D-Link *Air*Plus*XtremeG*™

DI-624

High-Speed 2.4 GHz Wireless Router

Manual

D-Link

Building Networks for People

Contents

Package Contents

Contents of Package:

- **D-Link *Air*PlusX*TREME* G DI-624**
  High-Speed 2.4GHz Wireless Router
- Power Adapter-DC 5V, 3.0A
- Manual and Warranty on CD
- Quick Installation Guide
- Ethernet Cable

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

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

System Requirements for Configuration:

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

Introduction

The D-Link *Air*PlusXtreme*G* DI-624 High-Speed Wireless Router is a draft 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-624 provides data transfers at up to 54 Mbps (compared to the standard 11 Mbps) when used with other D-Link *Air*PlusXtreme*G* products. The 802.11g standard is backwards compatible with 802.11b products. This means that you do not need to change your entire network to maintain connectivity. You may sacrifice some of 802.11g's speed when you mix 802.11b and 802.11g devices, but you will not lose the ability to communicate when you incorporate the 802.11g standard into your 802.11b network. You may choose to slowly change your network by gradually replacing the 802.11b devices with 802.11g devices .

In addition to offering faster data transfer speeds when used with other 802.11g products, the DI-624 has the newest, strongest, most advanced security features available today. When used with other 802.11g WPA (WiFi Protected Access) and 802.1x compatible products in a network with a radius server, the security features include:

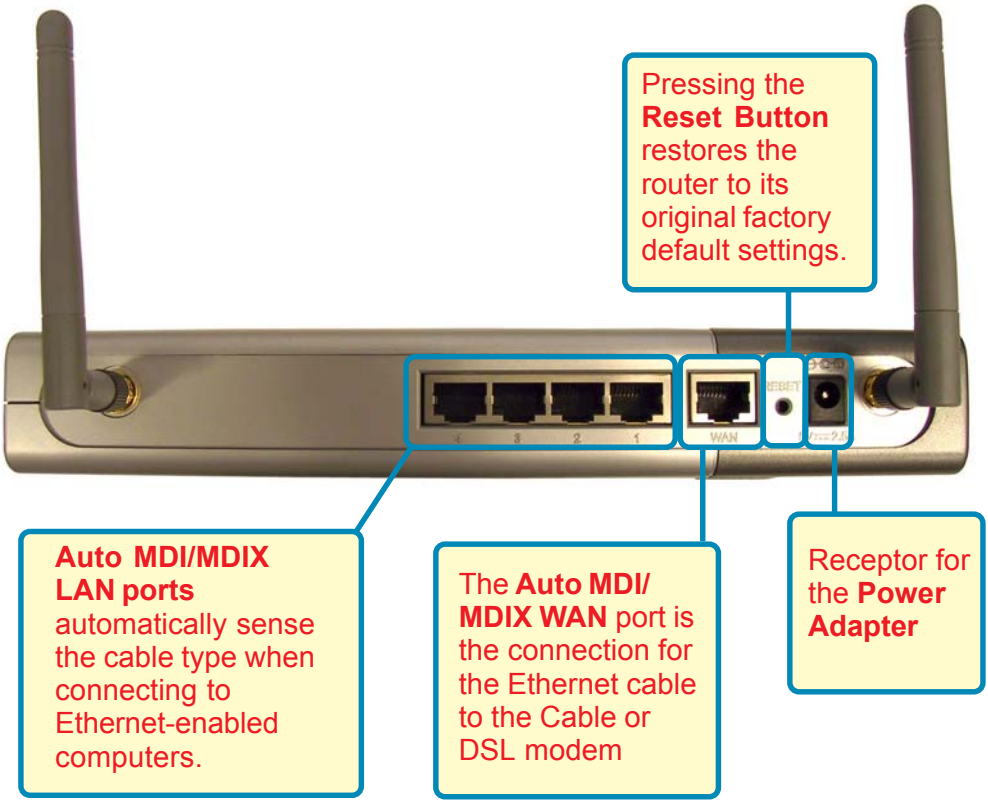
WPA*: A new security feature, **Wi-Fi Protected Access** authorizes and identifies users based on a secret key that changes automatically at a regular interval. **WPA** uses **TKIP** (**Temporal Key Integrity Protocol**) to change the temporal key every 10,000 packets (a packet is a kind of message transmitted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

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

For home users that will not incorporate a RADIUS server in their network, the security for the DI-624, 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-624 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-624, you will automatically receive a new key every time you connect, vastly increasing the safety of your communications.

**WPA will be available Spring 2003 as a free download*

Connections



LEDS

M1 LED -
A solid light indicates that the DI-624 is ready.

M2 LED -
A solid light indicates that the unit is defective.

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

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

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

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:
  - **TKIP** (Temporal Key Integrity Protocol), in conjunction with a RADIUS server, changes the temporal key every 10,000 packets, ensuring greater security
  - **Pre Shared Key** mode means that the home user, without a RADIUS server, will obtain a new security key every time the he or she connects to the network, vastly improving the safety of communications on the network.
- 802.1x **Authentication** in conjunction with the radius server verifies the identity of would be clients
- Utilizes **OFDM** technology (**O**rthogonal **F**requency **D**ivision **M**ultiplexing)
- User-friendly configuration and diagnostic utilities
- Operates in the 2.4GHz frequency range
- Connects multiple computers to a Broadband (Cable or DSL) modem to share the Internet connection
- Advanced Firewall features
  - Supports NAT with VPN pass-through, providing added security
  - MAC Filtering
  - IP Filtering
  - URL Filtering
  - Domain Blocking
  - Scheduling
- DHCP server supported enables all networked computers to automatically receive IP addresses
- Web-based interface for Managing and Configuring
- Access Control to manage users on the network
- Supports special applications that require multiple connections
- Equipped with 4 10/100 Ethernet ports, 1 WAN port, Auto MDI/MDIX

**WPA will be available Spring 2003 as a free download*

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 wherever a wireless network is available. 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 wireless local area network (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.

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

Wireless Basics *(continued)*

People use WLAN 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, both physically and logically, can benefit from a WLAN's 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 ways 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.

The DI-624 is compatible with the following wireless products:

- ***D-Link Air DWL-650***, ***D-Link Air*Plus *DWL-650+***,
  ***D-Link Air*Plus XtremeG DWL-G650**
  Wireless Cardbus Adapters used with laptop computers
- ***D-Link Air DWL-520*** *and* ***D-Link Air*Plus *DWL-520+*,**
  ***D-Link Air*Plus XtremeG DWL-G520**
  Wireless PCI cards used with desktop computers
- ***D-Link Air*Plus *DWL-900AP+ and DWL-2000AP+***
  Enhanced 2.4GHz Wireless Access Points
- ***D-Link Air*Plus *DWL-800AP+***
  Enhanced 2.4GHz Wireless Range Extender
- ***D-Link Air*Plus *DWL-810+***
  Enhanced 2.4GHz Ethernet-to-Wireless Bridge

Standards-Based Technology

The DI-624 Wireless Broadband Router utilizes the new **802.11g** standard.[1]

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

This means that in most environments, within the specified range of this device, you will be able to transfer large files quickly or even watch a movie in MPEG format over your network without noticeable delays. This technology works by transmitting high-speed digital data over a radio wave utilizing **OFDM** (**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 D-Link *DWL-G650* will automatically sense the best possible connection speed to ensure the greatest speed and range possible.

802.11g offers the most advanced network security features available today, including: *WPA*[2]*, 802.1x, TKIP, AES and Pre-Shared Key mode*. These security features are explained in more detail in the *Introduction* and the *Features* section of this manual.

The DI-624 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. Also based on the IEEE **802.11b** standard, the DI-624 is interoperable with existing compatible 2.4GHz wireless technology with data transfer speeds of up to 11Mbps.

1 *802.11g standard is scheduled for ratification by IEEE Q3 2003*

2 *WPA will be available Spring 2003 as a free download*

Installation Considerations

The D-Link *Air*Plus *X*treme*G* DI-624 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-624 and your receiving device (e.g., the DWL-G650 or the DWL-650+) to a minimum - each wall or ceiling can reduce your D-Link *Air*Plus Wireless product's range from 3-90 feet (1-30 meters.) Position your receiving devices so that the number of walls or ceilings is minimized.
2. Be aware of the direct line between routers and computers. 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 RF noise.

Getting Started

There are basically two modes of networking:

- **Infrastructure** – using an Access Point, or Wireless Router, such as the DI-624.

- **Ad-Hoc** – directly connecting to another computer, for peer-to-peer communication, using wireless network adapters on each computer, such as two or more DWL-G650 wireless network Cardbus adapters.

On the following pages we will show you an example of an **Infrastructure Network** and an **Ad-Hoc Network**.

An **Infrastructure** network contains an Access Point or a Wireless Router. The **Infrastructure Network** example shown on the following page contains the following D-Link network devices (your existing network may be comprised of other devices):

- A wireless Router - **D-Link *Air*Plus DI-624**

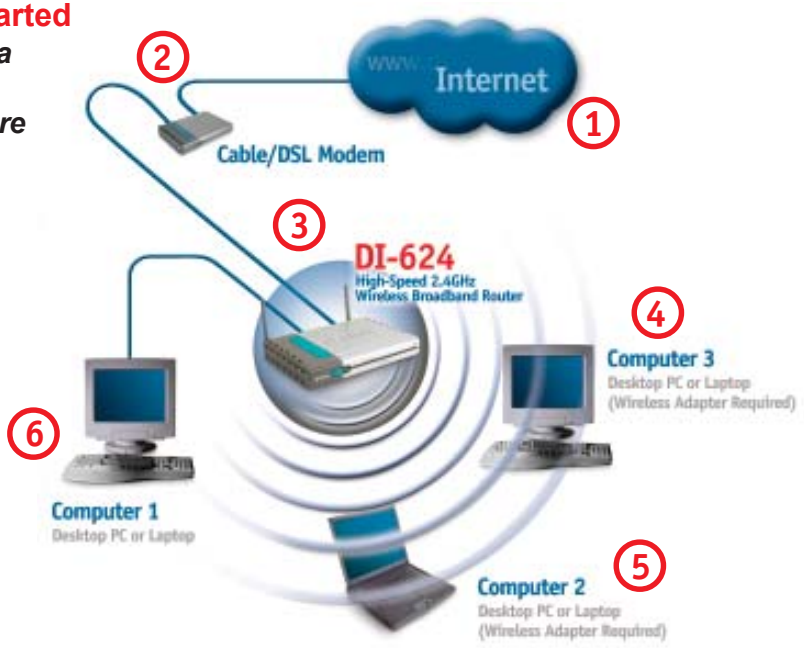
- A laptop computer with a wireless adapter - **D-Link *Air*Pro DWL-G650**

- A desktop computer with a wireless adapter - **D-Link *Air*Plus*XtremeG* DWL-G520, D-Link Air DWL-520,** or **D-Link AirPlus DWL-520+** (**D-Link *Air*** devices have speeds up to 11Mbps)

- A Cable modem - **D-Link DCM-200**

Getting Started

Setting up a Wireless Infrastructure Network



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

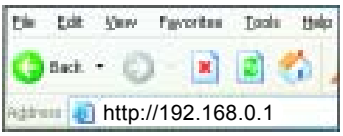
For a typical wireless setup at home (as shown above), please do the following:

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-624 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 *XtremeG* DWL-G520 wireless PCI adapter into an available PCI slot on your desktop computer. You may also install the DWL-520+, or the DWL-520. *(See the printed Quick Installation Guide included with the network adapter.)*
5. Install the drivers for the D-Link DWL-G650 wireless Cardbus adapter into a laptop computer. (*See the printed Quick Installation Guide included with the DWL-G650.*)
6. Install the drivers for the D-Link DFE-530TX wireless Cardbus adapter into a desktop computer. The four Ethernet LAN ports of the DI-624 are Auto MDI/MDIX and will work with both Straight-Through and Cross-Over cable. (*See the printed Quick Installation Guide included with the DFE-530TX.*)

Using the Configuration Menu

After you have completed the *Setup Wizard* (please see the *Quick Installation Guide* that came with the product) you can access the *Configuration* menu at any time by opening the web browser and typing in the IP Address of the DI-624. The DI-624 default IP Address is shown below:

- Open the web browser
- Type in the **IP Address** of the Router

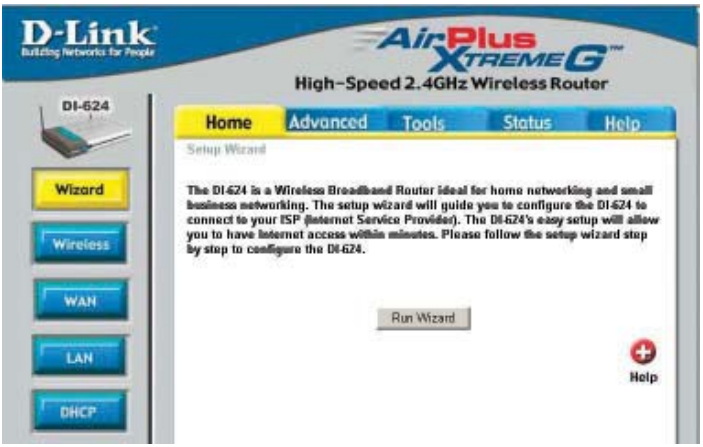


Note: if you have changed the default IP Address assigned to the DI-624, make sure to enter the correct IP Address.

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

Home > Wizard

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



Using the Configuration Menu

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.)*

WEP- Wired Equivalent Privacy (WEP) is a wireless security protocol for Wireless Local Area Networks (WLAN). WEP provides security by encrypting the data that is sent over the WLAN. Select **Enabled** or **Disabled. Disabled** is the default setting. *(Note: If you enable encryption on the DI-624 make sure to also enable encryption on all the wireless clients or wireless connection will not be established.)*

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

Key Type- Select **HEX** or **ASCII**

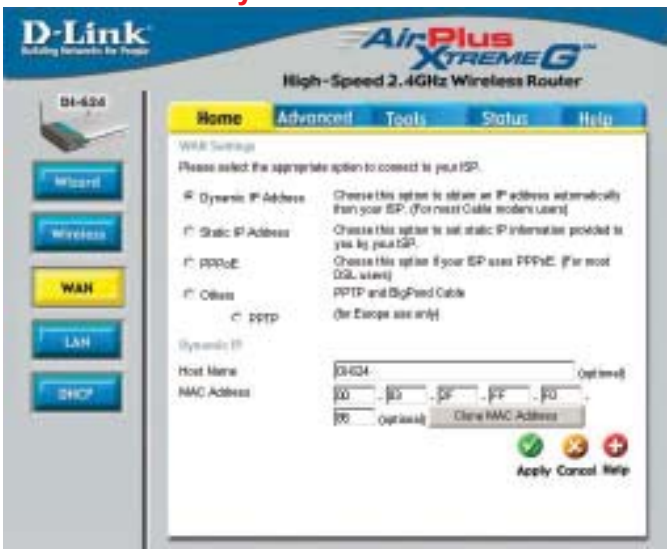
Passphrase- When you select Key Type: **ASCII**, you can enter a **Passphrase** for any or all of Keys 1-4

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

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

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

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

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

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

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- Input the public IP address of the ISP to which you are connecting

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

Secondary DNS Address- This is optional

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

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 PPPoeE 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.

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.

Primary DNS Address- Primary DNS IP address provided by our ISP

Secondary DNS Address- This option is only available for Static PPPoE. Enter the static IP Address for the PPPoE connection.

Maximum Idle Time- The amount of time of inactivity before disconnecting your PPPoE session. Enter a Maximum Idle Time (in minutes) to define a maximum period of time for which the Internet connection is maintained during inactivity. If the connection is inactive for longer than the defined Maximum Idle Time, then the connection will be dropped. Either set this to zero or enable Auto-reconnect to disable this feature.

(Continued on the next page)

Using the Configuration Menu

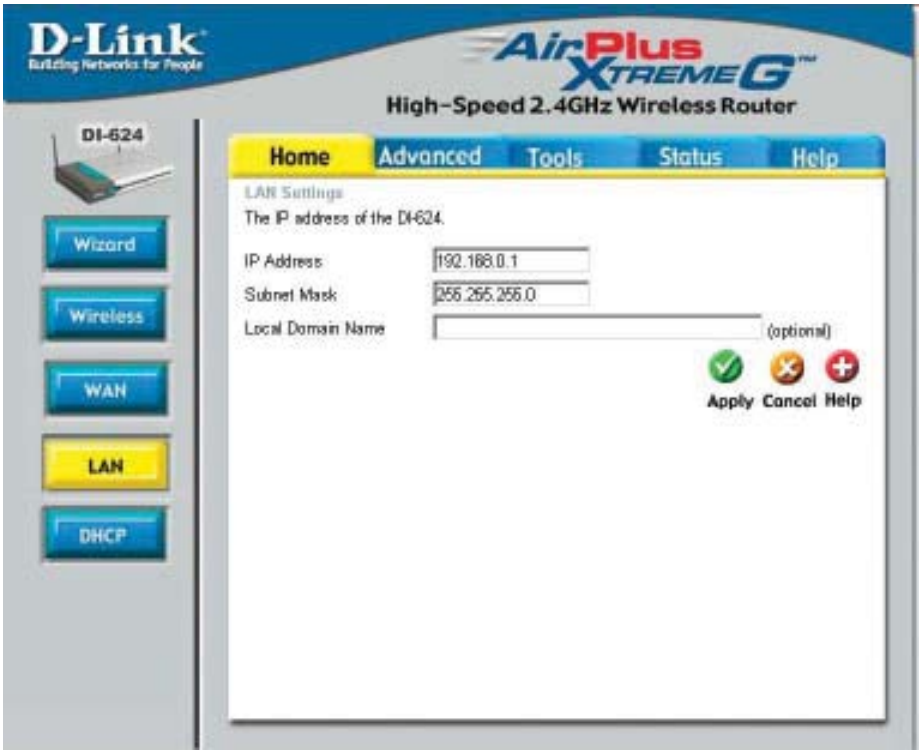
Home > WAN > PPPoE *continued*

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

Auto-reconnect- If enabled, the DI-754 will automatically connect to your ISP after your system is restarted or if the PPPoE connection is dropped.

Apply- Click **Apply** to save the changes.

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-624. 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.

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

Home > DHCP

DHCP stands for *Dynamic Host Control Protocol*. The DI-624 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-624. 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

Apply- click **Apply** to save the changes

Using the Configuration Menu

Advanced > Virtual Server

The DI-624 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-624 firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DI-624 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-624 redirects the external service request to the appropriate server within the LAN network.

Using the Configuration Menu
Advanced > Virtual Server *continued*

The DI-624 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.

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.

Apply- Click **Apply** to save the changes.

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

Using the Configuration Menu

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.

Using the Configuration Menu

Advanced > Applications

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-624. 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.

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

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.

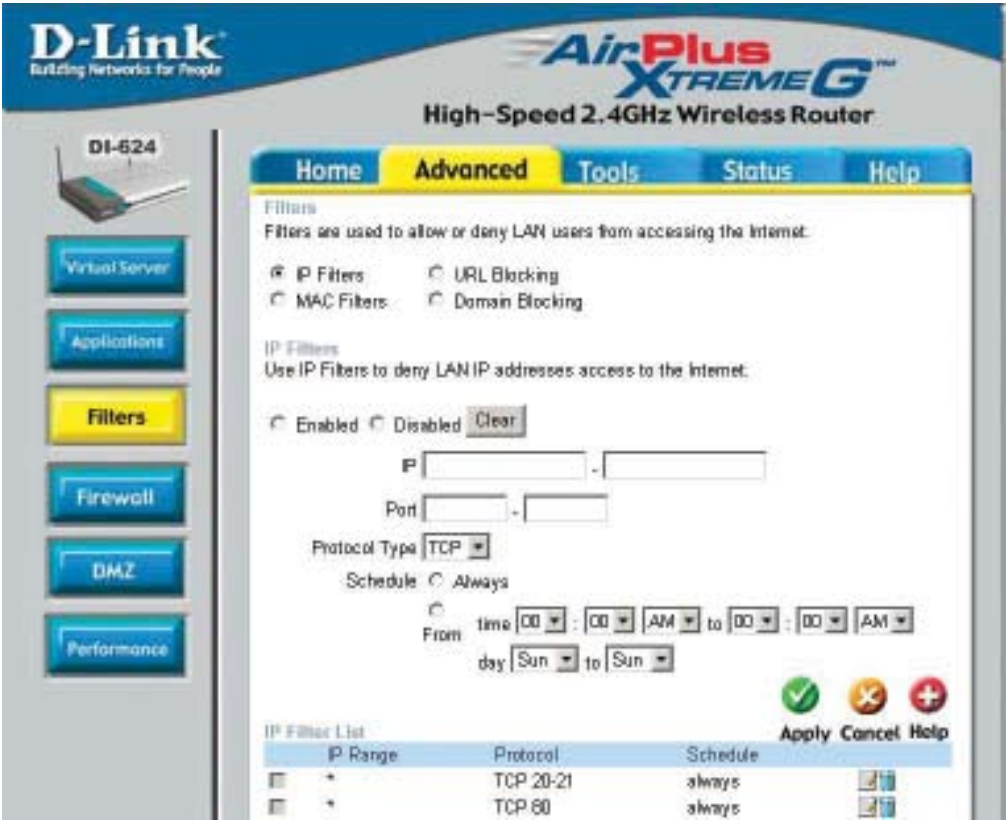
Public Port: This is the port number on the WAN side that will be used to access the application. You may define a single port or a range of ports. You can use a comma to add multiple ports or port ranges.

Public Type: This is the protocol used for the special application.

Apply: Click **Apply** to save the changes

Using the Configuration Menu

Advanced > Filters > IP Filters



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

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 will be denied access to the Internet.

Protocol Type: — Select the protocol type

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

Apply: — Click **Apply** to save changes.

Using the Configuration Menu

Advanced > Filters > URL Blocking

URL Blocking is used to deny LAN computers from accessing specific web sites by the URL. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display. To use this feature, enter the text string to be blocked and click **Apply.** The text to be blocked will appear in the list. To delete the text, just highlight it and click **Delete**.

Filters- Select the filter you wish to use; in this case, **URL Blocking** was chosen.

URL Blocking- Select **Enabled** or **Disabled**.

Keywords- Block URLs which contain keywords listed below. Enter the keywords in this space.

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

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

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

Advanced > Filters > Domain Blocking

Domain Blocking is used to allow or deny LAN (Local Area Network) computers from accessing specific domains on the Internet. Domain blocking will deny all requests to a specific domain such as http and ftp. It can also allow computers to access specific sites and deny all other sites.

Filters- Select the filter you wish to use; in this case, **Domain Blocking** was chosen.

Domain Blocking:

Disabled- Select **Disabled** to disable **Domain Blocking**

Allow- Allows users to access all domains except **Blocked Domains**

Deny- Denies users access to all domains except **Permitted Domains**

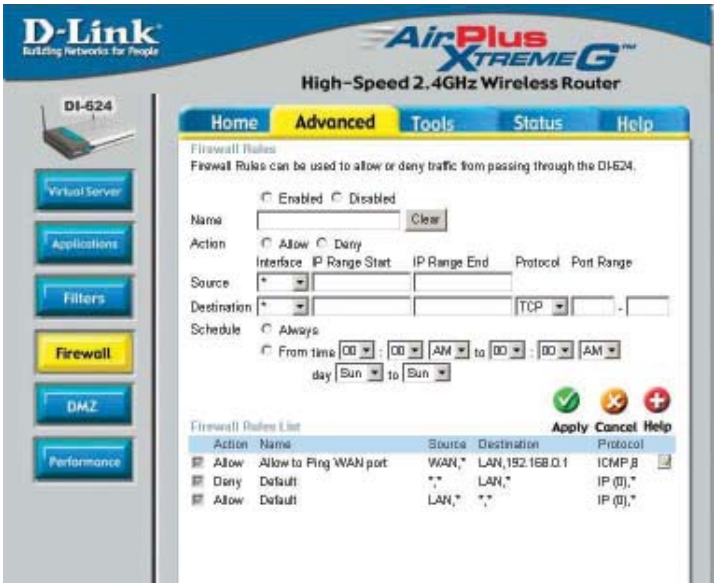
Permitted Domains- Enter the **Permitted Domains** in this field

Blocked Domains- Enter the **Blocked Domains** in this field

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

Advanced > Firewall



Firewall Rules is an advanced feature used to deny or allow traffic from passing through the DI-624. It works in the same way as IP Filters with additional settings. You can create more detailed access rules for the DI-624. 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.)

Note: The DI-624 MAC Address filtering rules have precedence over the Firewall Rules.

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**.

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

Advanced > DMZ

If you have a client PC that cannot run Internet applications properly from behind the DI-624, 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.

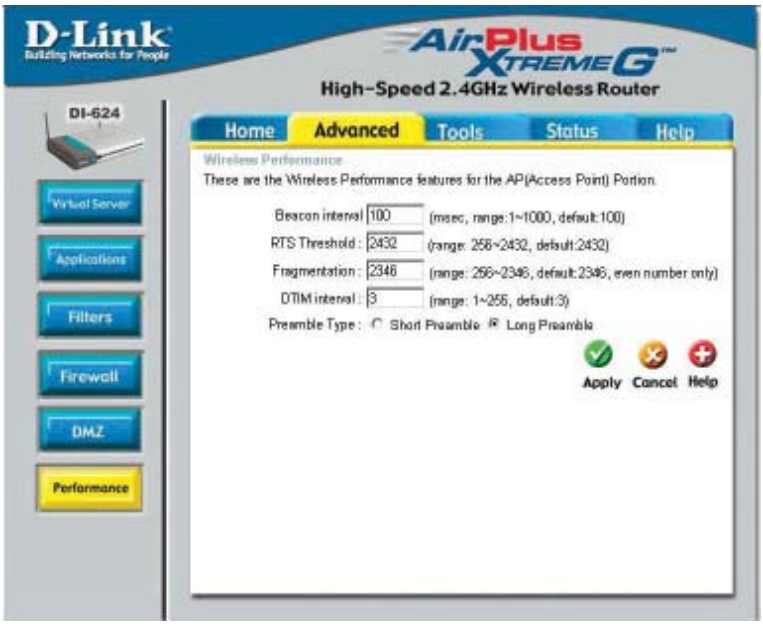
DMZ- **Enable** or **Disable** the DMZ. The DMZ (Demilitarized Zone) allows a single computer to be exposed to the internet. By **default** the DMZ is **disabled**.

IP Address- Enter the **IP Address** of the computer to be in the **DMZ**

Apply- Click **Apply** to save the changes.

Using the Configuration Menu

Advanced > Performance



Wireless Performance-

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

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.

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. **Auto** is the default setting. *Note: High network traffic areas should use the shorter preamble type.*

Apply- Click **Apply** to save changes

Using the Configuration Menu

Tools> Admin

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

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

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

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.

Apply- Click **Apply** to save the changes

Using the Configuration Menu

Tools > Time

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

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

Set the Time- To manually input the time, enter the values in these fields for the Year, Month, Day, Hour, Minute, and Second. Click **Set Time**.

Daylight Saving- To select Daylight Saving time manually, select **enabled** or **disabled,** and enter a start date and an end date for daylight saving time.

Apply- Click **Apply** to save the changes.

Using the Configuration 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.**

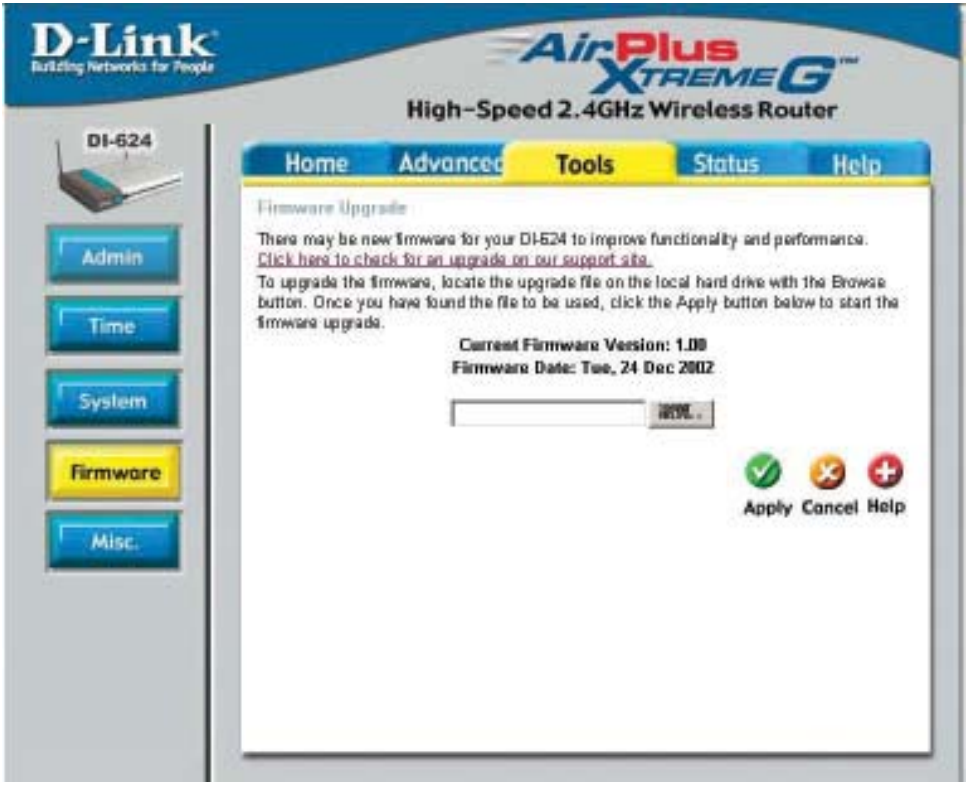
Save Settings to Local Hard Drive- Click **Save** to save the current settings to the local Hard Drive

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

Using the Configuration Menu

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.

Using the Configuration Menu

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-624

Block WAN Ping-

If you choose to block WAN Ping, the WAN IP Address of the DI-624 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 cooperate in the Plug and Play forum.

Gaming Mode-

Gaming mode allows a form of pass-through for certain Internet Games. If you are using XBOX, Playstation2 or a PC, make sure you are using the latest firmware and Gaming Mode is enabled. To utilize Gaming Mode, click **Enabled.** If you are not using a Gaming application, it is recommended that you **Disable** Gaming Mode.

Dynamic DNS-

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.

VPN Pass Through- The DI-624 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-624. This is useful when you have many VPN clients on the LAN network.

PPTP- select **Enabled** or **Disabled**

IPSec- select **Enabled** or **Disabled**

Apply- Click **Apply** to save changes

Using the Configuration Menu

Status > Device Info

This page displays the current information for the DI-624. It will display the LAN, WAN and MAC address 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-624's working status:

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
WAN Status: WAN Connection Status

LAN

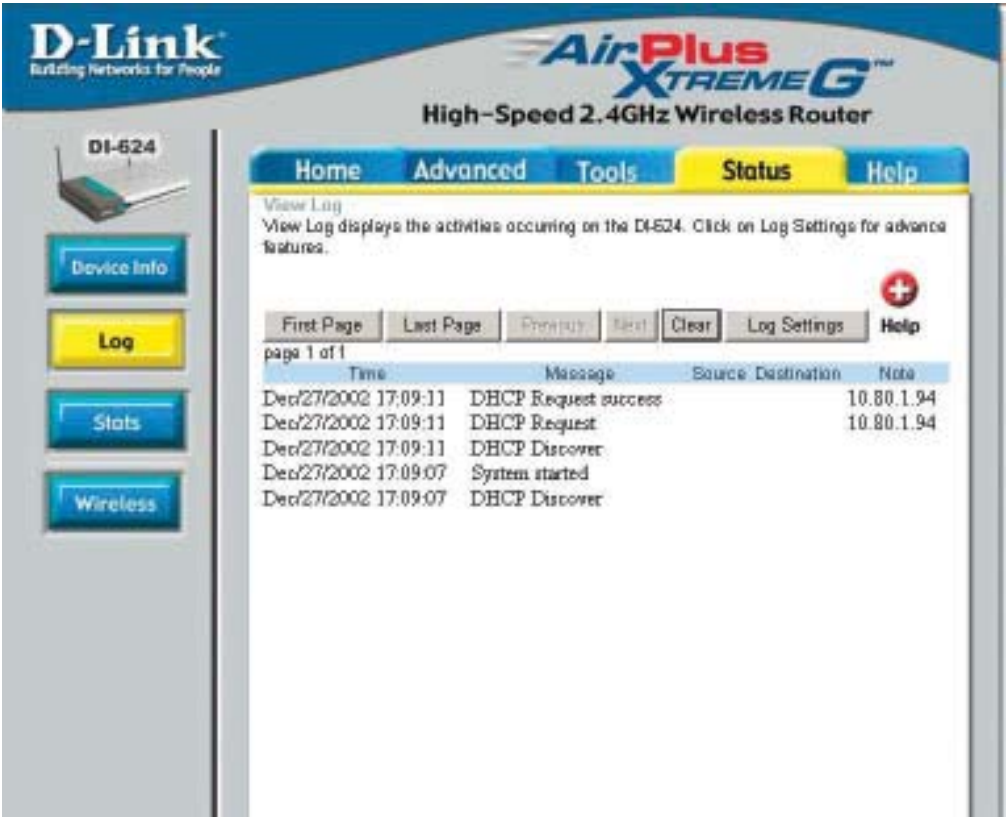
IP Address: LAN/Private IP Address of the DI-624
Subnet Mask: LAN/Private Subnet Mask of the DI-624

Wireless

MAC Address: Displays the MAC address
SSID: Displays the current SSID
Channel: Displays the current channel
WEP: indicates whether WEP is enabled or disabled

Using the Configuration Menu

Status > Log



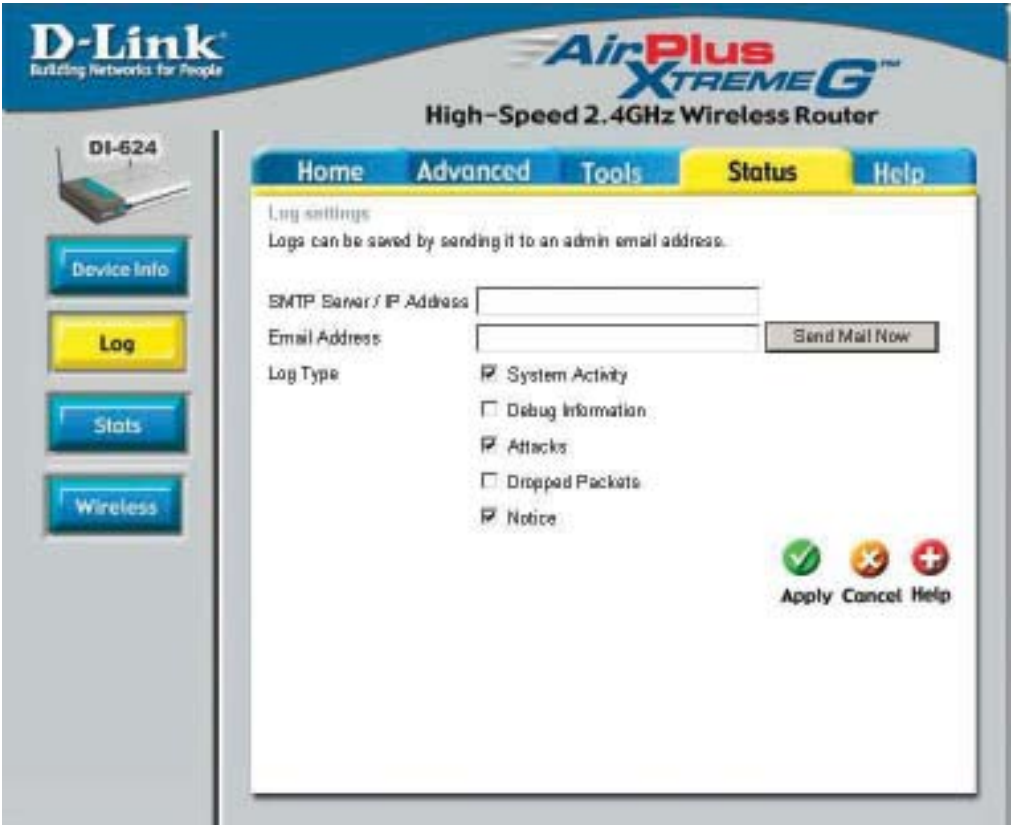
The Broadband Router keeps a running log of events and activities occurring on the Router. If the device is rebooted, the logs are automatically cleared. You may save the log files under Log Settings.

View Log-

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

Using the Configuration Menu

Status > Log > Log Settings



Log Settings-

Not only does the Broadband Router display the logs of activities and events, it can setup to send these logs to another location.

SMTP Server/IP Address - The address of the SMTP server that will be used to send the logs

Email Address - The email address to which the logs will be sent.
Click on **Send Mail Now** to send the email.

Click **Apply** to save the changes.

Using the Configuration Menu

Status > Stats

The screen above displays theTraffic Statistics. Here you can view the amount of packets that pass through the DI-624 on both the WAN and the LAN ports. 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 connection time and MAC address of the connected wireless client.

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