value should remain at its default setting of 2432. If inconsistent data flow is a problem, only a minor modification should be made.

Fragmentation: The fragmentation threshold, which is specified in bytes, determines whether packets will be fragmented. Packets exceeding the 2346 byte setting will be fragmented before transmission. 2346 is the default setting.

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

TX Rates: **Auto** is the default selection. Select from the drop down menu.

Mode Setting: Select **GMode** if your wireless network consists of only 802.11g clients. If your wireless network includes 802.11b clients, select **Mix Mode**.

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.

Advanced > Performance *(continued)*

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

Disabled:	Standard 802.11g support, no enhanced capabilities.
Super G without Turbo:	Capable of Packet Bursting, FastFrames, Compression, and no Turbo mode.
Super G with DynamiC Turbo:	Capable of Packet Bursting, FastFrames, Compression, and Dynamic Turbo. This setting is backwards compatible with non-Turbo (legacy) devices. Dynamic Turbo mode is only enabled when all nodes on the wireless network are Super G with Dynamic Turbo enabled.

Advanced > Folder

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

USB 1 Sharing System

Unplug: Click this button to safely remove the USB storage device that is connected to USB 1.

Share Whole Disk: Click this button to share the entire contents of the USB storage device that is connected to USB 1.

New Folder Name: This allows you to create new folders on the USB storage device that is connected to USB 1. Enter a name and then click the Create button.

Capacity: This shows you the total size, amount of used space, amount of free space, and the percentage of used space on the USB storage device that is connected to USB 1.

Current Folder: Shows you the current directory you are browsing on the USB storage device that is connected to USB 1.

Write: Select this checkbox to allow write permission to the corresponding folder.

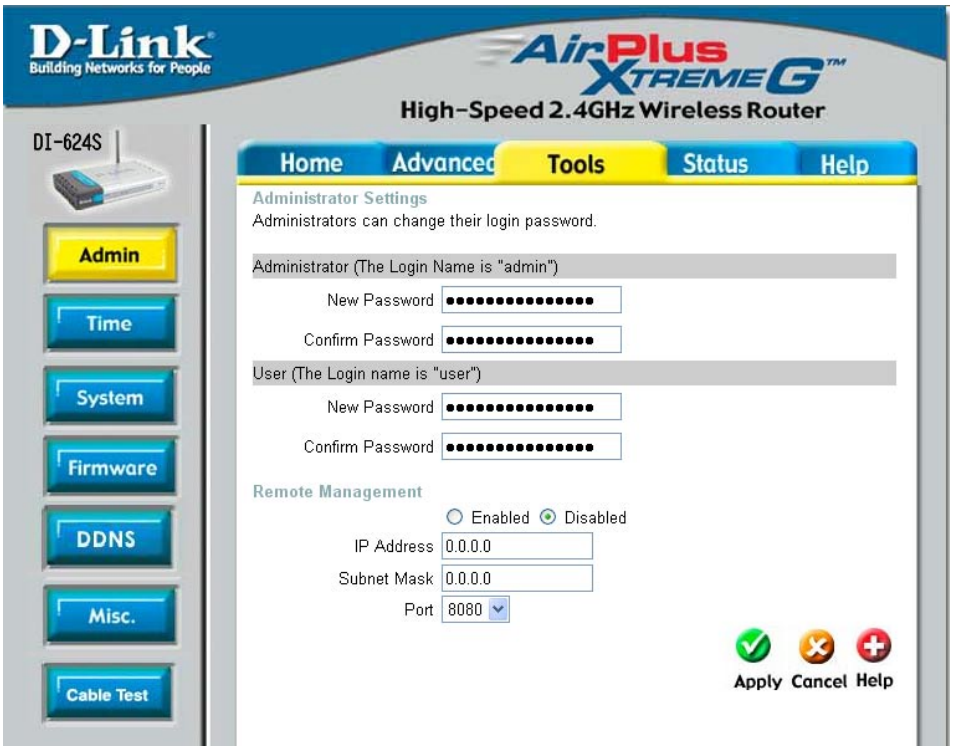
Share: Select this checkbox to allow other users on the network to view the contents of the corresponding folder.

Advanced > Folder *(continued)*

USB 2 Sharing System

Unplug:	Click this button to safely remove the USB storage device that is connected to USB 1.
Share Whole Disk:	Click this button to share the entire contents of the USB storage device that is connected to USB 2.
New Folder Name:	This allows you to create new folders on the USB storage device that is connected to USB 2. Enter a name and then click the **Create** button.
Capacity:	This shows you the total size, amount of used space, amount of free space, and the percentage of used space on the USB storage device that is connected to USB 2.
Current Folder:	Shows you the current directory you are browsing on the USB storage device that is connected to USB 2.
Write:	Select this checkbox to allow write permission to the corresponding folder.
Share:	Select this checkbox to allow other users on the network to view the contents of the corresponding folder.

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: **admin** is the **Administrator login name.**

Password: Enter the password and enter again to confirm.

User: **user** is the **User login name.**

Password: Enter the password and enter again to confirm.

Remote Management: Remote management allows the DI-624S 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.

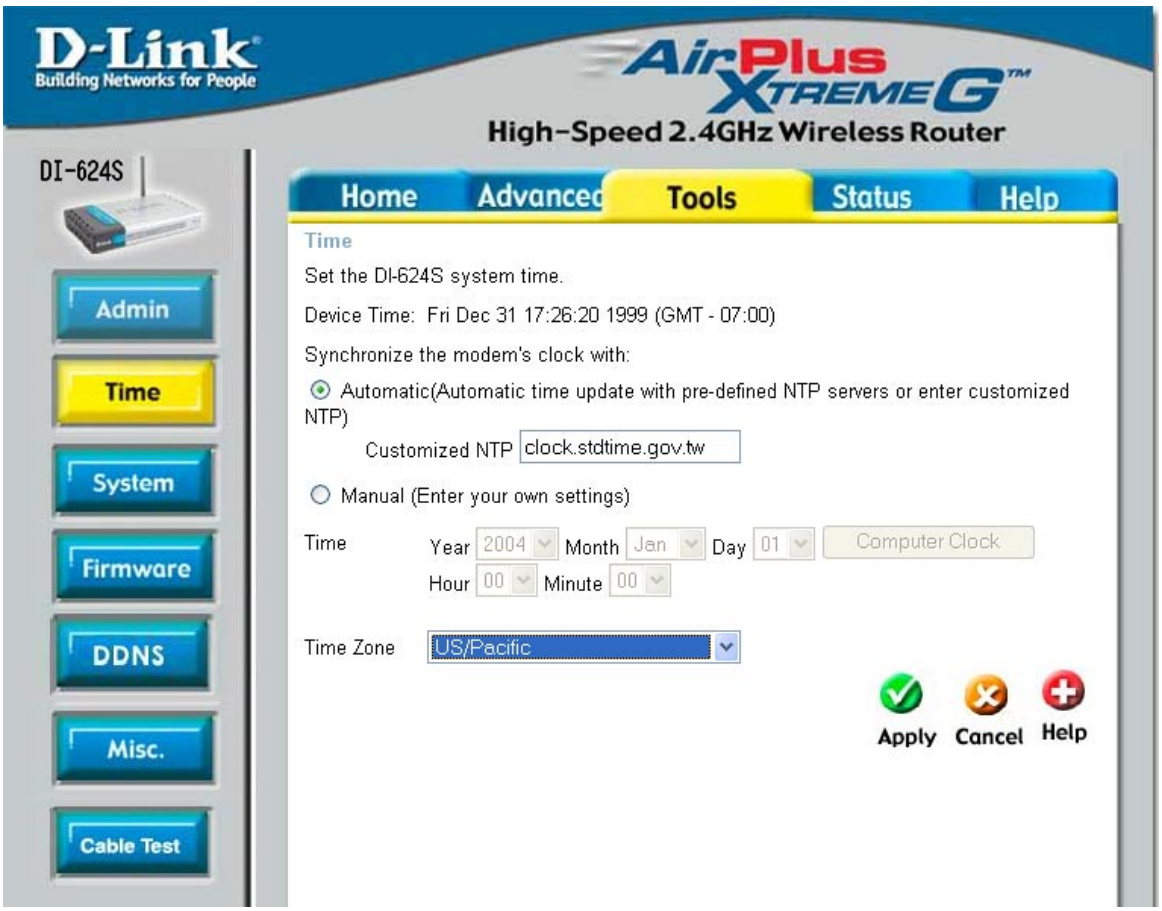
IP Address: The Internet IP address of the computer that has access to the Broadband Router. If you input 0.0.0.0 into this field, then any computer will be able to access the Router. Putting 0.0.0.0 into this field would present a security risk and is not recommended.

IP Address: Input a subnet mask to define the computer or group of computers that are allowed to access the router.

Port: The port number used to access the Broadband Router.

Example: http://x.x.x.x:8080 where x.x.x.x is the WAN IP address of the Broadband Router and 8080 is the port used for the Web-Mangement interface.

Tools > Time

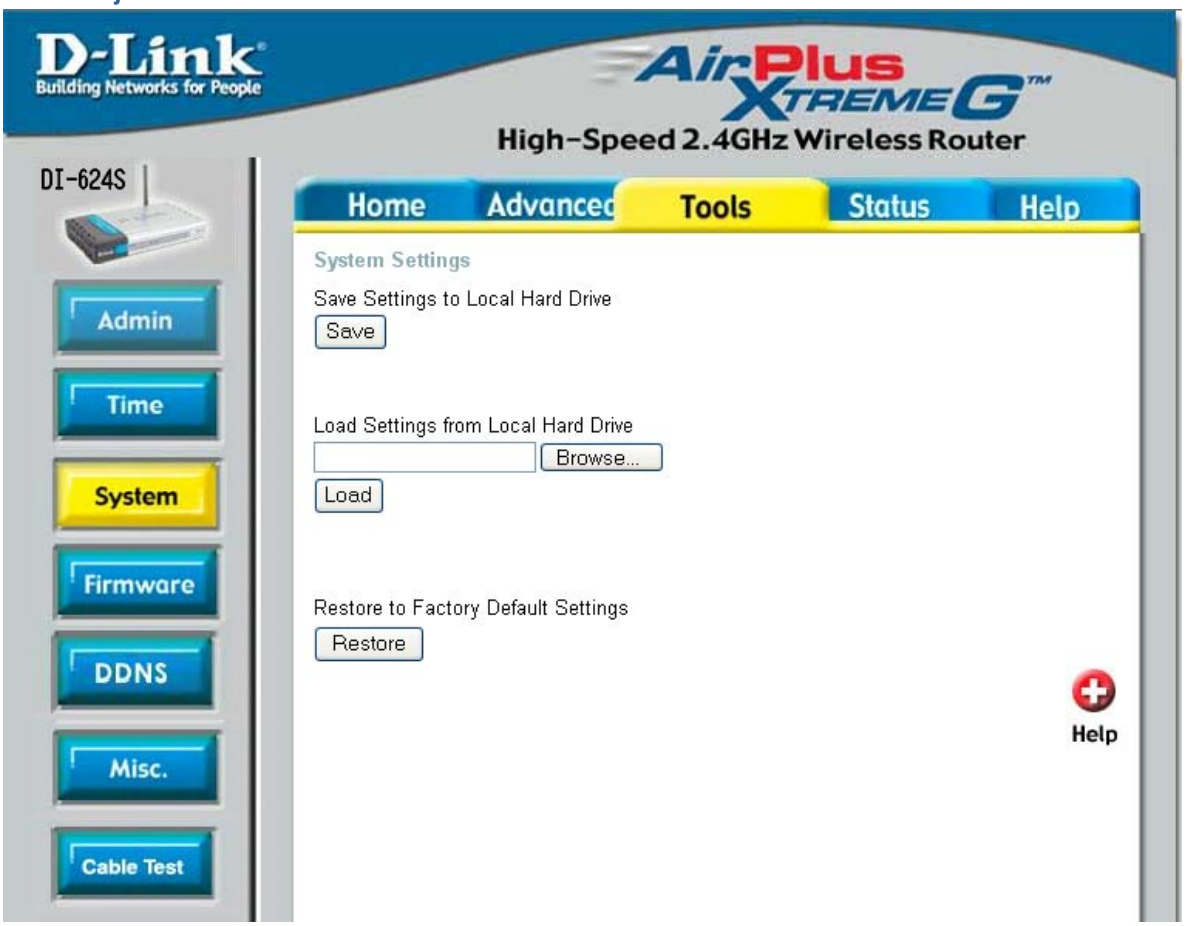


Customized NTP: NTP is short for *Network Time Protocol.* NTP synchronizes computer clock times in a network of computers.
This field is optional.

Manual: To manually input the time, select this option and enter the values for the Year, Month, Day, Hour, Minute, and Second. Click the **Computer Clock** button, to copy your computer's time.

Time Zone: Select the Time Zone from the pull-down menu.

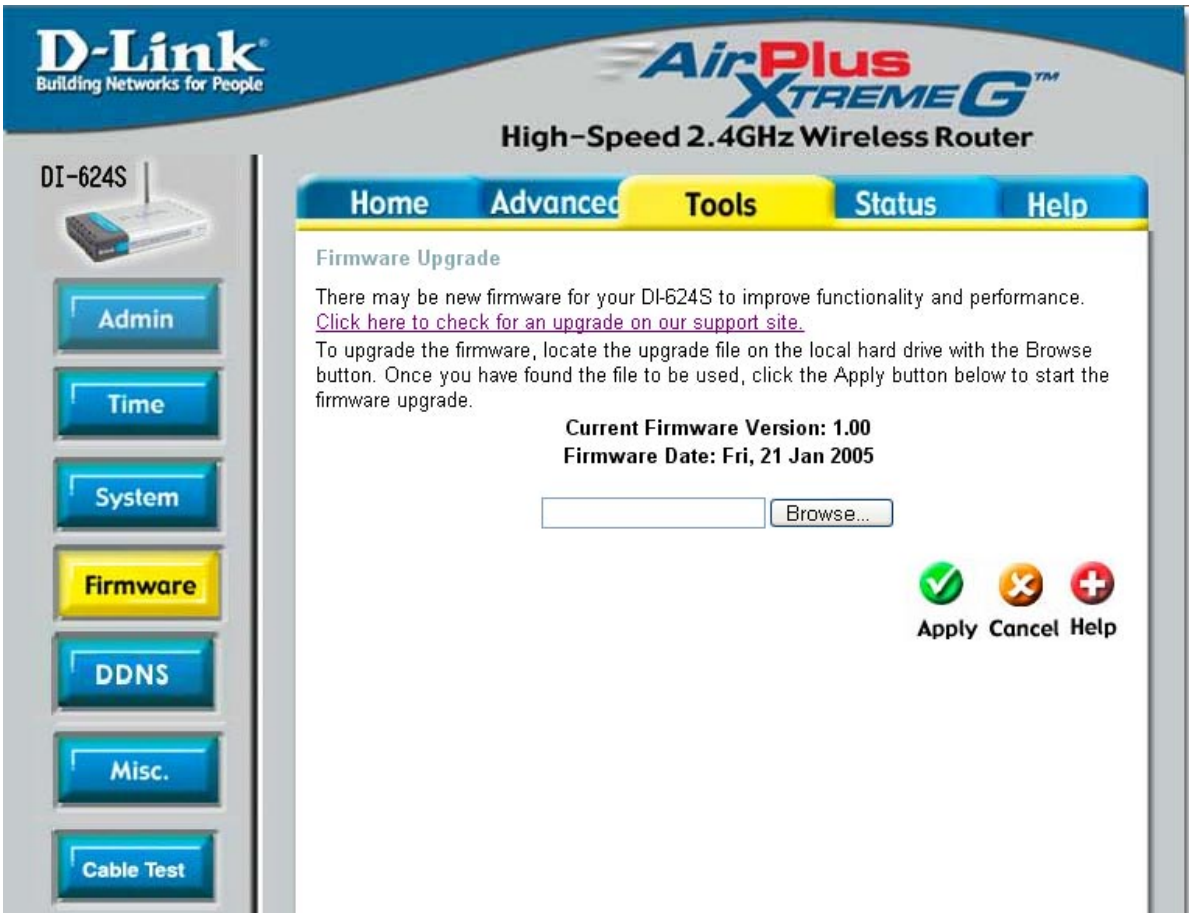
Tools > System



The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file can be loaded back on the Broadband Router. To reload a system settings file, click on **Browse** to browse the local hard drive and locate the system file to be used. You may also reset the Broadband Router back to factory settings by clicking on **Restore.**

Save Settings to Local Hard Drive:	Click **Save** to save the current settings to the local Hard Drive.
Load Settings from Local Hard Drive:	Click **Browse** to find the settings, then click **Load.**
Restore to Factory Default Settings:	Click **Restore** to restore the factory default settings.

Tools > Firmware

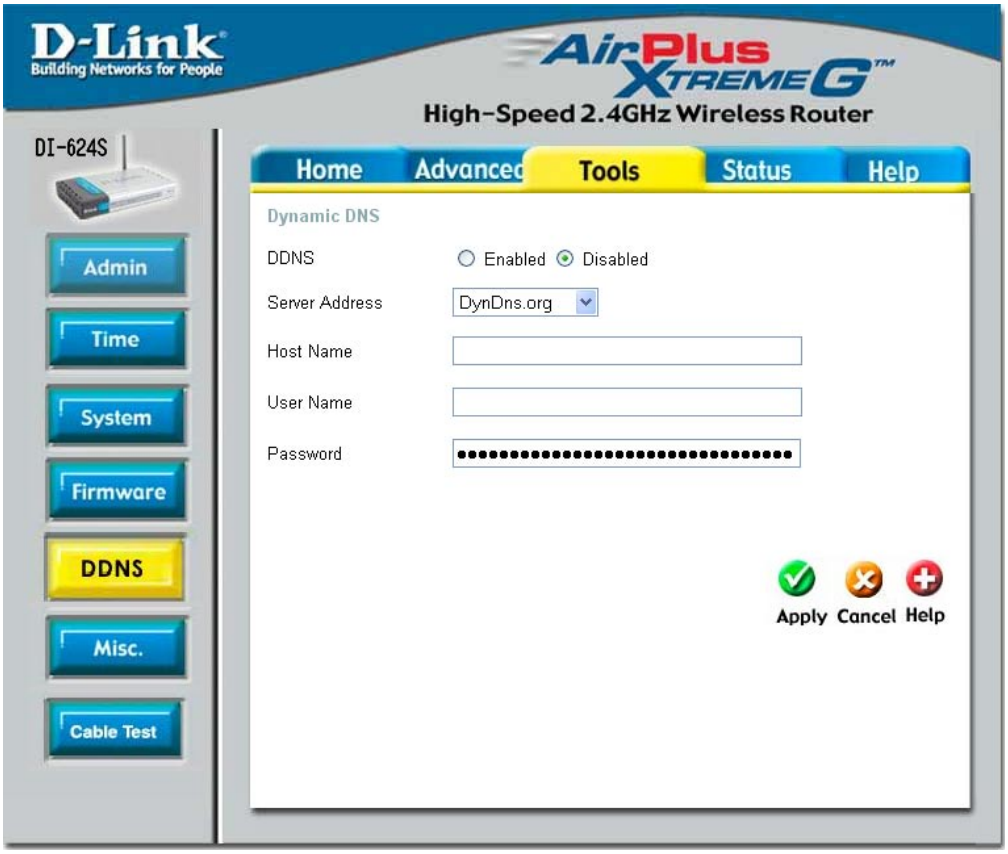


You can upgrade the firmware of the Router here. Make sure the firmware you want to use is on the local hard drive of the computer. Click on **Browse** to browse the local hard drive and locate the firmware to be used for the update. Please check the D-Link support site for firmware updates at http://support.dlink.com.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



Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. This is a useful feature since many computers do not use a static IP address.

To use the DDNS update client built into the router, click on **Enabled**.

Server Address:	Choose your DDNS provider from the drop down menu.
Host Name:	Enter the **Host Name** that you registered with your DDNS service provider.
Username:	Enter the **username** for your DDNS account.
Password:	Enter the **password** for your DDNS account.

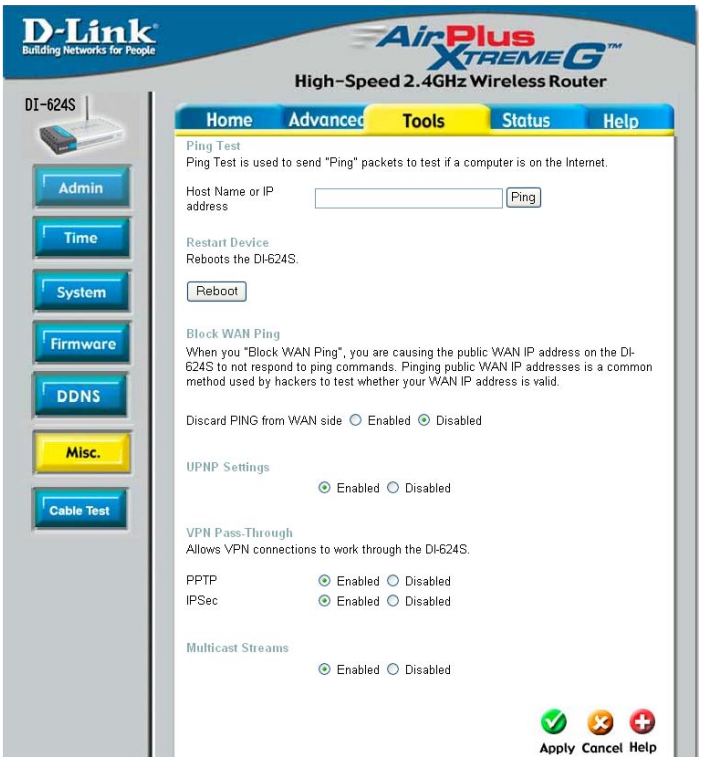
Tools > Misc

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**.

Restart Device: Click **Reboot** to restart the DI-624S.

Block WAN Ping: 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.

Discard Ping from WAN side: Click **Enabled** to block the WAN ping.



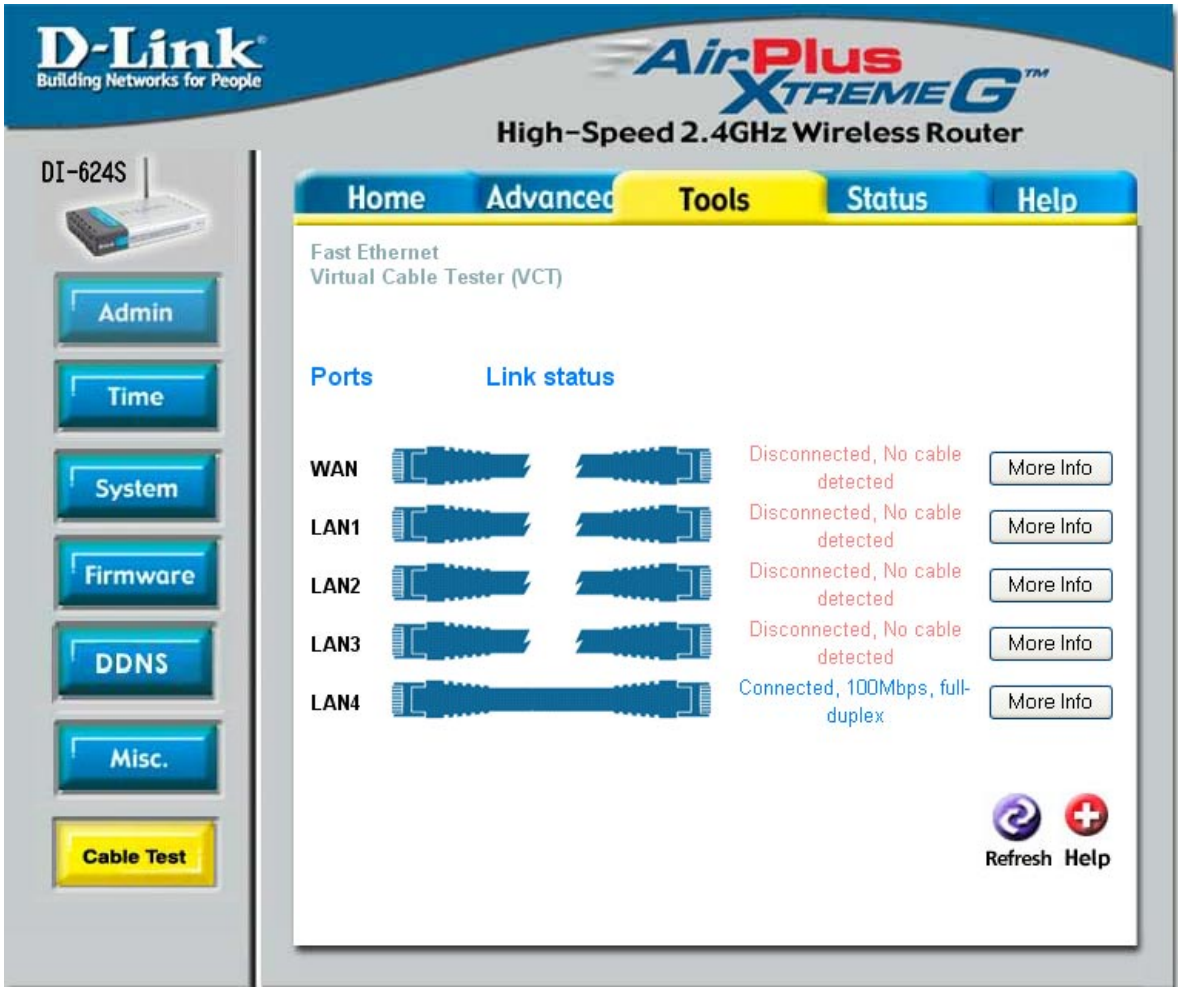
UPNP: To use the *Universal Plug and Play* feature click on **Enabled**. UPNP provides compatibility with networking equipment, software and peripherals of the over 400 vendors that co-operate in the Plug and Play forum.

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.**

Multicast Streams: **Enable** this option to allow multicast traffic to pass through the router from the Internet.

Tools > Cable Test



This page displays the current information for the DI-624S, which will assist you in troubleshooting your network. It will display which port on the router is currently connected.

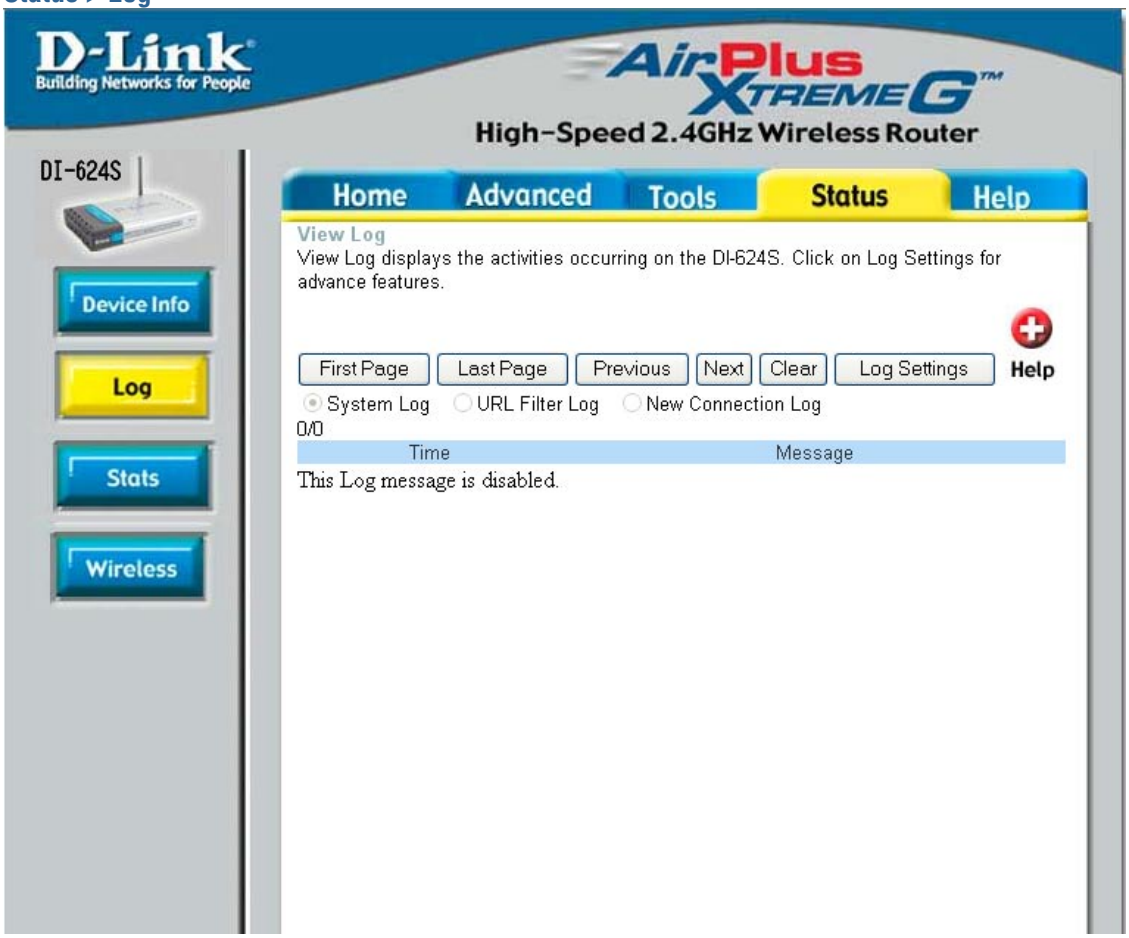
Status > Device Info

This page displays the current information for the DI-624S. It will display the LAN, WAN and Wireless information.
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:

LAN:	IP Address: LAN/Private IP Address of the DI-624S. Subnet Mask: LAN/Private Subnet Mask of the DI-624S.
WAN:	IP Address: WAN/Public IP Address. Subnet Mask: WAN/Public Subnet Mask. Gateway: WAN/Public Gateway IP Address. Domain Name Server: WAN/Public DNS IP Address.
Wireless:	SSID: Displays the current SSID. Channel: Displays the current channel. WEP: indicates whether WEP is enabled or disabled.

Status > Log

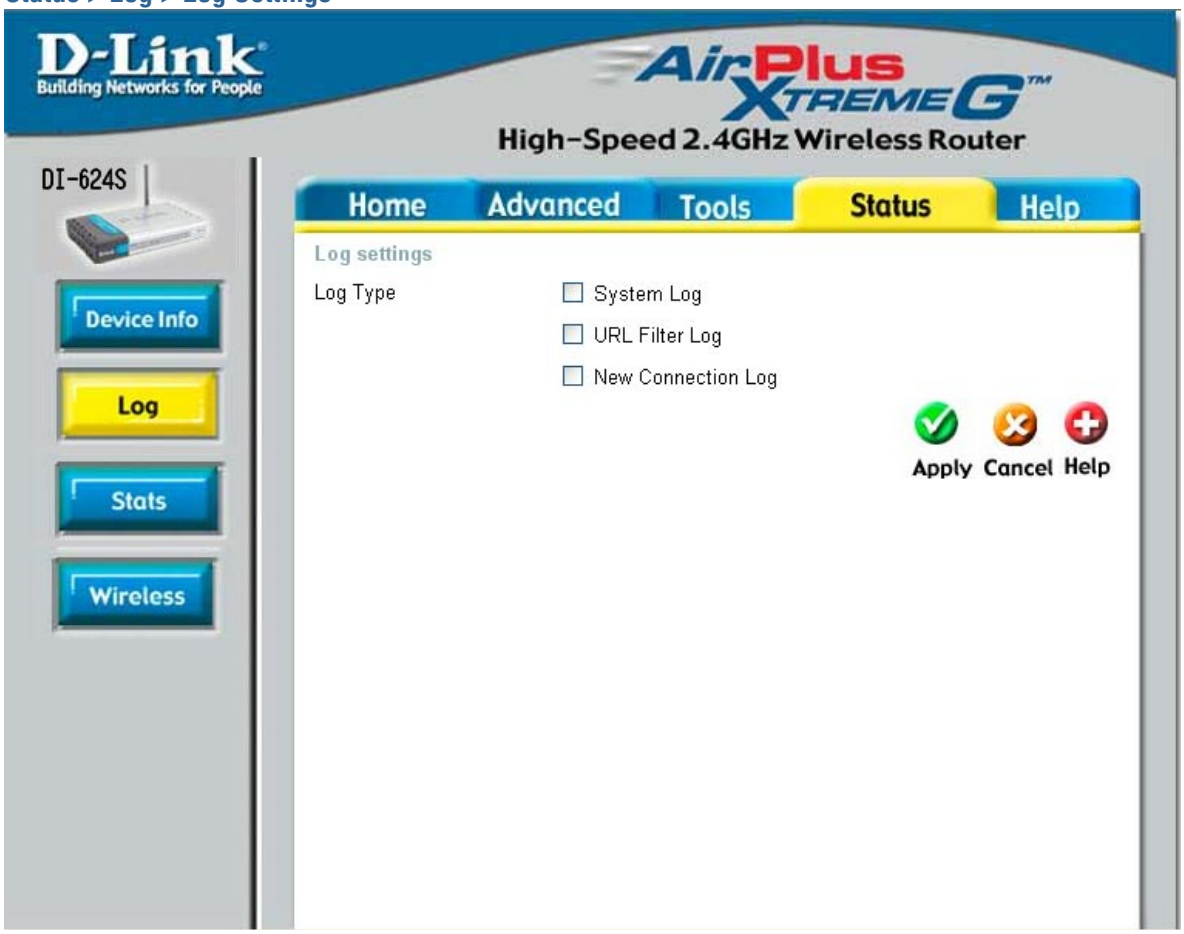


The Broadband Router keeps a running log of events and activities occurring on the Router. If the device is rebooted, the logs are automatically cleared.

View Log:

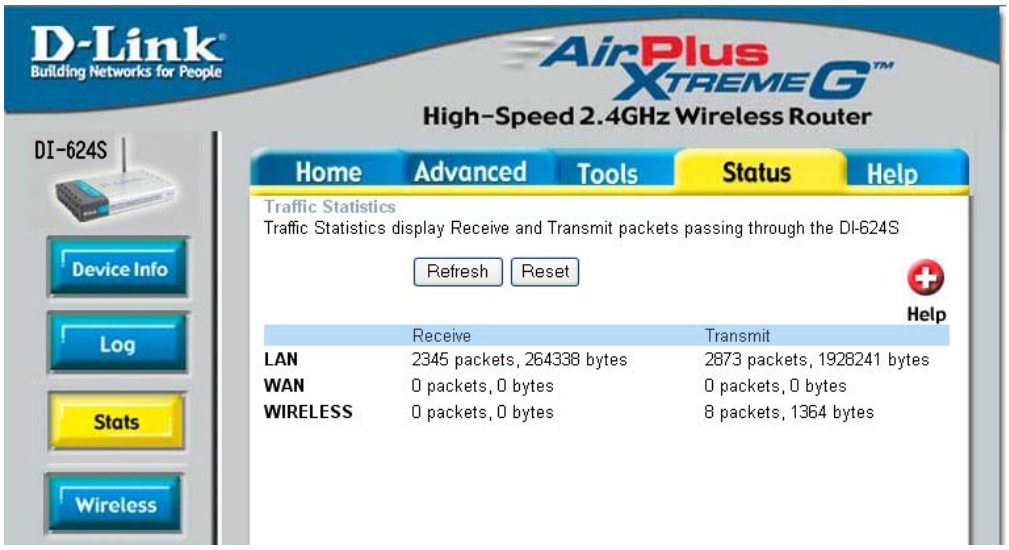
First Page - The first page of the log.
Last Page - The last page of the log.
Previous - Moves back one log page.
Next - Moves forward one log page.
Clear - Clears the logs completely.
Log Settings - Brings up the page to configure the log.

Status > Log > Log Settings



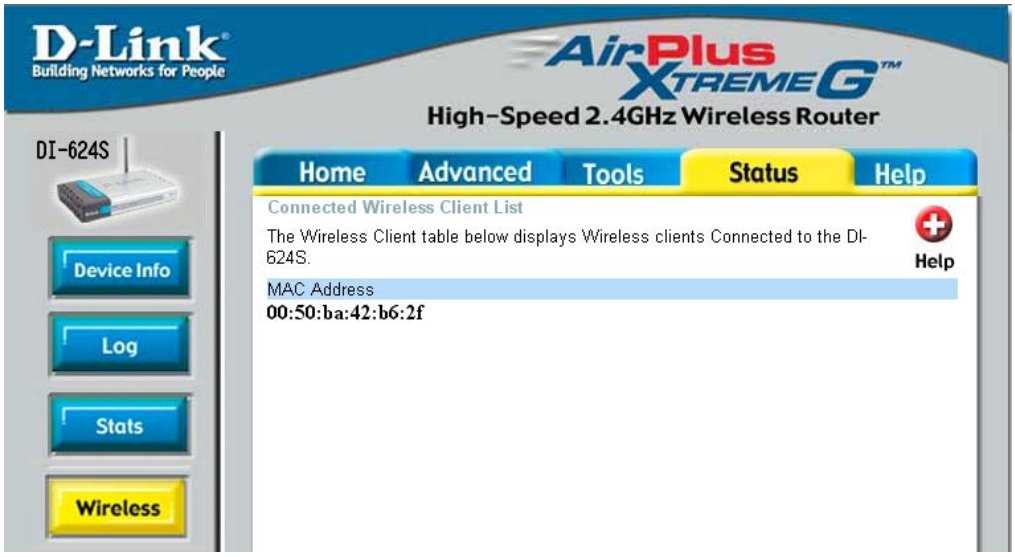
Choose the type of information you would like the router to log.

Status > Stats



The screen above displays theTraffic Statistics. Here you can view the amount of packets that pass through the DI-624S on the WAN, LAN, and Wireless interfaces. The traffic counter will reset if the device is rebooted.

Status > Wireless



The wireless client table displays a list of current connected wireless clients. This table also displays the MAC address of the connected wireless client.
Click on **Help** at any time, for more information.

Networking Basics

Using the Network Setup Wizard in Windows XP

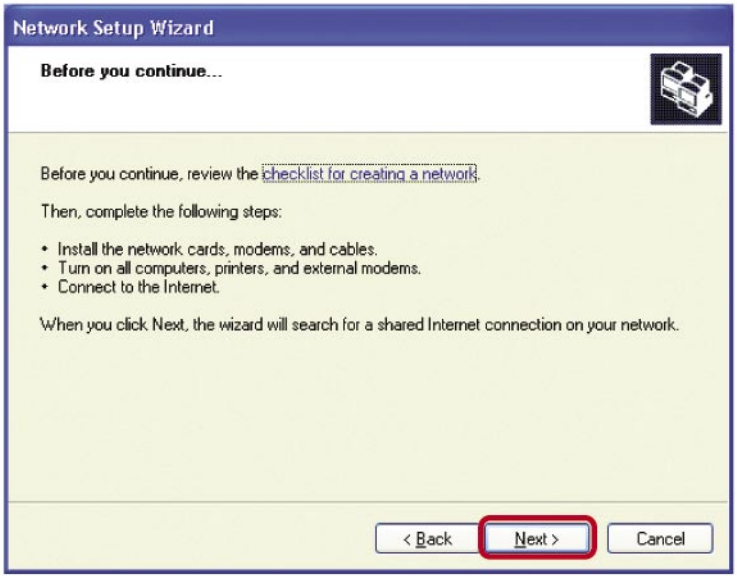
In this section you will learn how to establish a network at home or work, using **Microsoft Windows XP.**

Note: Please refer to websites such as http://www.homenethelp.com and http://www.microsoft.com/windows2000 for information about networking computers using Windows 2000.

Go to **Start>Control Panel>Network Connections**
Select **Set up a home or small office network**

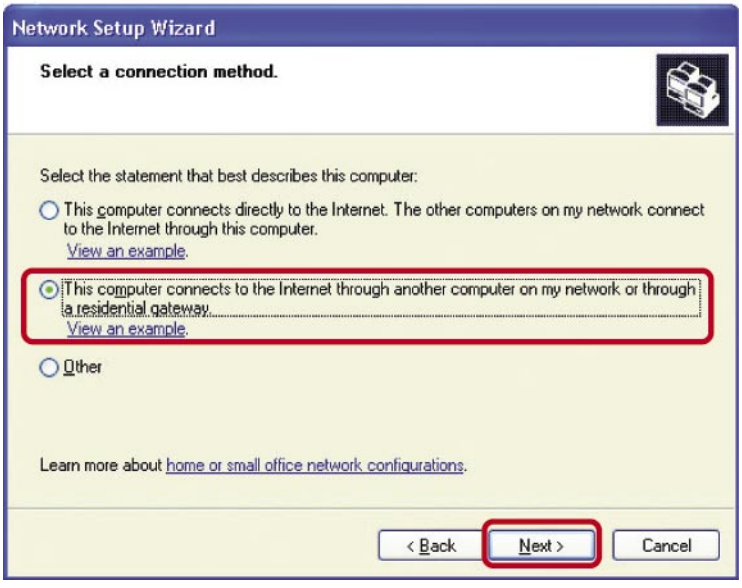
When this screen appears, **Click Next.**

Please follow all the instructions in this window:



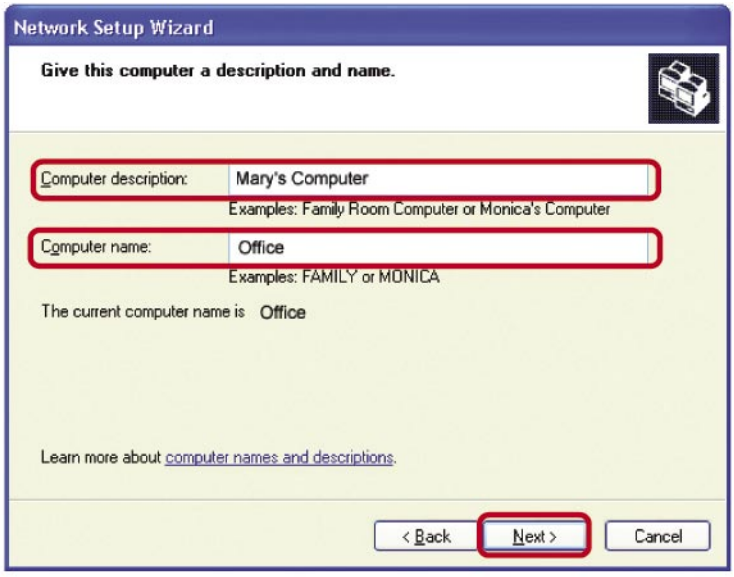
Click **Next**.

In the following window, select the best description of your computer. If your computer connects to the internet through a gateway/router, select the second option as shown.



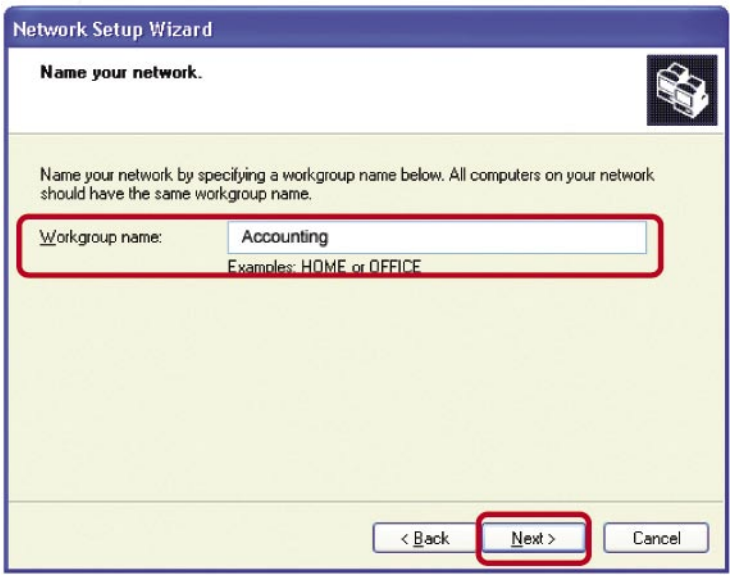
Click **Next**.

Enter a **Computer description** and a **Computer name** (optional.)



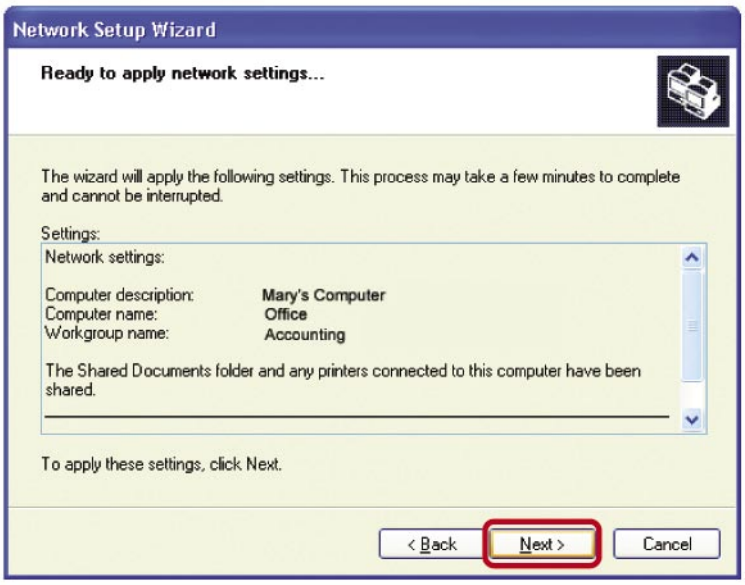
Click **Next**.

Enter a **Workgroup** name. All computers on your network should have the same **Workgroup name.**



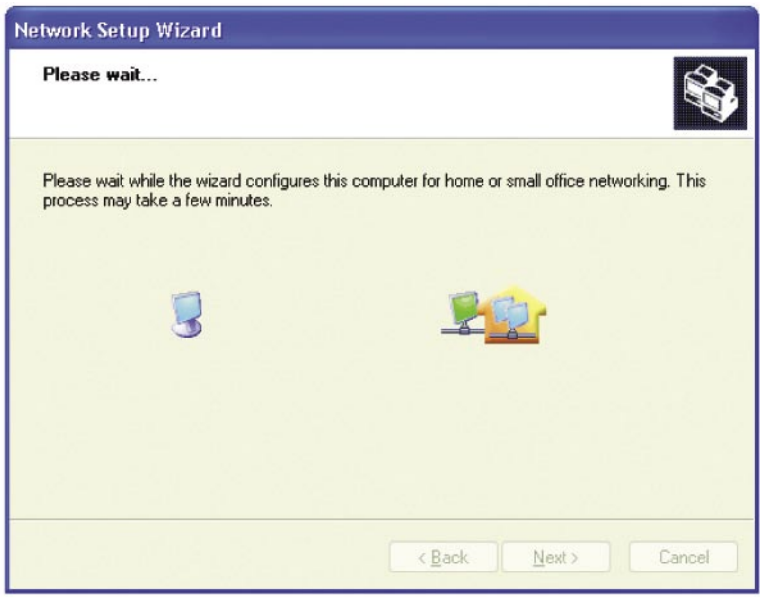
Click **Next**.

Please wait while the **Network Setup Wizard** applies the changes.



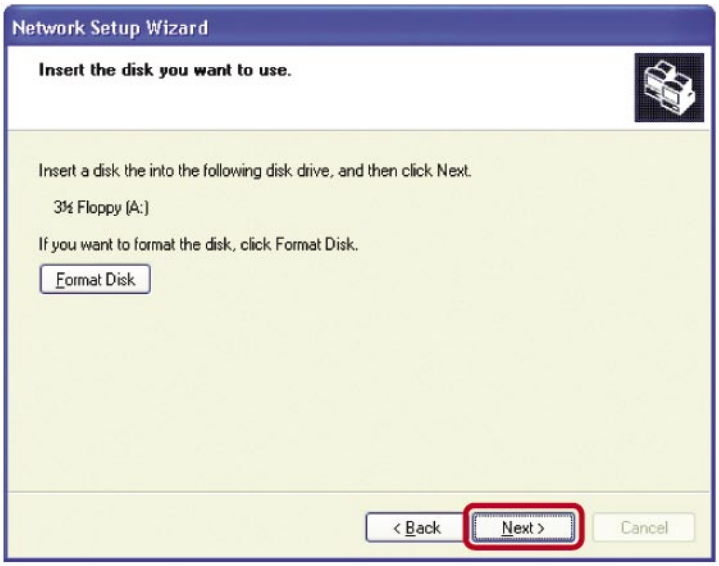
When the changes are complete, click **Next**.

Please wait while the **Network Setup Wizard** configures the computer. This may take a few minutes.



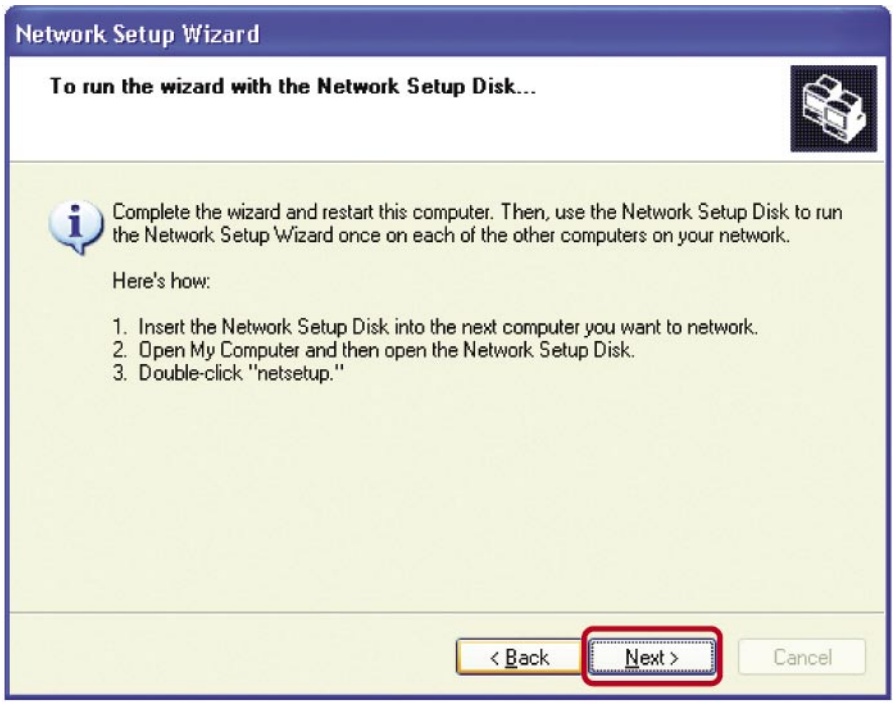
In the window below, select the option that fits your needs. In this example, **Create a Network Setup Disk** has been selected. You will run this disk on each of the computers on your network. Click **Next**.

Insert a disk into the Floppy Disk Drive, in this case drive **A.**



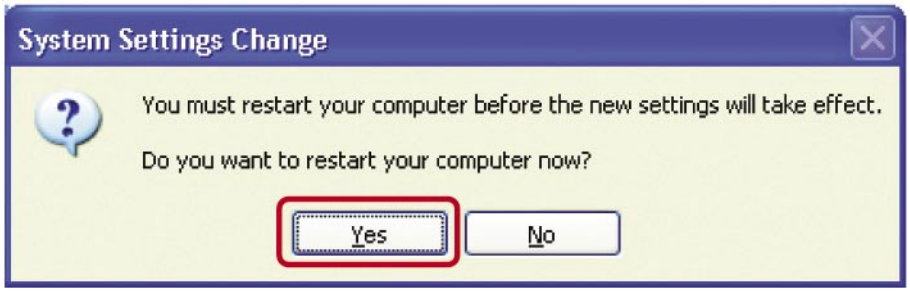
Click **Next**.

Please read the information under **Here's how** in the screen below. After you complete the **Network Setup Wizard** you will use the **Network Setup Disk** to run the **Network Setup Wizard** once on each of the computers on your network. To continue click **Next.**



Please read the information on this screen, then click **Finish** to complete the **Network Setup Wizard**.

The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.



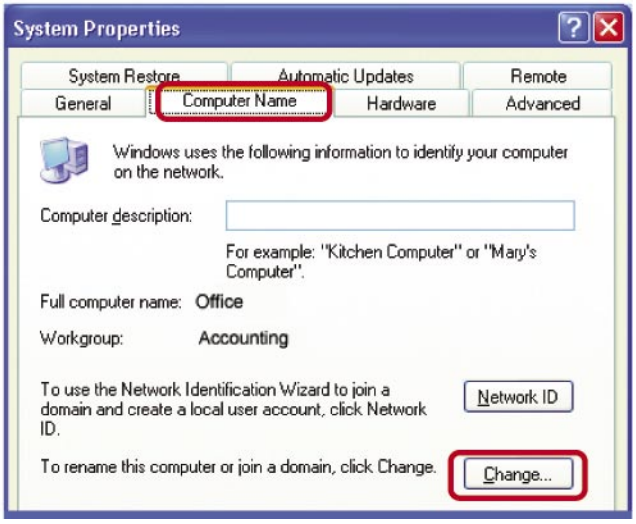
You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new wireless network will be ready to use.

Naming your Computer

To name your computer, please follow these directions:In **Windows XP**:

- Click **Start** (in the lower left corner of the screen)
- **Right-click** on **My Computer**
- Select **Properties** and click

- Select the **Computer Name Tab** in the System Properties window.
- You may enter a **Computer Description** if you wish; this field is optional.
- To rename the computer and join a domain, Click **Change**.



Naming your Computer

- In this window, enter the **Computer name**.
- Select **Workgroup** and enter the name of the **Workgroup**.
- All computers on your network must have the same **Workgroup** name.
- Click **OK**.

Checking the IP Address in Windows XP

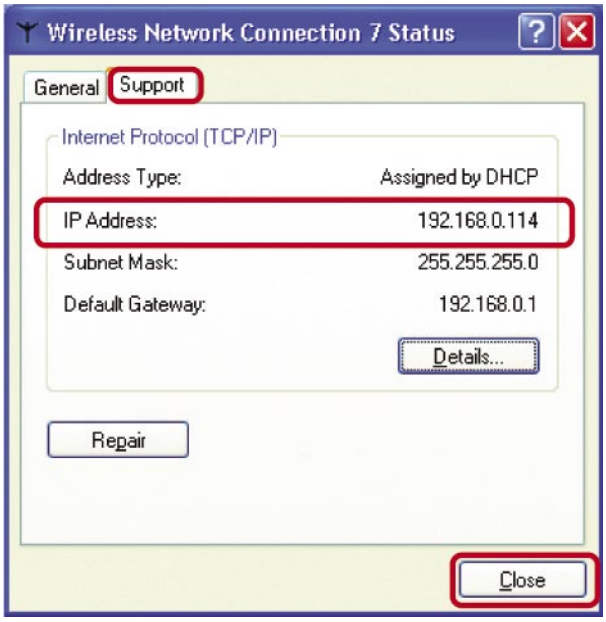
The wireless adapter-equipped computers in your network must be in the same IP Address range (see Getting Started in this manual for a definition of IP Address Range.) To check on the IP Address of the adapter, please do the following:

- Click on **Status**.

- Right-click on the ***Local Area Connection icon*** in the task bar.

Checking the IP Address in Windows XP

This window will appear.



- Click the **Support tab**
- Click **Close**

Assigning a Static IP Address in Windows XP/2000

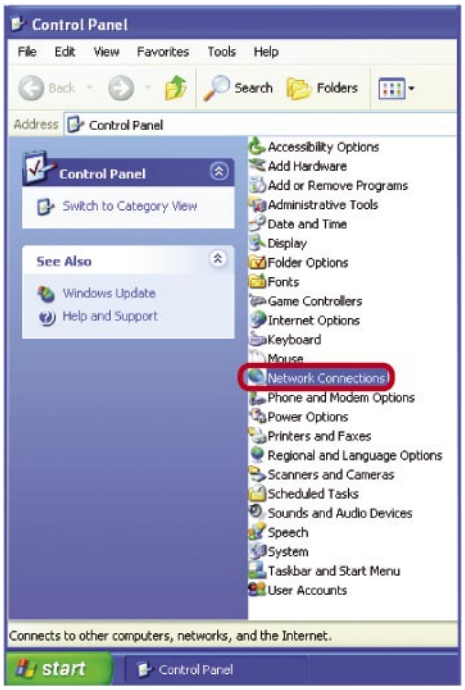
***Note**: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.*

If you are not using a DHCP capable Gateway/Router, or you need to assign a Static IP Address, please follow these instructions:

- Go to **Start**
- Double-click on **Control Panel**

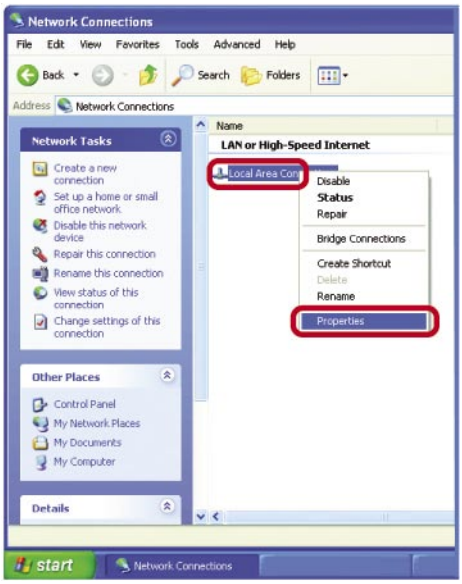
Assigning a Static IP Address in Windows XP/2000

- Double-click on **Network Connections**



- Right-click on **Local Area Connections**

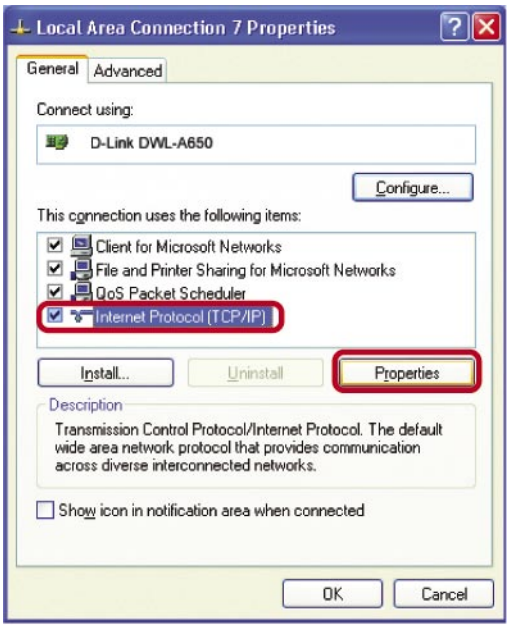
- Double-click on **Properties**



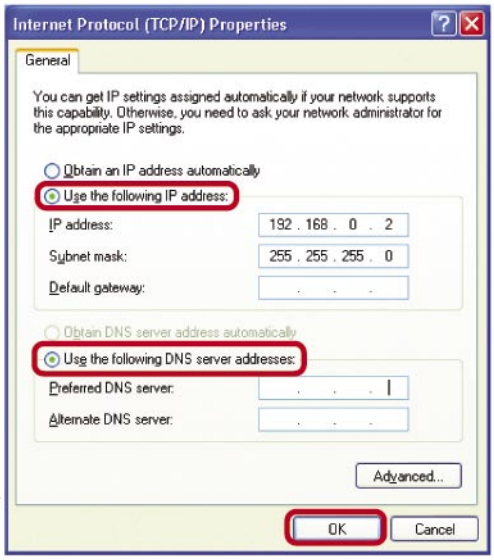
Assigning a Static IP Address in Windows XP/2000

- Click on **Internet Protocol (TCP/IP)**

- Click **Properties**



- Input your **IP address and subnet mask.** (The IP Addresses on your network must be within the same range. For example, if one computer has an IP Address of 192.168.0.2, the other computers should have IP Addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)



- Input your **DNS server addresses. (Note: If you are entering a DNS server, you must enter the IP Address of the Default Gateway.)**

The DNS server information will be supplied by your ISP (Internet Service Provider.)

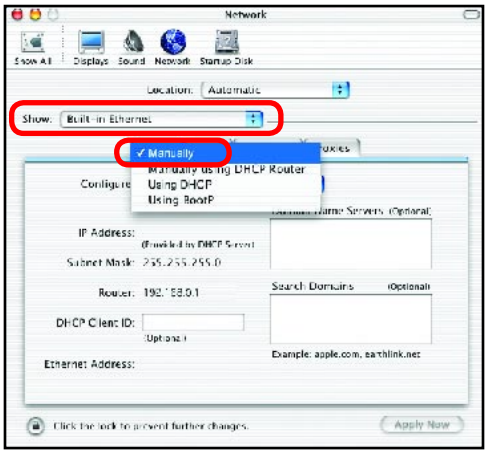
- Click **OK**

Assigning a Static IP Address with Macintosh OSX

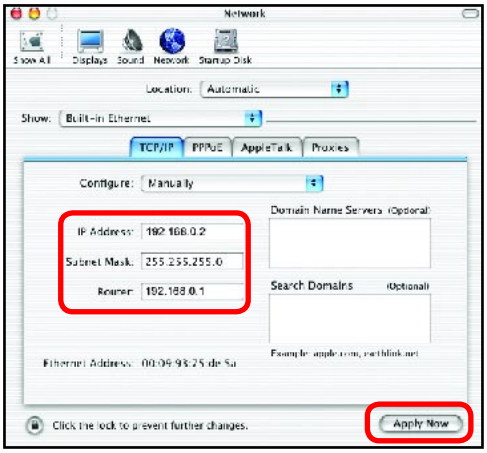
- Go to the **Apple Menu** and select **System Preferences**

- Click on **Network**

- Select **Built-in Ethernet** in the **Show** pull-down menu
- Select **Manually** in the **Configure** pull-down menu

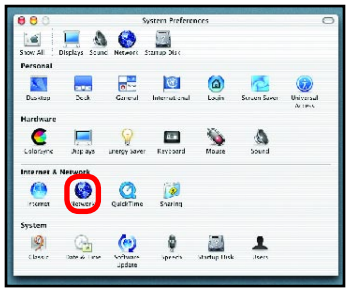


- Input the **Static IP Address**, the **Subnet Mask** and the **Router IP Address** in the appropriate fields
- Click **Apply Now**

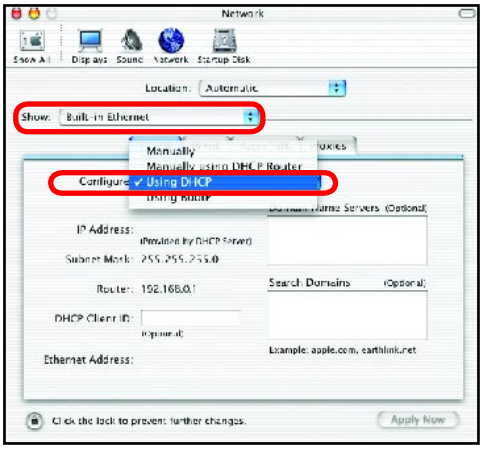


Selecting a Dynamic IP Address with Macintosh OSX

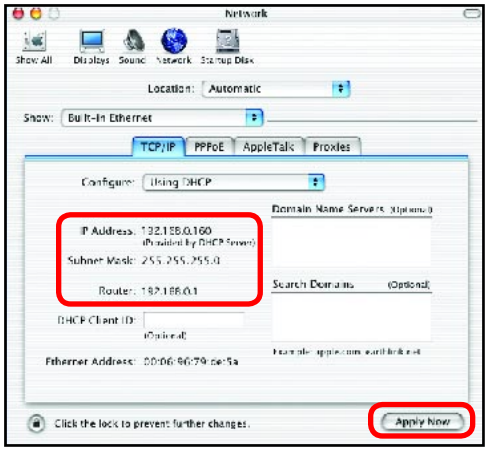
- Go to the **Apple Menu** and select **System Preferences**
- Click on **Network**



- Select **Built-in Ethernet** in the **Show** pull-down menu
- Select **Using DHCP** in the **Configure** pull-down menu

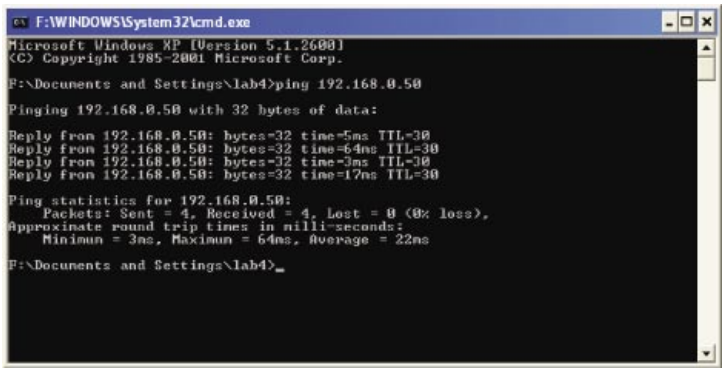


- Click **Apply Now**
- The **IP Address, Subnet mask**, and the **Router's IP Address** will appear in a few seconds



Checking the Wireless Connection by Pinging in Windows XP and 2000

- Go to **Start** > **Run** > type **cmd**. A window similar to this one will appear. Type **ping xxx.xxx.xxx.xxx**, where **xxx** is the **IP Address** of the Wireless Router or Access Point. A good wireless connection will show four replies from the Wireless Router or Acess Point, as shown.



.

Troubleshooting

This Chapter provides solutions to problems that can occur during the installation and operation of the DI-624S Wireless Broadband Router. We cover various aspects of the network setup, including the network adapters. Please read the following if you are having problems.

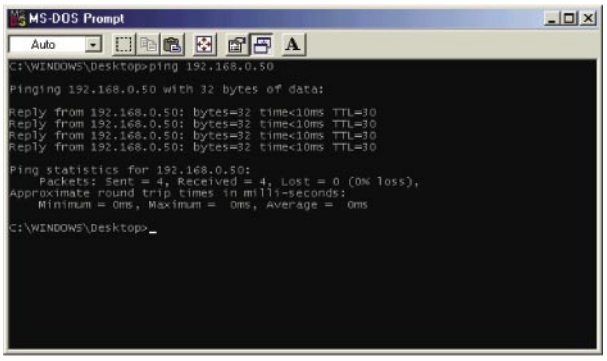
> ***Note: It is recommended that you use an Ethernet connection to configure the DI-624S Wireless Broadband Router.***

1.The computer used to configure the DI-624S cannot access the Configuration menu.

- Check that the **Ethernet LED** on the DI-624S is **ON**. If the **LED** is not **ON**, check that the cable for the Ethernet connection is securely inserted.
- Check that the Ethernet Adapter is working properly. Please see item 3 (***Check that the drivers for the network adapters are installed properly***) in this **Troubleshooting** section to check that the drivers are loaded properly.
- Check that the **IP Address** is in the same range and subnet as the DI-624S. Please see ***Checking the IP Address in Windows XP*** in the **Networking Basics** section of this manual.

Note: The IP Address of the DI-624S is 192.168.0.1. All the computers on the network must have a unique IP Address in the same range, e.g., 192.168.0.x. Any computers that have identical IP Addresses will not be visible on the network. They must all have the same subnet mask, e.g., 255.255.255.0

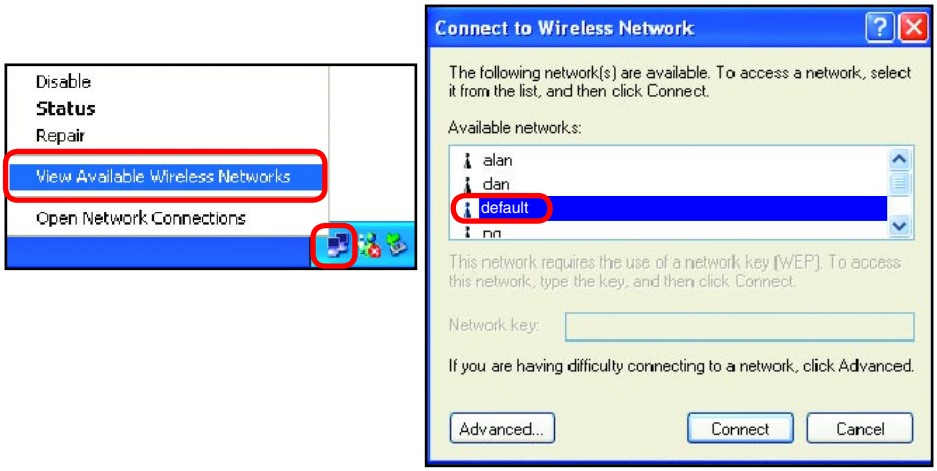
- Do a **Ping test** to make sure that the DI-624S is responding. Go to **Start**>**Run**>Type **Command**>Type **ping 192.168.0.1.** A successful ping will show four replies.



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

2. The wireless client cannot access the Internet in the Infrastructure mode.

Make sure the wireless client is associated and joined with the correct Access Point. To check this connection: **Right-click** on the **Local Area Connection icon** in the taskbar> select **View Available Wireless Networks**. The **Connect to Wireless Network** screen will appear. Please make sure you have selected the correct available network, as shown in the illustrations below.



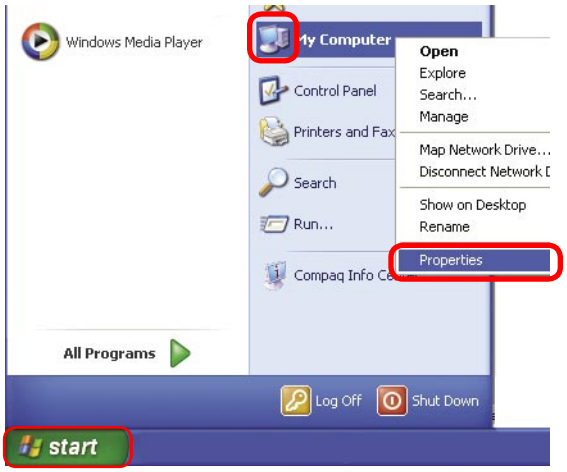
- Check that the **IP Address** assigned to the wireless adapter is within the same **IP Address range** as the access point and gateway. *(Since the DI-624S has an IP Address of 192.168.0.1, wireless adapters must have an IP Address in the same range, e.g., 192.168.0.x. Each device must have a unique IP Address; no two devices may have the same IP Address. The subnet mask must be the same for all the computers on the network.)* To check the **IP Address** assigned to the wireless adapter, **double-click** on the **Local Area Connection icon** in the taskbar > select the **Support tab** and the **IP Address** will be displayed. *(Please refer to **Checking the IP Address** in the **Networking Basics** section of this manual.)*

- If it is necessary to assign a **Static IP Address** to the wireless adapter, please refer to the appropriate section in **Networking Basics**. If you are entering a **DNS Server address** you must also enter the **Default Gateway Address.** *(Remember that if you have a DHCP-capable router, you will not need to assign a Static IP Address. See **Networking Basics: Assigning a Static IP Address.**)*

3. Check that the drivers for the network adapters are installed properly.

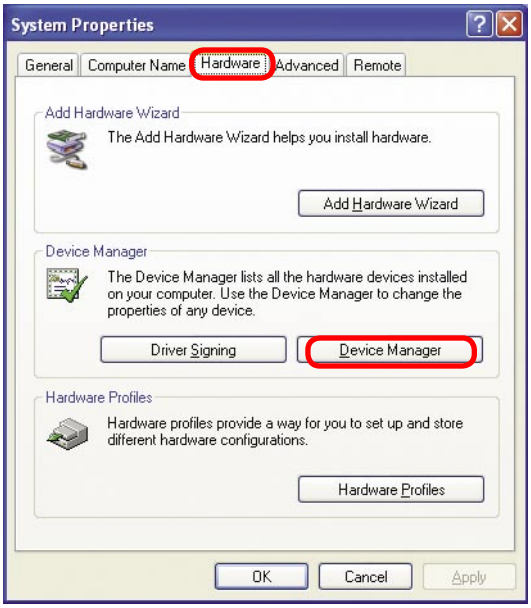
You may be using different network adapters than those illustrated here, but this procedure will remain the same, regardless of the type of network adapters you are using.

- Go to **Start** > **My Computer** (Right-click) > **Properties**

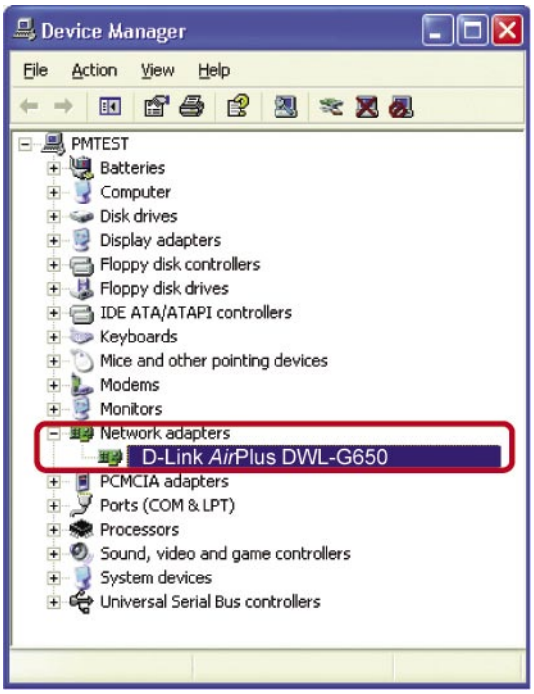


- **Select** the **Hardware Tab**

- Click **Device Manager**



- Double-click on **Network Adapters**



- Right-click on **D-Link *Air*Plus DWL-G650 Wireless Cardbus Adapter** (In this example we use the DWL-G650; you may be using other network adapters, but the procedure will remain the same.)

- Select **Properties** to check that the drivers are installed properly.

- Look under **Device Status** to check that the device is working properly.

- Click **OK**

4. What variables may cause my wireless products to lose reception?

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

5. Why does my wireless connection keep dropping?

- Antenna Orientation- Try different antenna orientations for the DI-624S. Try to keep the antenna at least 6 inches away from the wall or other objects.
- If you are using 2.4GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, and lights, your wireless connection will degrade dramatically or drop altogether. Try changing the Channel on your Router, Access Point and Wireless adapter to a different Channel to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

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

If you have enabled Encryption on the DI-624S, you must also enable encryption on all wireless clients in order to establish a wireless connection.

- For 802.11g, the Encryption settings are: 64 or 128 bit. Make sure that the encryption bit level is the same on the Router and the Wireless Client.
- Make sure that the SSID on the Router and the Wireless Client are exactly the same. If they are not, wireless connection will not be established.
- Move the DI-624S and the wireless client into the same room and then test the wireless connection.
- Disable all security settings. (WEP, MAC Address Control)

6. Why can't I get a wireless connection? (continued)

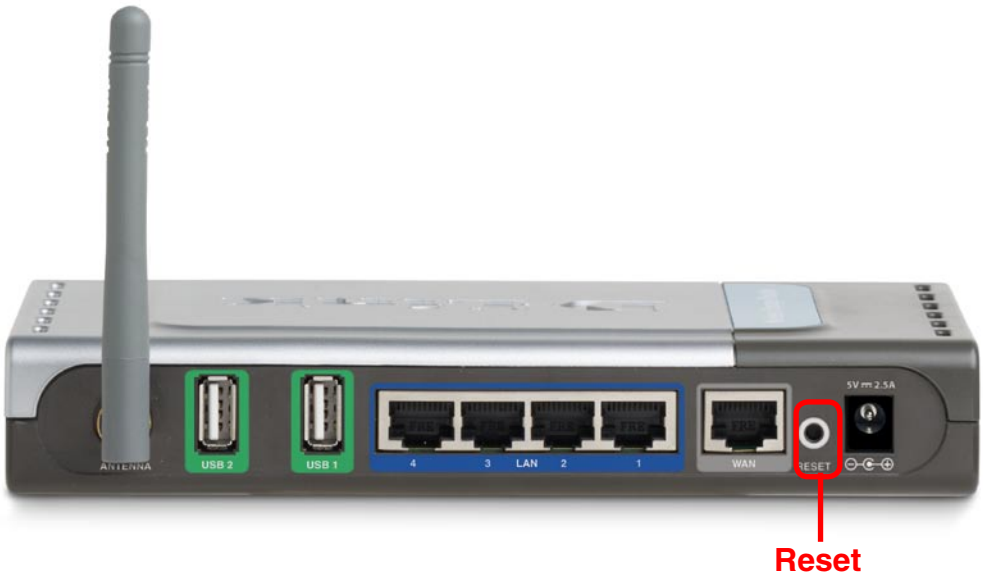
- Turn off your DI-624S and the client. Turn the DI-624S back on again, and then turn on the client.
- Make sure that all devices are set to **Infrastructure** mode.
- Check that the LED indicators are indicating normal activity. If not, check that the AC power and Ethernet cables are firmly connected.
- Check that the IP Address, subnet mask, gateway and DNS settings are correctly entered for the network.
- If you are using 2.4GHz cordless phones, X-10 equipment or other home security systems, ceiling fans, and lights, your wireless connection will degrade dramatically or drop altogether. Try changing the Channel on your DI-624S, and on all the devices in your network to avoid interference.
- Keep your product away (at least 3-6 feet) from electrical devices that generate RF noise, like microwaves, monitors, electric motors, etc.

7. I forgot my encryption key.

- Reset the DI-624S to its factory default settings and restore the other devices on your network to their default settings. You may do this by pressing the Reset button on the back of the unit. You will lose the current configuration settings.

8. Resetting the DI-624S to Factory Default Settings

After you have tried other methods for troubleshooting your network, you may choose to **Reset** the DI-624S to the factory default settings. Remember that D-Link *Air*Plus *Xtreme G*™ products network together, out of the box, at the factory default settings.



To hard-reset the DI-624S to Factory Default Settings, please do the following:

- Locate the **Reset** button on the back of the DI-624S
- Use a paper clip to press the **Reset** button
- Hold for about 10 seconds and then release
- After the DI-624S reboots (this may take a few minutes) it will be reset to the factory **Default** settings

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 v7 or later; or other Java-enabled browsers
- 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

- 32ºF to 131ºF (0ºC to 55ºC)

Humidity:

- 95% maximum (non-condensing)

Safety and Emissions:

- FCC
- CE

Wireless Frequency Range:

- 2.4GHz to 2.462GHz

LEDs:

- Power
- Status
- WAN
- LAN (10/100) x 4
- USB x 2
- WLAN (Wireless Connection)

Physical Dimensions:

- L = 7.56 inches (189mm)
- W = 4.65 inches (116.25mm)
- H = 1.375 inches (34.375mm)

Wireless Transmit Power:

- 15dBm ?2dB

Security:

- WPA- WiFi Protected Access (64-,128-WEP with TKIP, MIC, IV Expansion, Shared Key Authentication)

External Antenna Type:

- Single detachable reverse SMA

Modulation Technology:

- Orthogonal Frequency Division Multiplexing (OFDM) Complementary Code Keying (CCK)

Power Input:

- Ext. Power Supply DC 5V, 2.5A

Weight:

- 10.8 oz. (0.3kg)

Warranty:

- 1 year

Wireless Data Rates with Automatic Fallback:

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

Receiver Sensitivity:

- 108Mbps
- 54Mbps OFDM, 10% PER, -68dBm
- 48Mbps OFDM, 10% PER, -68dBm
- 36Mbps OFDM, 10% PER, -75dBm
- 24Mbps OFDM, 10% PER, -79dBm
- 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

Frequently Asked Questions

Why can´t I access the web-based configuration?

When entering the IP Address of the DI-624S (192.168.0.1), you are not connecting to the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

To resolve difficulties accessing a web utility, please follow the steps below.

Step 1 Verify physical connectivity by checking for solid link lights on the device. If you do not get a solid link light, try using a different cable or connect to a different port on the device if possible. If the computer is turned off, the link light may not be on.

What type of cable should I be using?

The following connections require a Crossover Cable:
Computer to Computer
Computer to Uplink Port
Computer to Access Point
Computer to Print Server
Computer/XBOX/PS2 to DWL-810
Computer/XBOX/PS2 to DWL-900AP+
Uplink Port to Uplink Port (hub/switch)
Normal Port to Normal Port (hub/switch)

The following connections require a Straight-through Cable:
Computer to Residential Gateway/Router
Computer to Normal Port (hub/switch)
Access Point to Normal Port (hub/switch)
Print Server to Normal Port (hub/switch)
Uplink Port to Normal Port (hub/switch)

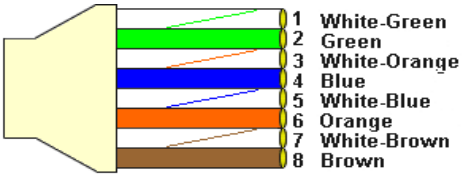
Rule of Thumb:
"If there is a link light, the cable is right."

Why can´t I access the web based configuration? (continued)

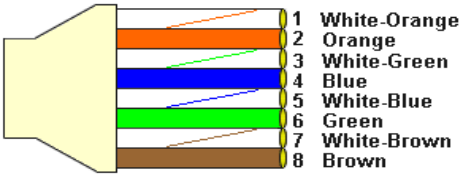
What type of cable should I be using? (continued)

What´s the difference between a crossover cable and a straight-through cable?

The wiring in crossover and straight-through cables are different. The two types of cable have different purposes for different LAN configurations. EIA/TIA 568A/568B define the wiring standards and allow for two different wiring color codes as illustrated in the following diagram.



568A CABLE END



568B CABLE END

**The wires with colored backgrounds may have white stripes and may be denoted that way in diagrams found elsewhere.*

How to tell straight-through cable from a crossover cable:

The main way to tell the difference between the two cable types is to compare the wiring order on the ends of the cable. If the wiring is the same on both sides, it is straight-through cable. If one side has opposite wiring, it is a crossover cable.

All you need to remember to properly configure the cables is the pinout order of the two cable ends and the following rules:

A straight-through cable has identical ends
A crossover cable has different ends

It makes no functional difference which standard you follow for straight-through cable ends, as long as both ends are the same. You can start a crossover cable with either standard as long as the other end is the other standard. It makes no functional difference which end is which. The order in which you pin the cable is important. Using a pattern other than what is specified in the above diagram could cause connection problems.

When to use a crossover cable and when to use a straight-through cable:

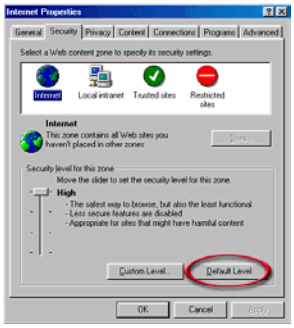
Computer to Computer – Crossover
Computer to an normal port on a Hub/Switch – Straight-through
Computer to an uplink port on a Hub/Switch - Crossover
Hub/Switch uplink port to another Hub/Switch uplink port – Crossover
Hub/Switch uplink port to another Hub/Switch normal port - Straight-through

Why can´t I access the web based configuration? (continued)

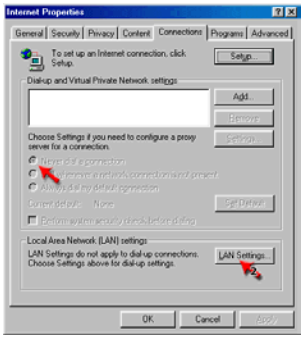
Step 2 Disable any Internet security software running on the computer. Software firewalls like Zone Alarm, Black Ice, Sygate, Norton Personal Firewall, etc. might block access to the configuration pages. Check the help files included with your firewall software for more information on disabling or configuring it.

Step 3 Configure your Internet settings.

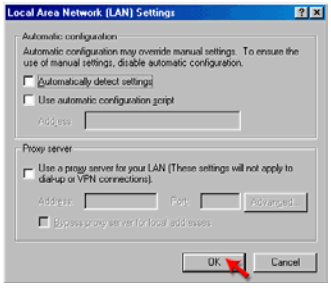
Go to **Start>Settings>Control Panel**. Double click the **Internet Options** Icon. From the **Security** tab, click the button to restore the settings to their defaults.



Click the **Connection** tab and set the dial-up option to **Never Dial a Connection**. Click the **LAN Settings** button.

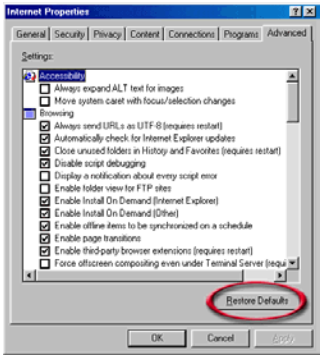


Nothing should be checked. Click **OK**.



Go to the **Advanced** tab and click the button to restore these settings to their defaults.

Click **OK**. Go to the desktop and close any open windows.



Why can´t I access the web based configuration? (continued)

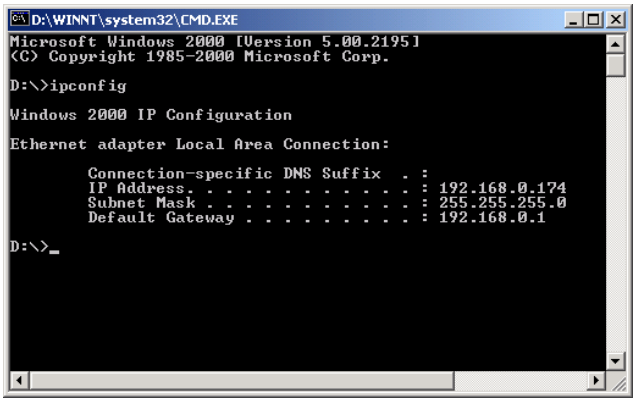
Step 4 (continued) Check your IP Address. Your computer must have an IP Address in the same range of the device you are attempting to configure. Most D-Link devices use the 192.168.0.X range.

How can I find my IP Address in Windows 2000/XP?

Step 1 Click on **Start** and select **Run**.

Step 2 Type **cmd** then click **OK**.

Step 3 From the Command Prompt, enter **ipconfig**. It will return your IP Address, subnet mask, and default gateway



Step 4 Type **exit** to close the command prompt.

Why can´t I access the web based configuration? (continued)

Step 4 (continued) Check your IP Address. Your computer must have an IP Address in the same range of the device you are attempting to configure. Most D-Link devices use the 192.168.0.X range.

Make sure you take note of your computer´s Default Gateway IP Address. The Default Gateway is the IP Address of the D-Link router. By default, it should be 192.168.0.1.

How can I assign a Static IP Address in Windows XP?

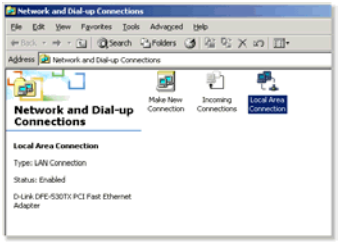
Step 1

Click on **Start > Control Panel > Network and Internet Connections > Network connections**.

Step 2 See Step 2 for Windows 2000 and continue from there.

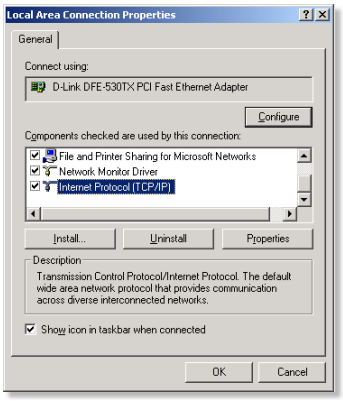
How can I assign a Static IP Address in Windows 2000?

Step 1 Right-click on **My Network Places** and select **Properties**.



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

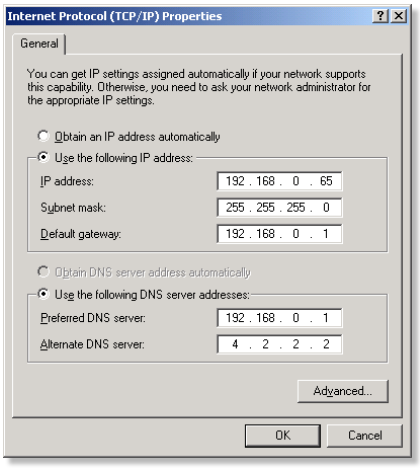
Highlight **Internet Protocol (TCP/IP)** and click **Properties.**



Why can´t I access the web based configuration? (continued)

How can I assign a Static IP Address in Windows 2000? (continued)

Click **Use the following IP Address** and enter an IP Address that is on the same subnet as the LAN IP Address on your router. Example: If the router´s LAN IP Address is 192.168.0.1, make your IP Address 192.168.0.X where X = 2-99. Make sure that the number you choose is not in use on the network.



Set **the Default Gateway** to be the same as the LAN IP Address of your router (192.168.0.1).

Set **the Primary DNS** to be the same as the LAN IP address of your router (192.168.0.1).

The Secondary DNS is not needed or enter a DNS server from your ISP.

Click **OK** twice. You may be asked if you want to reboot your computer. Click **Yes**.

How can I setup my router to work with a Cable modem connection?

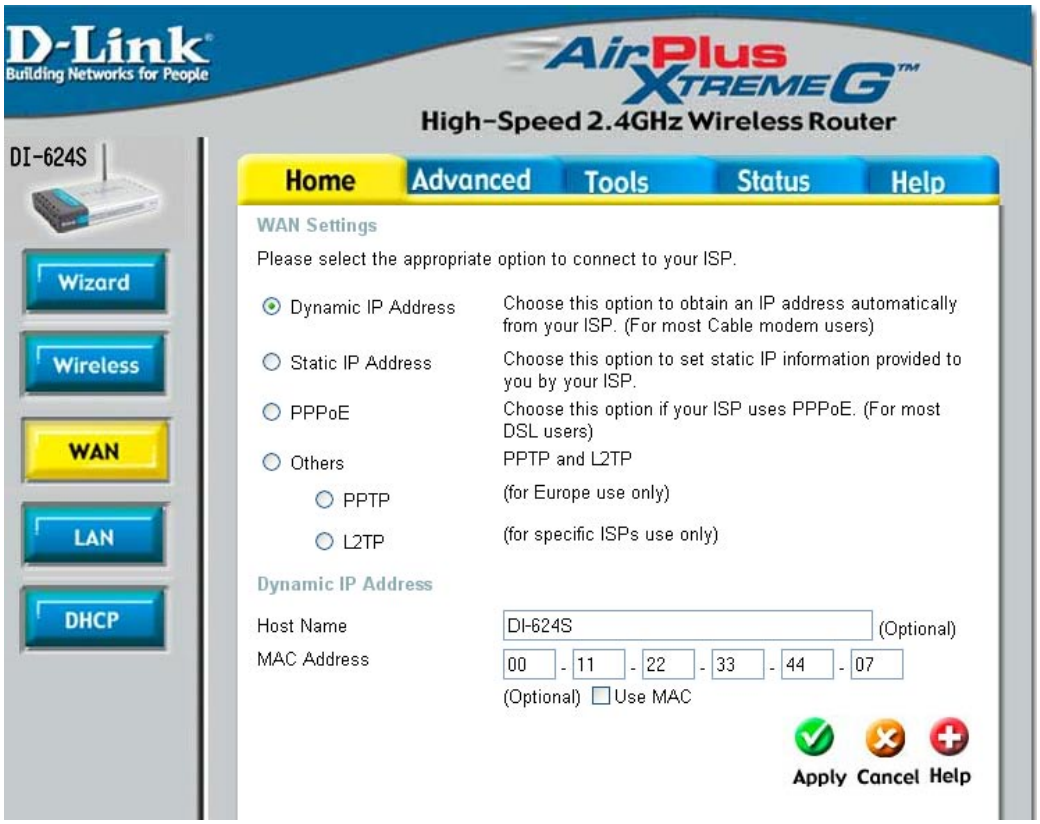
Dynamic Cable connection

(i.e. AT&T-BI, Cox, Adelphia, Rogers, Roadrunner, Charter, and Comcast)

Note: Please configure the router with the computer that was last connected directly to the cable modem.

Step 1 Log into the web based configuration by typing in the IP Address of the router (default:192.168.0.1) in your web browser. The username is **admin** (all lowercase) and the password is **blank** (nothing).

Step 2 Click the **Home** tab and click the **WAN** button. Dynamic IP Address is the default value, however, if Dynamic IP Address is not selected as the WAN type, select Dynamic IP Address by clicking on the radio button. Click **Clone Mac Address**. Click on **Apply** and then **Continue** to save the changes.



How can I setup my router to work with a Cable modem connection? (continued)

Step 3 Power cycle the cable modem and router:

Turn the cable modem off (first) . Turn the router off Leave them off for 2 minutes.** Turn the cable modem on (first). Wait until you get a solid cable light on the cable modem. Turn the router on. Wait 30 seconds.

** If you have a Motorola (Surf Board) modem, leave off for at least 5 minutes.

Step 4 Follow step 1 again and log back into the web configuration. Click the **Status** tab and click the **Device Info** button. If you do not already have a public IP Address under the **WAN** heading, click on the **DHCP Renew** and **Continue** buttons.

Static Cable Connection

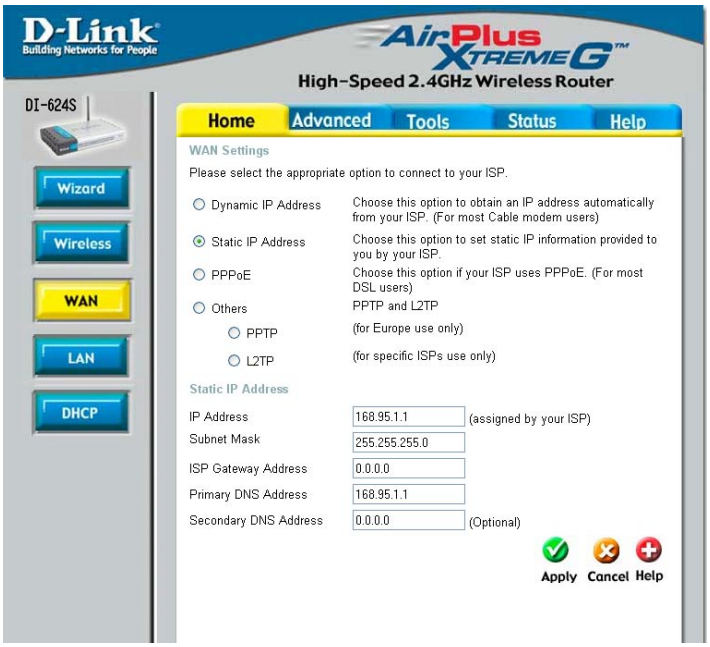
Step 1 Log into the web based configuration by typing in the IP Address of the router (default:192.168.0.1) in your web browser. The username is **admin** (all lowercase) and the password is **blank** (nothing).

Step 2 Click the **Home** tab and click the **WAN** button. Select **Static IP Address** and enter your static settings obtained from the ISP in the fields provided.

If you do not know your settings, you must contact your ISP.

Step 3 Click on **Apply** and then click **Continue** to save the changes.

Step 4 Click the **Status** tab and click the **Device Info** button. Your IP Address information will be displayed under the **WAN** heading.



How can I setup my router to work with Earthlink DSL or any PPPoE connection?

Make sure you disable or uninstall any PPPoE software such as WinPoet or Enternet 300 from your computer or you will not be able to connect to the Internet.

Step 1 Upgrade Firmware if needed.

(Please visit the D-Link tech support website at: http://support.dlink.com for the latest firmware upgrade information.)

Step 2 Take a paperclip and perform a hard reset. With the unit on, use a paperclip and hold down the reset button on the back of the unit for 10 seconds. Release it and the router will recycle, the lights will blink, and then stabilize.

Step 3 After the router stabilizes, open your browser and enter 192.168.0.1 into the address window and hit the **Enter** key. When the password dialog box appears, enter the username **admin** and leave the password blank. Click **OK**.

If the password dialog box does not come up repeat **Step 2**.

Note: Do not run Wizard.

Step 4 Click on the **WAN** tab on left-hand side of the screen. Select **PPPoE**.

Step 5 Select **Dynamic PPPoE** (unless your ISP supplied you with a static IP Address).

Step 6 In the username field enter **ELN/username@earthlink.net** and your password, where username is your own username.

For SBC Global users, enter **username@sbcglobal.net**.
For Ameritech users, enter **username@ameritech.net**.
For BellSouth users, enter **username@bellsouth.net**.
For Mindspring users, enter **username@mindspring.com.**
For most other ISPs, enter **username**.

Step 7 **Maximum Idle Time** should be set to zero. Set **MTU** to 1492, unless specified by your ISP, and set **Autoreconnect** to **Enabled**.

Note: If you experience problems accessing certain websites and/or email issues, please set the MTU to a lower number such as 1472, 1452, etc. Contact your ISP for more information and the proper MTU setting for your connection.

How can I setup my router to work with Earthlink DSL or any PPPoE connection? (continued)

Step 8 Click **Apply**. When prompted, click **Continue**. Once the screen refreshes, unplug the power to the D-Link router.

Step 9 Turn off your DSL modem for 2-3 minutes. Turn back on. Once the modem has established a link to your ISP, plug the power back into the D-Link router. Wait about 30 seconds and log back into the router.

Step 10 Click on the **Status** tab in the web configuration where you can view the device info. Under **WAN**, click **Connect**. Click **Continue** when prompted. You should now see that the device info will show an IP Address, verifying that the device has connected to a server and has been assigned an IP Address.

Can I use my D-Link Broadband Router to share my Internet connection provided by AOL DSL Plus?

In most cases yes. AOL DSL+ may use PPPoE for authentication bypassing the client software. If this is the case, then our routers will work with this service. Please contact AOL if you are not sure.

To set up your router:

Step 1 Log into the web-based configuration (192.168.0.1) and configure the WAN side to use PPPoE.

Step 2 Enter your screen name followed by @aol.com for the user name. Enter your AOL password in the password box.

Step 3 You will have to set the MTU to 1400. AOL DSL does not allow for anything higher than 1400.

Step 4 Apply settings.

Step 5 Recycle the power to the modem for 1 minute and then recycle power to the router. Allow 1 to 2 minutes to connect.

If you connect to the Internet with a different internet service provider and want to use the AOL software, you can do that without configuring the router's firewall settings. You need to configure the AOL software to connect using TCP/IP.

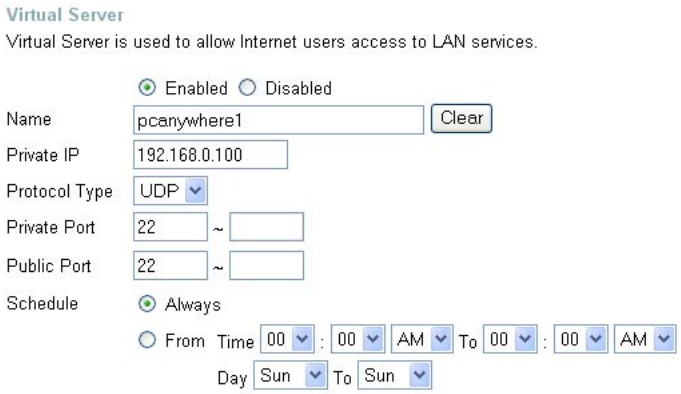
Go to http://www.aol.com for more specific configuration information of their software.

How do I open ports on my router?

To allow traffic from the internet to enter your local network, you will need to open up ports or the router will block the request.

Step 1 Open your web browser and enter the IP Address of your D-Link router (192.168.0.1). Enter username (admin) and your password (blank by default).

Step 2 Click on the **Advanced** on top and then click **Virtual Server** on the left side.



Step 3 Check **Enabled** to activate entry.

Step 4 Enter a name for your virtual server entry.

Step 5 Next to **Private IP**, enter the IP Address of the computer on your local network that you want to allow the incoming service to.

Step 6 Choose **Protocol Type** - either TCP, UDP, or both. If you are not sure, select both.

Step 7 Enter the port information next to **Private Port** and **Public Port**. The private and public ports are usually the same. The public port is the port seen from the WAN side, and the private port is the port being used by the application on the computer within your local network.

Step 8 Enter the **Schedule** information.

Step 9 Click **Apply** and then click **Continue**.

Note: Make sure DMZ host is disabled. If DMZ is enabled, it will disable all Virtual Server entries.

Because our routers use NAT (Network Address Translation), you can only open a specific port to one computer at a time. For example: If you have 2 web servers on your network, you cannot open port 80 to both computers. You will need to configure 1 of the web servers to use port 81. Now you can open port 80 to the first computer and then open port 81 to the other computer.

What is DMZ?

Demilitarized Zone:
In computer networks, a DMZ (demilitarized zone) is a computer host or small network inserted as a neutral zone between a company´s private network and the outside public network. It prevents outside users from getting direct access to a server that has company data. (The term comes from the geographic buffer zone that was set up between North Korea and South Korea following the UN police action in the early 1950s.) A DMZ is an optional and more secure approach to a firewall and effectively acts as a proxy server as well.

In a typical DMZ configuration for a small company, a separate computer (or host in network terms) receives requests from users within the private network for access to Web sites or other companies accessible on the public network. The DMZ host then initiates sessions for these requests on the public network. However, the DMZ host is not able to initiate a session back into the private network. It can only forward packets that have already been requested.

Users of the public network outside the company can access only the DMZ host. The DMZ may typically also have the company´s Web pages so these could be served to the outside world. However, the DMZ provides access to no other company data. In the event that an outside user penetrated the DMZ hosts security, the Web pages might be corrupted but no other company information would be exposed. D-Link, a leading maker of routers, is one company that sells products designed for setting up a DMZ.

How do I configure the DMZ Host?

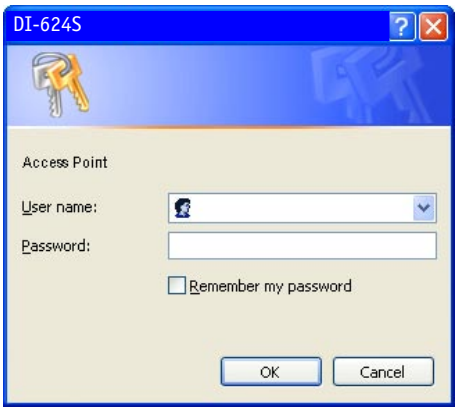
The DMZ feature allows you to forward all incoming ports to one computer on the local network. The DMZ, or Demilitarized Zone, will allow the specified computer to be exposed to the Internet. DMZ is useful when a certain application or game does not work through the firewall. The computer that is configured for DMZ will be completely vulnerable on the Internet, so it is suggested that you try opening ports from the Virtual Server or Firewall settings before using DMZ.

Step 1 Find the IP address of the computer you want to use as the DMZ host.

To find out how to locate the IP Address of the computer in Windows XP/2000 or Macintosh operating systems please refer to Step 4 of the first question in this section (Frequently Asked Questions).

How do I configure the DMZ Host? (continued)

Step 2 Log into the web based configuration of the router by typing in the IP Address of the router (default:192.168.0.1) in your web browser. The username is **admin** (all lowercase) and the password is **blank** (nothing)



Step 3 Click the **Advanced** tab and then click on the **DMZ** button. Select **Enable** and type in the IP Address you found in step 1.

Step 4 Click **Apply** and then **Continue** to save the changes.

Note: When DMZ is enabled, Virtual Server settings will still be effective. Remember, you cannot forward the same port to multiple IP Addresses, so the Virtual Server settings will take priority over DMZ settings.

How do I open a range of ports on my DI-624S using Firewall rules?

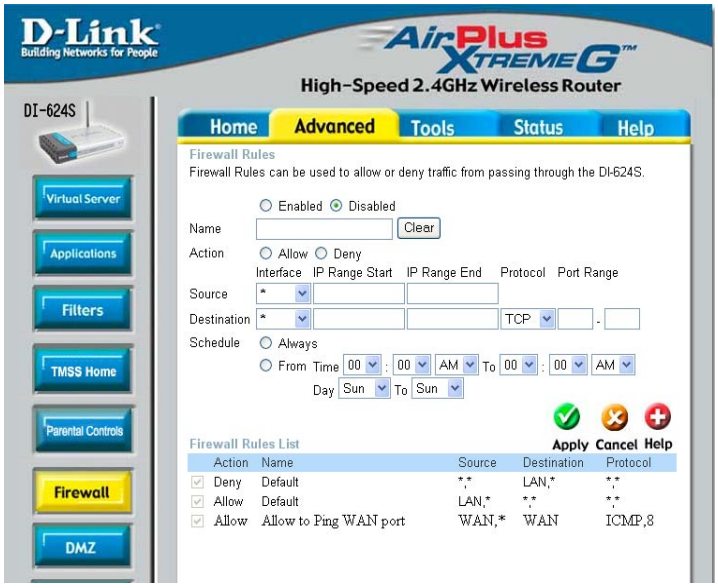
Step 1 Access the router's web configuration by entering the router's IP Address in your web browser. The default IP Address is **192.168.0.1**. Login using your password. The default username is **"admin"** and the password is blank.

If you are having difficulty accessing web management, please see the first question in this section.

Step 2 From the web management Home page, click the **Advanced** tab then click the **Firewall** button.

Step 3 Click on **Enabled** and type in a name for the new rule.

Step 4 Choose **WAN** as the **Source** and enter a range of IP Addresses out on the internet that you would like this rule applied to. If you would like this rule to allow all internet users to be able to access these ports, then put an **Asterisk** in the first box and leave the second box empty.



Step 5 Select **LAN** as the **Destination** and enter the IP Address of the computer on your local network that you want to allow the incoming service to. This will not work with a range of IP Addresses.

Step 6 Enter the port or range of ports that are required to be open for the incoming service.

Step 7 Click **Apply** and then click **Continue**.

Note: Make sure DMZ host is disabled.

Because our routers use NAT (Network Address Translation), you can only open a specific port to one computer at a time. For example: If you have 2 web servers on your network, you cannot open port 80 to both computers. You will need to configure 1 of the web servers to use port 81. Now you can open port 80 to the first computer and then open port 81 to the other computer.

What are virtual servers?

A Virtual Server is defined as a service port, and all requests to this port will be redirected to the computer specified by the server IP. For example, if you have an FTP Server (port 21) at 192.168.0.5, a Web server (port 80) at 192.168.0.6, and a VPN server at 192.168.0.7, then you need to specify the following virtual server mapping table:

Server Port	Server IP	Enable
21	192.168.0.5	X
80	192.168.0.6	X
1723	192.168.0.7	X

How do I use *PC Anywhere* with my DI-624S router?

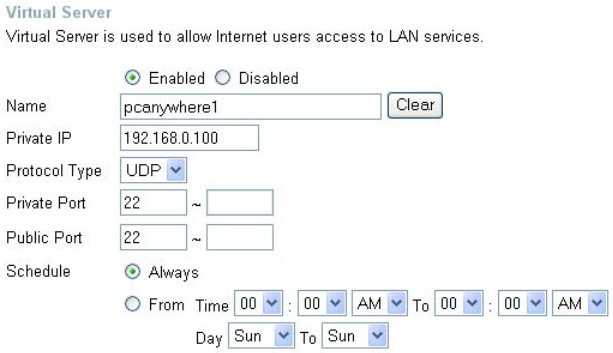
You will need to open 3 ports in the Virtual Server section of your D-Link router.

Step 1 Open your web browser and enter the IP Address of the router (192.168.0.1).

Step 2 Click on **Advanced** at the top and then click **Virtual Server** on the left side.

Step 3 Enter the information as seen below. The **Private IP** is the IP Address of the computer on your local network that you want to connect to.

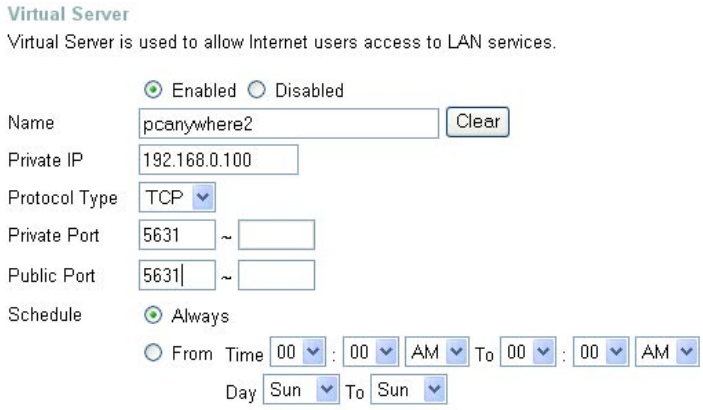
Step 4 The first entry will read as shown here:



Step 5 Click **Apply** and then click **Continue**.

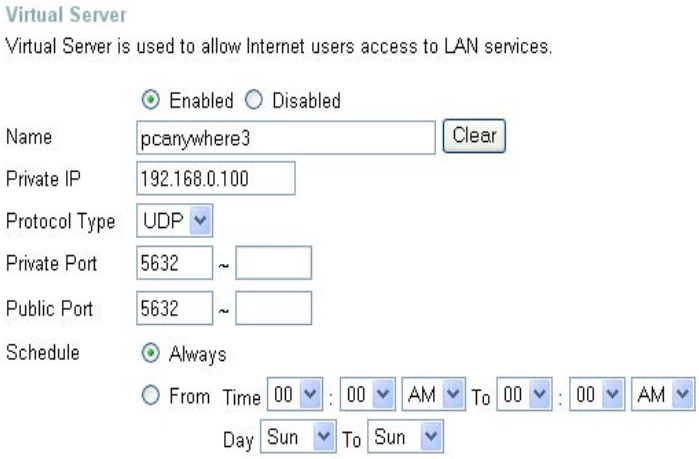
How do I use *PC Anywhere* with my DI-624S router? (continued)

Step 6 Create a second entry as shown here:



Step 7 Click **Apply** and then click **Continue**.

Step 8 Create a third and final entry as shown here:



Step 9 Click **Apply** and then click **Continue**.

Step 10 Run *PCAnywhere* from the remote site and use the WAN IP Address of the router, not your computer´s IP Address.

How can I use *eDonkey* behind my D-Link Router?

You must open ports on your router to allow incoming traffic while using *eDonkey.*

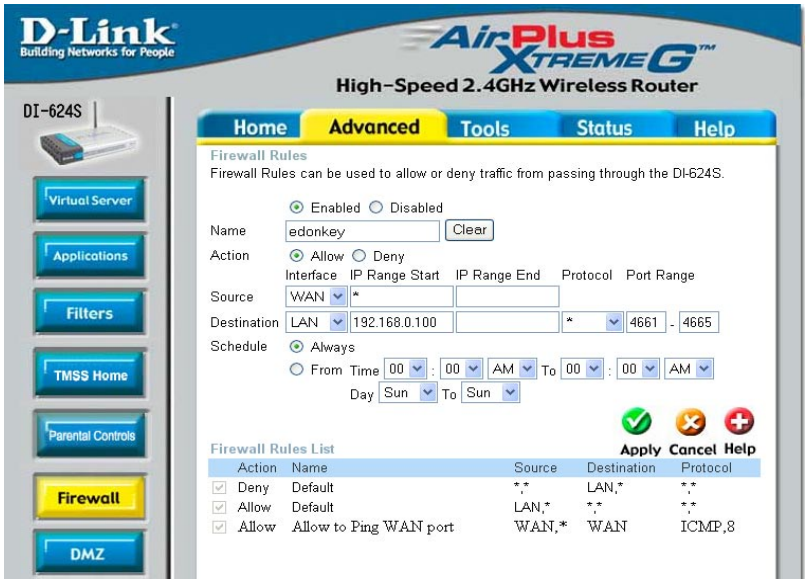
eDonkey uses three ports (4 if using CLI):

4661 (TCP) To connect with a server
4662 (TCP) To connect with other clients
4665 (UDP) To communicate with servers other than the one you are connected to. 4663 (TCP) *Used with the command line (CLI) client when it is configured to allow remote connections. This is the case when using a Graphical Interface (such as the Java Interface) with the client.

Step 1 Open your web browser and enter the IP Address of your router (192.168.0.1). Enter username (admin) and your password (leave blank).

Step 2 Click on **Advanced** and then click **Firewall**.

Step 3 Create a new firewall rule:
Click **Enabled**.
Enter a name (edonkey).
Click **Allow**.
Next to Source, select **WAN** under interface. In the first box, enter an *****. Leave the second box empty.
Next to Destination, select **LAN** under interface. Enter the IP Address of the computer you are running eDonkey from. Leave the second box empty. Under Protocol, select *****. In the port range boxes, enter **4661** in the first box and then **4665** in the second box. Click **Always** or set a schedule.



Step 4 Click **Apply** and then **Continue**.

How do I set up my router for SOCOM on my Playstation 2?

To allow you to play SOCOM and hear audio, you must download the latest firmware for the router (if needed), enable Game Mode, and open port 6869 to the IP Address of your Playstation.

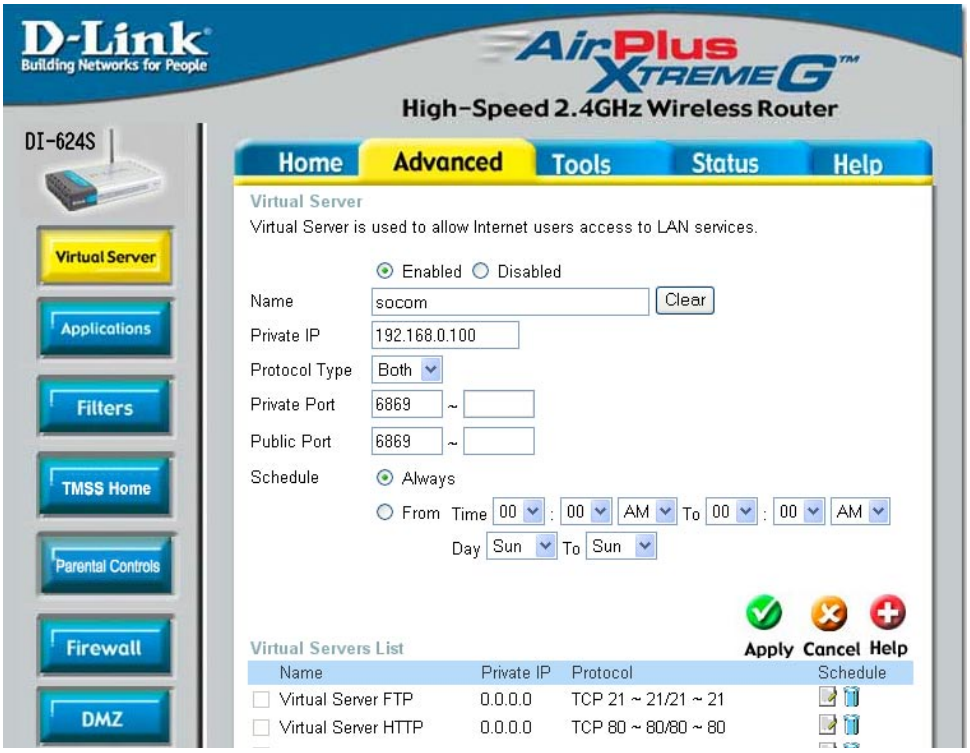
Step 1 Upgrade firmware (follow link above).

Step 2 Open your web browser and enter the IP Address of the router (192.168.0.1). Enter username (admin) and your password (blank by default).

Step 3 Click on the **Advanced** tab and then click on **Virtual Server** on the left side.

Step 4 You will now create a new Virtual Server entry. Click **Enabled** and enter a name (socom). Enter the IP Address of your Playstation for **Private IP**.

Step 5 For **Protocol Type** select Both. Enter **6869** for both the **Private Port** and **Public Port**. Click **Always**. Click **Apply** to save changes and then **Continue**.



Step 6 Click on the **Tools** tab and then **Misc** on the left side.

Step 7 Make sure **Gaming Mode** is Enabled. If not, click **Enabled**. Click **Apply** and then **Continue**.

How can I use Gamespy behind my D-Link router?

Step 1 Open your web browser and enter the IP Address of the router (192.168.0.1). Enter admin for the username and your password (blank by default).

Step 2 Click on the Advanced tab and then click Virtual Server on the left side.

Step 3 You will create 2 entries.

Step 4 Click Enabled and enter Settings:

NAME - Gamespy1

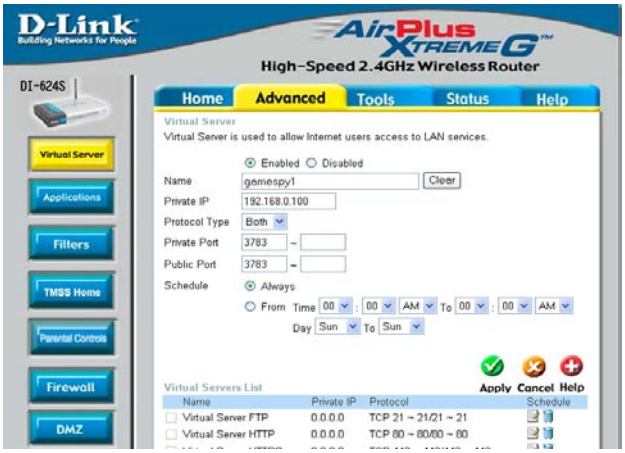
PRIVATE IP - The IP Address of your computer that you are running Gamespy from.

PROTOCOL TYPE - Both

PRIVATE PORT - 3783

PUBLIC PORT - 3783

SCHEDULE - Always.



Click **Apply** and then **continue**.

Step 5 Click Enabled and enter 2nd entry:

NAME - Gamespy2

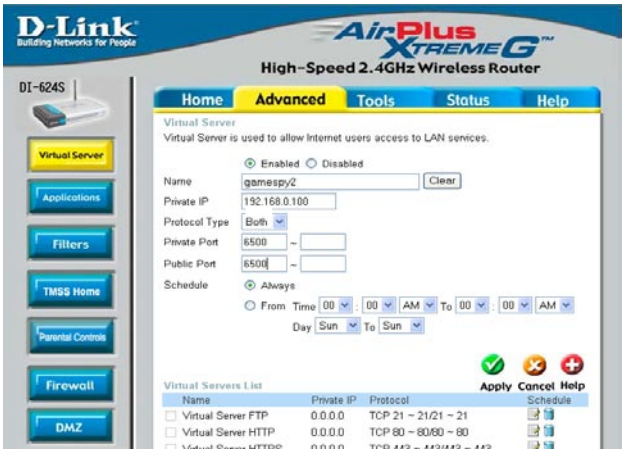
PRIVATE IP - The IP Address of your computer that you are running Gamespy from.

PROTOCOL TYPE - Both

PRIVATE PORT - 6500

PUBLIC PORT - 6500

SCHEDULE - Always.



Click **Apply** and then **continue**.

How do I configure my router for KaZaA and Grokster?

The following is for KaZaA, Grokster, and others using the FastTrack P2P file sharing system.

In most cases, you do not have to configure anything on the router or on the KazaA software. If you are having problems, please follow steps below:

Step 1 Enter the IP Address of your router in a web browser (192.168.0.1).

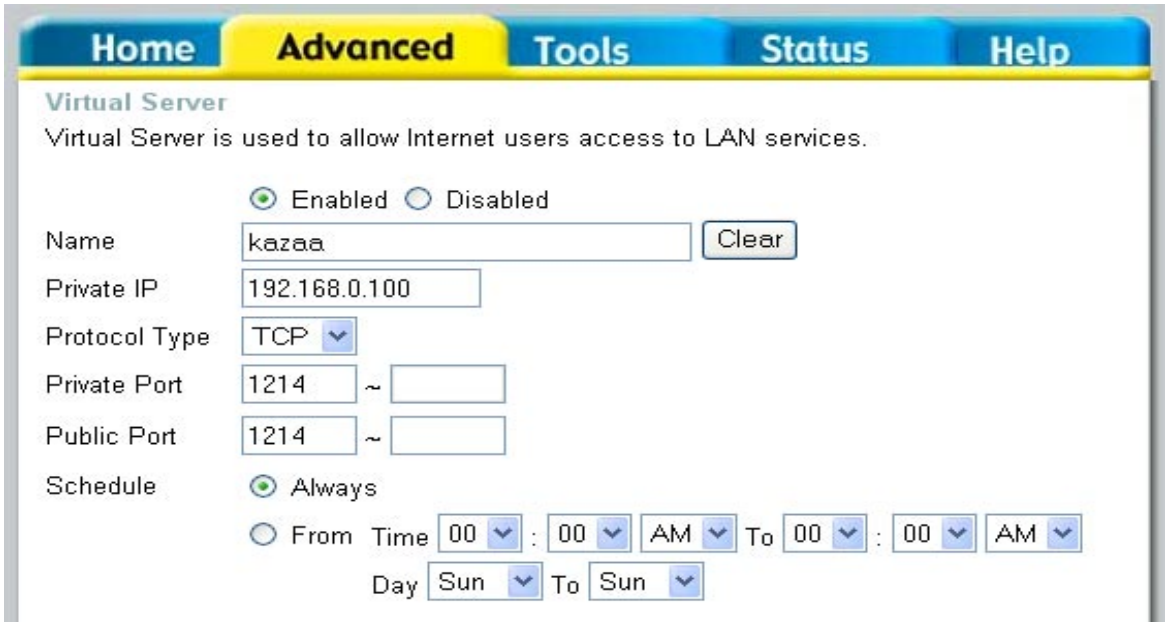
Step 2 Enter your username (admin) and your password (blank by default).

Step 3 Click on Advanced and then click Virtual Server.

Step 4 Click Enabled and then enter a Name (KaZaA for example).

Step 5 Enter the IP Address of the computer you are running KaZaA from in the Private IP box. Select TCP for the Protocol Type.

Step 6 Enter 1214 in the Private and Public Port boxes. Click Always under schedule or set a time range. Click Apply.



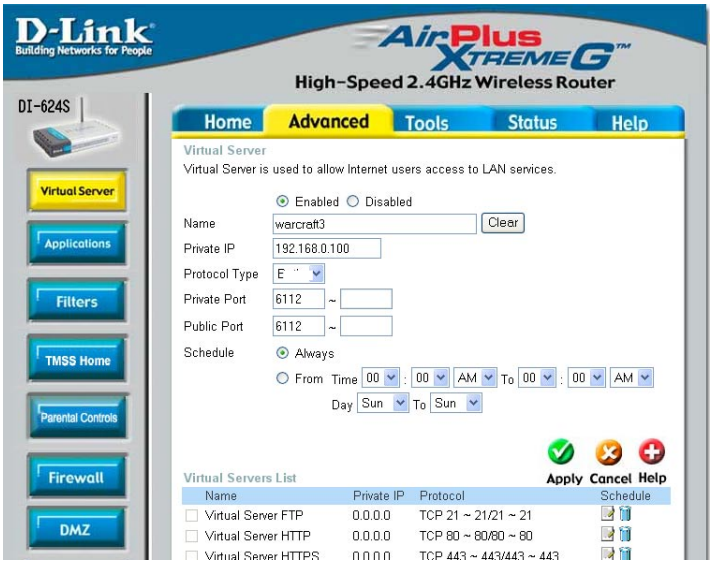
Make sure that you did not enable proxy/firewall in the KaZaA software.

How do I configure my router to play Warcraft 3?

You must open ports on your router to allow incoming traffic while hosting a game in Warcraft 3. To play a game, you do not have to configure your router.

Warcraft 3 (Battlenet) uses port 6112.

For the DI-604, DI-614+. DI624, DI-624S, DI-754, DI-764, or DI-774:



Step 1 Open your web browser and enter the IP Address of your router (192.168.0.1). Enter username (admin) and your password (leave blank).

Step 2 Click on **Advanced** and then click **Virtual Server**.

Step 3 Create a new entry: Click **Enabled**. Enter a name (warcraft3). Private IP - Enter the IP Address of the computer you want to host the game. Select **Both** for Protocol Type Enter **6112** for both Private Port and Public Port Click **Always** or set a schedule.

Step 4 Click **Apply** and then **Continue**.

Note: If you want multiple computers from you LAN to play in the same game that you are hosting, then repeat the steps above and enter the IP Addresses of the other computers. You will need to change ports. Computer #2 can use port 6113, computer #3 can use 6114, and so on.

You will need to change the port information within the Warcraft 3 software for computers #2 and up.

Configure the Game Port information on each computer:
Start Warcraft 3 on each computer, click **Options** > **Gameplay**. Scroll down and you should see **Game Port**. Enter the port number as you entered in the above steps.

How do I use NetMeeting with my D-Link Router?

Unlike most TCP/IP applications, NetMeeting uses **DYNAMIC PORTS** instead of STATIC PORTS. That means that each NetMeeting connection is somewhat different than the last. For instance, the HTTP web site application uses port 80. NetMeeting can use any of over 60,000 different ports.

All broadband routers using (only) standard NAT and all internet sharing programs like Microsoft ICS that use (only) standard NAT will NOT work with NetMeeting or other H.323 software packages.

The solution is to put the router in DMZ.

Note: A few hardware manufacturers have taken it on themselves to actually provide H.323 compatibility. This is not an easy task since the router must search each incoming packet for signs that it might be a netmeeting packet. This is a whole lot more work than a router normally does and may actually be a **weak point in the firewall**. D-Link is not one of the manufacturers.

To read more on this visit http://www.HomenetHelp.com

How do I set up my router to use iChat? -for Macintosh users-

You must open ports on your router to allow incoming traffic while using iChat.

iChat uses the following ports: 5060 (UDP) 5190 (TCP) File Sharing 16384-16403 (UDP) To video conference with other clients.

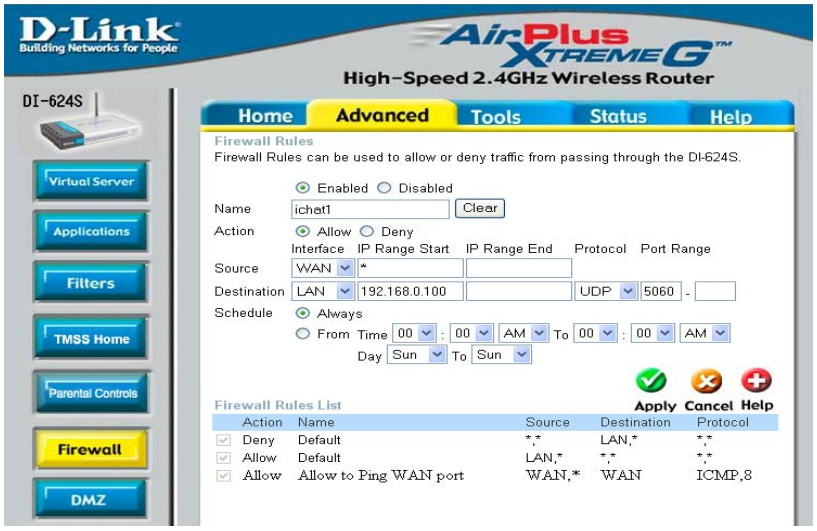
Step 1 Open your web browser and enter the IP Address of your router (192.168.0.1). Enter username (admin) and your password (leave blank).

Step 2 Click on **Advanced** and then click **Firewall**.

How do I set up my router to use iChat? -for Macintosh users- (continued)

Step 3 Create a new firewall rule:

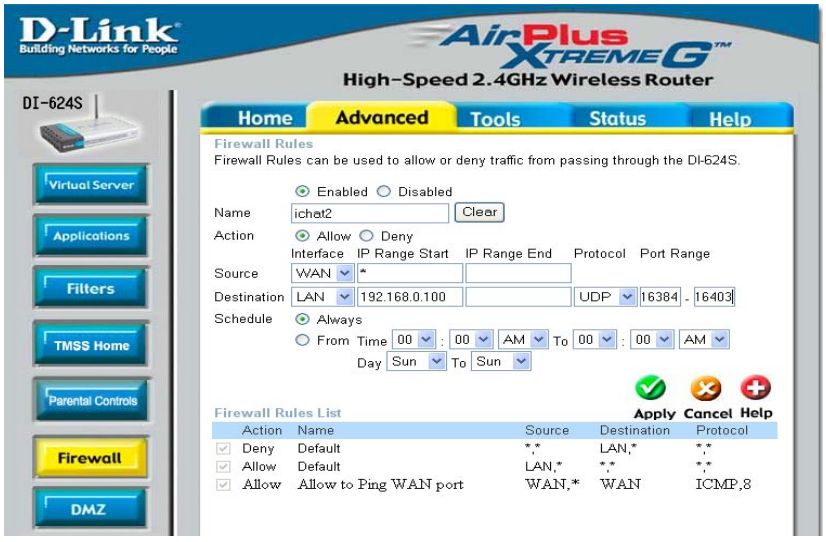
Click **Enabled**.
Enter a name (ichat1).
Click **Allow**.
Next to Source, select **WAN** under interface.
In the first box, enter an ***.**
Leave the second box empty.
Next to Destination, select **LAN** under interface.
Enter the IP Address of the computer you are running iChat from.



Leave the second box empty. Under Protocol, select **UDP**. In the port range boxes, enter **5060** in the first box and leave the second box empty.
Click **Always** or set a schedule.

Step 4 Click **Apply** and then **Continue**.

Step 5
Repeat steps 3 and 4 enter **ichat2** and open ports **16384-16403** (UDP).



How do I set up my router to use iChat? -for Macintosh users- (continued)

For File Sharing:

Step 1 Click on **Advanced** and then **Virtual Server**.

Step 2 Check **Enabled** to activate entry.

Step 3 Enter a name for your virtual server entry (ichat3).

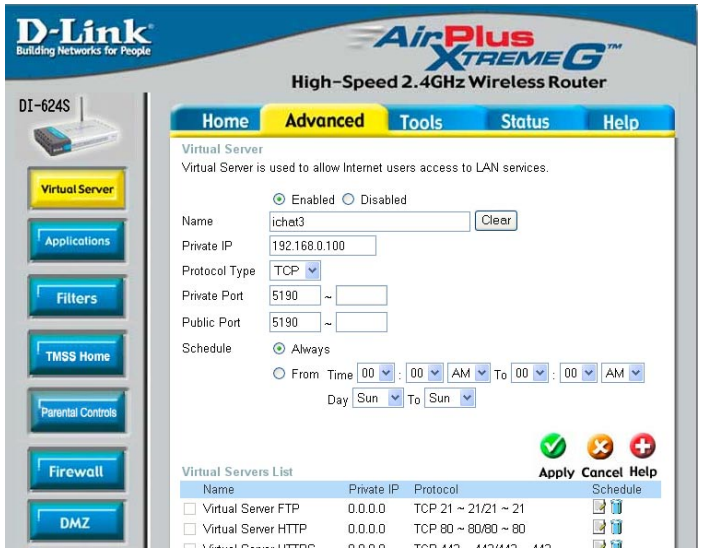
Step 4 Next to Private IP, enter the IP Address of the computer on your local network that you want to allow the incoming service to.

Step 5 Select **TCP** for Protocol Type.

Step 6 Enter **5190** next to Private Port and Public Port.

Stsp 7 Click **Always** or configure a schedule.

Step 8 Click **Apply** and then **Continue**.



If using Mac OS X Firewall, you may need to temporarily turn off the firewall in the Sharing preference pane on both computers.

To use the Mac OS X Firewall, you must open the same ports as in the router:

Step 1 Choose **Apple menu** > **System Preferences**.
Step 2 Choose **View** > **Sharing**.
Step 3 Click the **Firewall** tab.
Step 4 Click **New**.
Step 5 Choose **Other** from the Port Name pop-up menu.
Step 6 In the Port Number, Range or Series field, type in: **5060**, **16384-16403**.
Step 7 In the Description field type in: **iChat AV**.
Step 8 Click **OK**.

How do I send or receive a file via iChat when the Mac OSX firewall is active? -for Macintosh users- Mac OS X 10.2 and later

The following information is from the online Macintosh AppleCare knowledge base:

"iChat cannot send or receive a file when the Mac OS X firewall is active in its default state. If you have opened the AIM port, you may be able to receive a file but not send them.

In its default state, the Mac OS X firewall blocks file transfers using iChat or America Online AIM software. If either the sender or receiver has turned on the Mac OS X firewall, the transfer may be blocked.

The simplest workaround is to temporarily turn off the firewall in the Sharing preference pane on both computers. This is required for the sender. However, the receiver may keep the firewall on if the AIM port is open. To open the AIM port:

Step 1 Choose Apple menu > System Preferences.

Step 2 Choose View > Sharing.

Step 3 Click the Firewall tab.

Step 4 Click New.

Step 5 Choose AOL IM from the Port Name pop-up menu. The number 5190 should already be filled in for you.

Step 6 Click OK.

If you do not want to turn off the firewall at the sending computer, a different file sharing service may be used instead of iChat. The types of file sharing available in Mac OS X are outlined in technical document 106461, "Mac OS X: File Sharing" in the *AppleCare Knowledge base* online.

Note: If you use a file sharing service when the firewall is turned on, be sure to click the Firewall tab and select the service you have chosen in the "Allow" list. If you do not do this, the firewall will also block the file sharing service. "

What is NAT?

NAT stands for **Network Address Translator**. It is proposed and described in RFC-1631 and is used for solving the IP Address depletion problem. Basically, each NAT box has a table consisting of pairs of local IP Addresses and globally unique addresses, by which the box can "translate" the local IP Addresses to global address and vice versa. Simply put, it is a method of connecting multiple computers to the Internet (or any other IP network) using one IP Address.

D-Link´s broadband routers (ie: DI-604) support NAT. With proper configuration, multiple users can access the Internet using a single account via the NAT device.

For more information on RFC-1631: The IP Network Address Translator (NAT), visit http://www.faqs.org/rfcs/rfc1631.html

Contacting Technical Support

Technical Support

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

D-Link provides free technical support for customers within the United States and within Canada for the duration of the warranty period on this product.

U.S. and Canadian customers can contact D-Link technical support through our web site, or by phone.

Tech Support for customers within the United States:

D-Link Technical Support over the Telephone:
(877) 453-5465
24 hours a day, seven days a week.

D-Link Technical Support over the Internet:
http://support.dlink.com
email:support@dlink.com

Tech Support for customers within Canada:

D-Link Technical Support over the Telephone:
(800) 361-5265
Monday to Friday 7:30am to 12:00am EST

D-Link Technical Support over the Internet:
http://support.dlink.ca
email:support@dlink.ca

When contacting technical support, please provide the following information:

- *Serial number of the unit*
- *Model number or product name*
- *Software type and version number*

Warranty

Subject to the terms and conditions set forth herein, D-Link Systems, Inc. ("D-Link") provides this Limited Warranty:

- Only to the person or entity that originally purchased the product from D-Link or its authorized reseller or distributor, and
- Only for 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, or addresses with an APO or FPO.

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

- Hardware (excluding power supplies and fans): One (1) year
- Power supplies and fans: One (1) year
- Spare parts and spare kits: Ninety (90) days

The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, to repair or replace the defective Hardware during the Warranty Period at no charge to the original owner or to refund the actual purchase price paid. Any 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, at its option, 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 or ninety (90) days, whichever is longer, and is subject to the same limitations and exclusions. If a material defect is incapable of correction, or if D-Link determines that it is not practical to repair or replace the defective Hardware, the actual 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 ("Software 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 Software Warranty Period, the magnetic media on which D-Link delivers the Software will be free of physical defects. The customer's sole and exclusive remedy and the entire liability of D-Link and its suppliers under this Limited Warranty will be, at D-Link's option, 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 the portion of the actual purchase price paid that is attributable to the Software. 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. Replacement Software will be warranted for the remainder of the original Warranty Period and is subject to the same limitations and exclusions. 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 portions 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, along with proof of purchase of the product (such as a copy of the dated purchase invoice for the product) if the product is not registered.
- The customer must obtain a Case ID Number from D-Link Technical Support at 1-877-453-5465, who will attempt to assist the customer in resolving any suspected defects with the product. If the product is considered defective, the customer must obtain a Return Material Authorization ("RMA") number by completing the RMA form and entering the assigned Case ID Number at https://rma.dlink.com/.
- 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 and shipped to **D-Link Systems, Inc., 17595 Mt. Herrmann, Fountain Valley, CA 92708**. 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. Return shipping charges shall be prepaid by D-Link if you use an address in the United States, otherwise we will ship the product to you freight collect. Expedited shipping is available upon request and provided shipping charges are prepaid by the customer.

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: The Limited Warranty provided herein by D-Link does not cover: Products that, 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; and 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. While necessary maintenance or repairs on your Product can be performed by any company, we recommend that you use only an Authorized D-Link Service Office. Improper or incorrectly performed maintenance or repair voids this Limited 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 THE DURATION OF THE APPLICABLE WARRANTY PERIOD SET FORTH ABOVE. 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 you 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 owners.

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.

For detailed warranty information applicable to products purchased outside the United States, please contact the corresponding local D-Link office.

Registration

Product registration is entirely voluntary and failure to complete or return this form will not diminish your warranty rights.

(05/31/05)