D-Link®
Building Networks for People

Manual

Version 1.0

DI-624M

Super G™ MIMO Wireless Router

Table of Contents

Package Contents

- D-Link DI-624M Super G MIMO Wireless Router
- CAT-5 Ethernet Cable (All the DI-624M's Ethernet ports are Auto-MDIX)
- Power Adapter (5.0V, 2.5A)
- Vertical Stands
- Mounting Kit
- CD-ROM with Software and Manual
- Quick Installation Guide

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

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

Minimum System Requirements

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

Introduction

The D-Link DI-624M Super G MIMO Wireless 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-624M provides data transfers at up to 108 Mbps* (compared to the standard 54 Mbps) when used with other D-Link Super G MIMO 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-624M has the newest, strongest, most advanced security features available today. When used with other 802.11g WPA (WiFi Protected Access) compatible products in a network, the security features include:

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

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

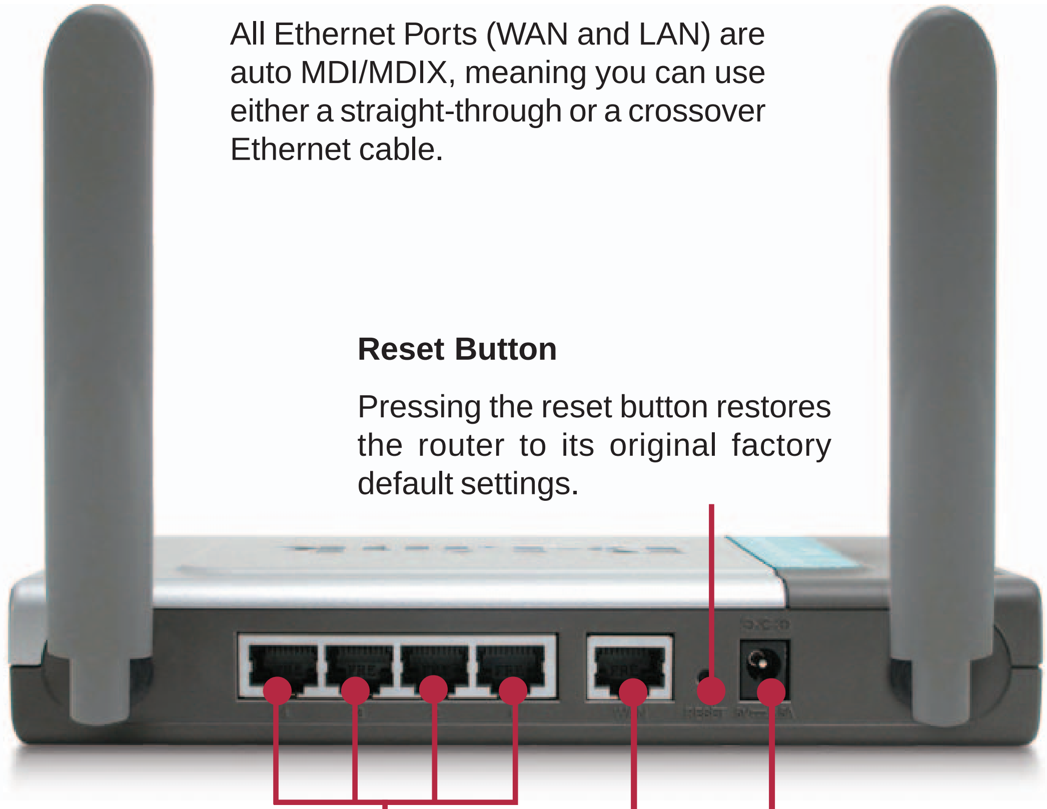
Features and Benefits

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

  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 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, and Scheduling
- DHCP server enables all networked computers to automatically receive IP addresses
- Web-based interface for Managing and Configuring
- Access Control to manage users on the network
- Supports special applications that require multiple connections
- Equipped with 4 10/100 Ethernet ports, 1 WAN port, Auto MDI/MDIX

Hardware Overview

Connections



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

Reset Button

Pressing the reset button restores the router to its original factory default settings.

Auto MDI/MDIX LAN Ports

These ports automatically sense the cable type when connecting to Ethernet-enabled computers.

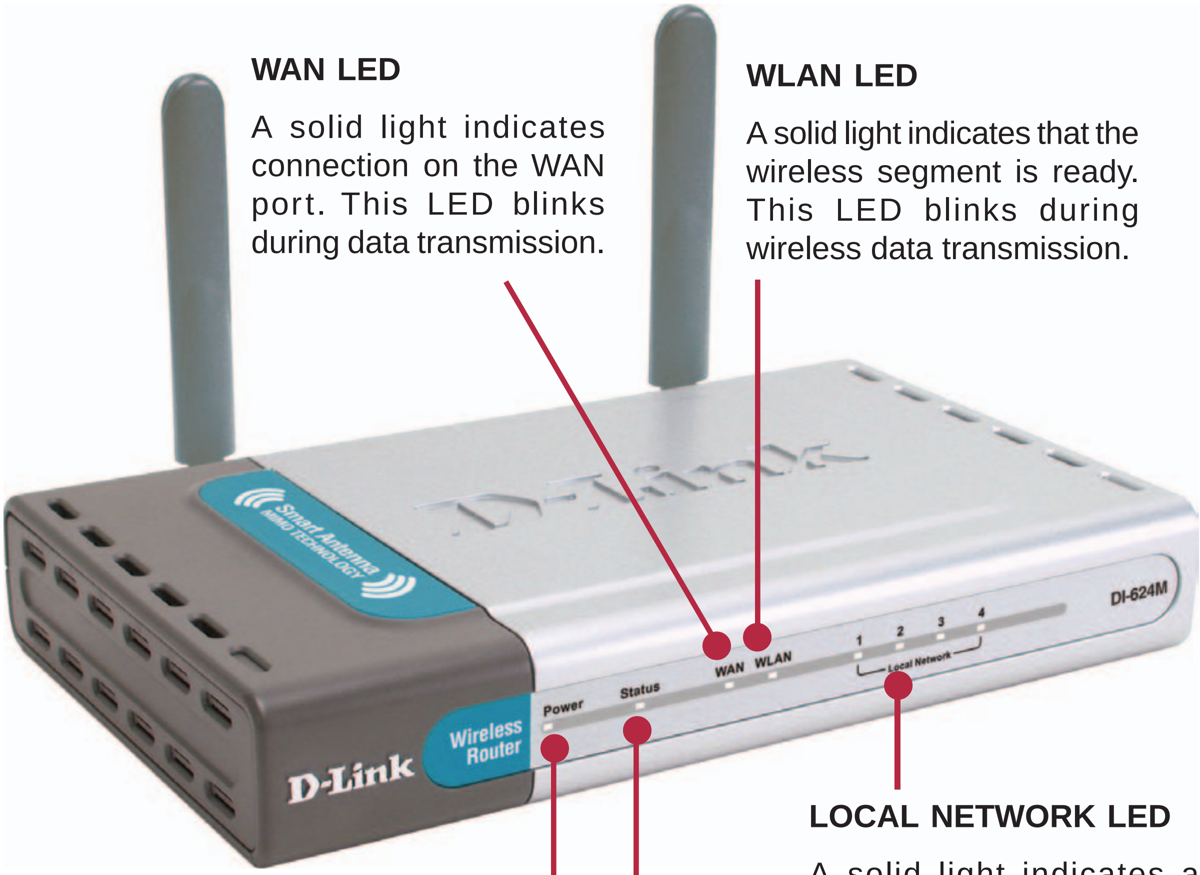
DC Power Connector

The DC power input connector is labeled **DC 5V** with a single jack socket to supply power to the DI-624M.

Auto MDI/MDIX WAN Port

This is the connection for the Ethernet cable to the Cable or DSL modem

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.

LOCAL NETWORK LED

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

POWER LED

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

STATUS

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

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-624M Super G MIMO Wireless Router utilizes the **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-624M 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 DI-624MSuper G MIMO Wireless Router 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-624M 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.

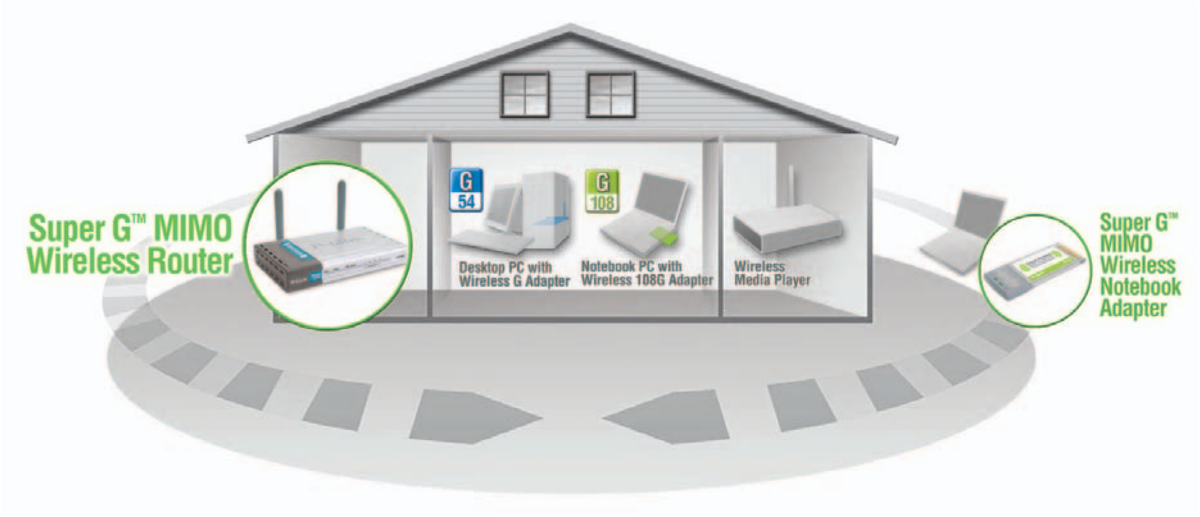
2 Be aware of the direct line between network devices. A wall that is 1.5 feet thick (.5 meters), at a 45-degree angle appears to be almost 3 feet (1 meter) thick. At a 2-degree angle it looks over 42 feet (14 meters) thick! Position devices so that the signal will travel straight through a wall or ceiling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


Super G™ MIMO Wireless Router
G 54
G 108
Desktop PC with Wireless G Adapter
Notebook PC with Wireless 108G Adapter
Wireless Media Player
Super G™ MIMO Wireless Notebook Adapter

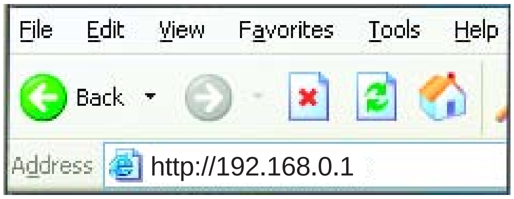
Please remember that **D-Link Super G MIMO** *wireless devices are pre-configured to connect together, right out of the box, with their default settings.*

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-624M 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. 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 D-Link DWL-G650M wireless Cardbus adapter into a laptop computer. (*See the printed Quick Installation Guide included with the DWL-G650M.*)
6. Install the D-Link DFE-530TX+ adapter into a desktop computer. The four Ethernet LAN ports of the DI-624M 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+.*)

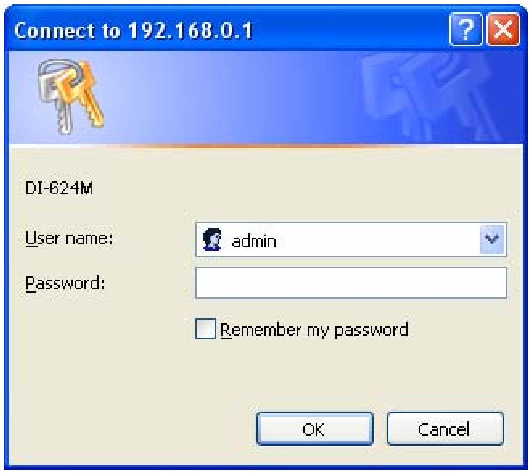
Using the Configuration Menu

Whenever you want to configure your DI-624M, you can access the Configuration Menu by opening the Web-browser and typing in the IP Address of the DI-624M. The DI-624M's default IP Address is shown below:



Address http://192.168.0.1

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



Connect to 192.168.0.1

DI-624M

User name: admin

Password:

□ Remember my password

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

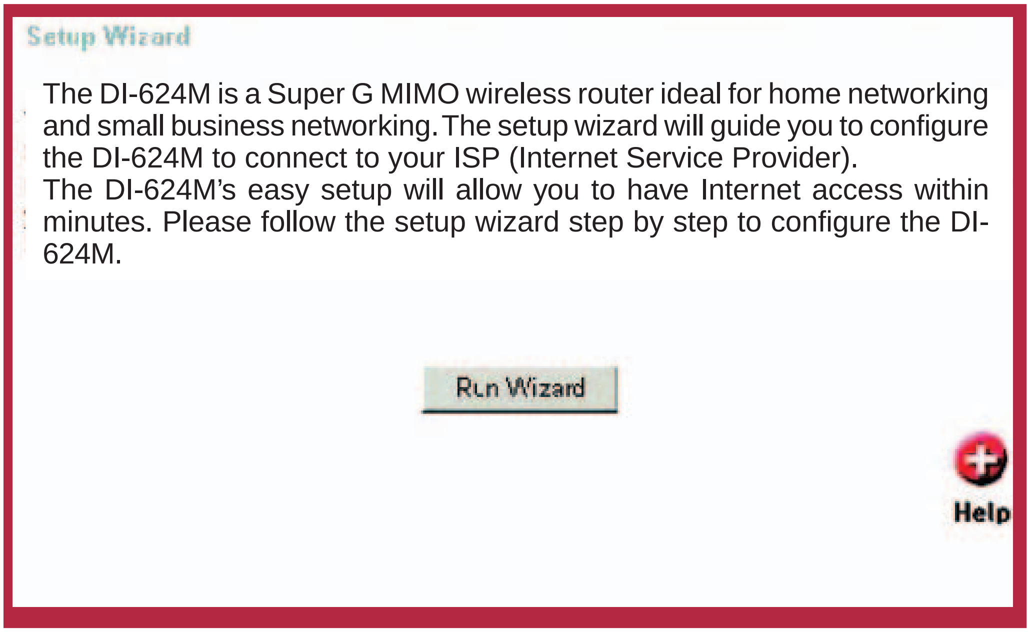
- Type **admin** in the **User Name** field.
- Leave the **Password** blank.
- Click OK.

Home

The Advanced tab provides the following configuration options: Wizard, Wireless, WAN, LAN, and DHCP.

Wizard

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



Setup Wizard

The DI-624M is a Super G MIMO wireless router ideal for home networking and small business networking. The setup wizard will guide you to configure the DI-624M to connect to your ISP (Internet Service Provider).
The DI-624M's easy setup will allow you to have Internet access within minutes. Please follow the setup wizard step by step to configure the DI-624M.

Home > 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.

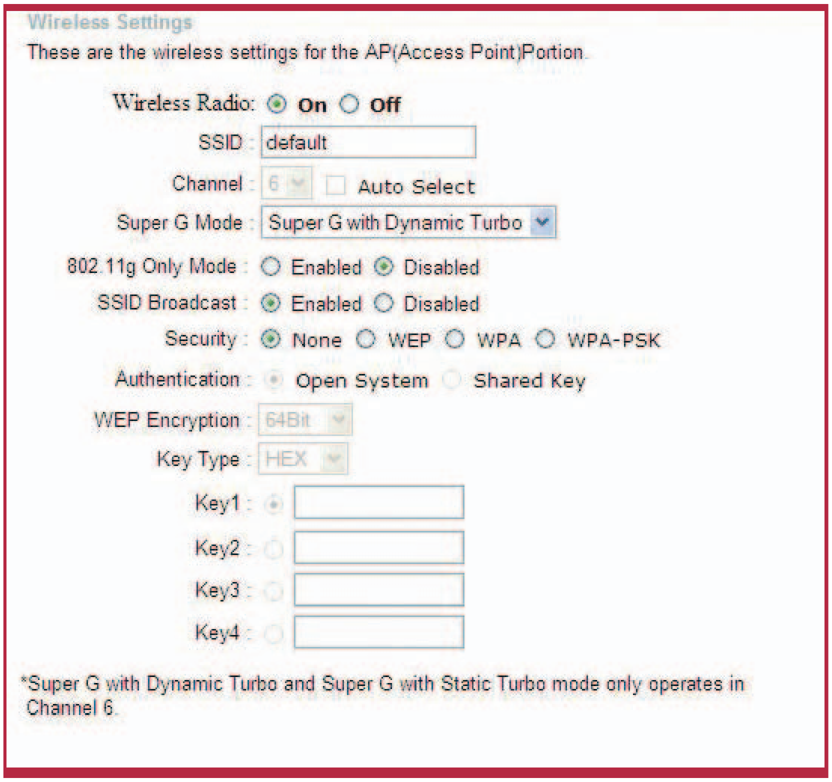
✓ **Apply** — Clicking **Apply** will save changes made to the page

✗ **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.)

Wireless



Wireless Settings

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

Wireless Radio: ● On ○ Off

SSID : default

Channel : 6 □ Auto Select

Super G Mode : Super G with Dynamic Turbo

802.11g Only Mode : ○ Enabled ● Disabled

SSID Broadcast : ● Enabled ○ Disabled

Security : ● None ○ WEP ○ WPA ○ WPA-PSK

Authentication : ● Open System ○ Shared Key

WEP Encryption : 64Bit

Key Type : HEX

Key1 : ●

Key2 : ○

Key3 : ○

Key4 : ○

*Super G with Dynamic Turbo and Super G with Static Turbo mode only operates in Channel 6.

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.)

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 backwarsd 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, Super G with Dynamic Turbo, or Super G with Static 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 Static 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 is Super G with Dynamic Turbo enabled.

Super G with DynamicTurbo:: Capable of Packet Bursting, FastFrames, Compression, and Static Turbo. This setting is not backwards compatible with non-Turbo (legacy) devices. Static turbo mode is always on and is only enabled when all nodes on the wireless network is Super G with Static Turbo enabled.

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

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.

Security: Select **None**, **WEP**, **WPA**, or **WPA-PSK** encryption.

Authentication: Select **Open System** or **Shared Key** authentication.

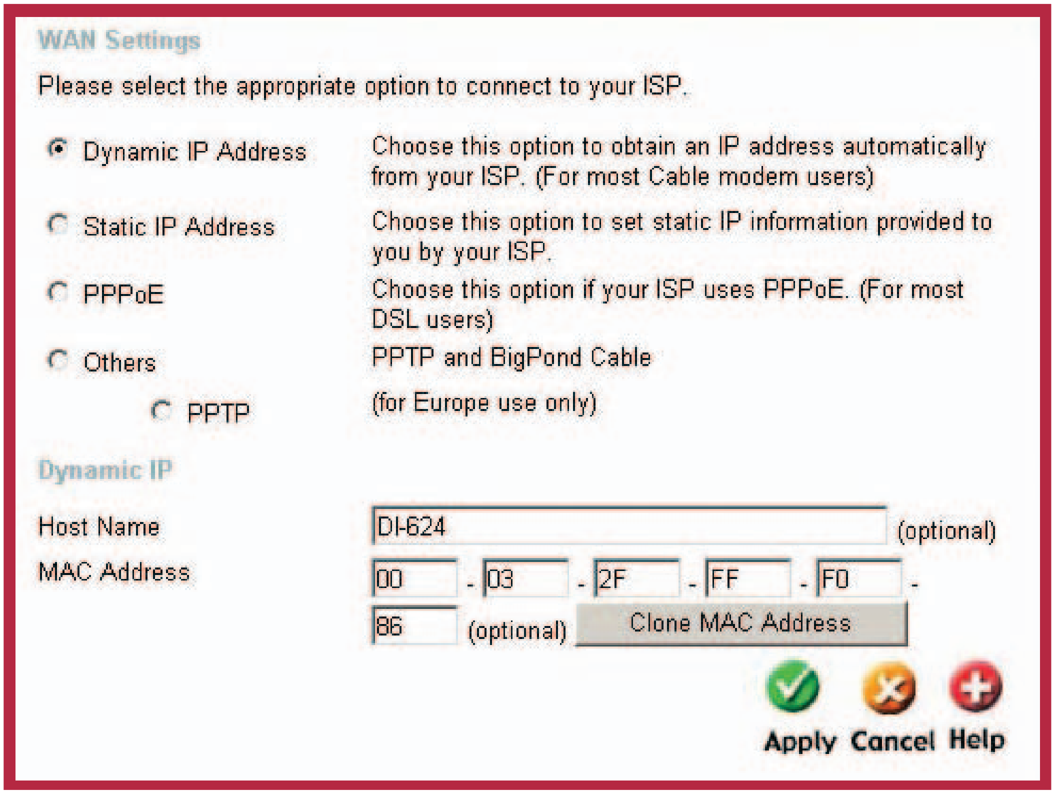
WEP Encryption: Wired Equivalent Privacy (WEP) is a wireless security protocol for Wireless Local Area Networks (WLAN). WEP provides security by encrypting the data that is sent over the WLAN. Select **Enabled** or **Disabled**. **Disabled** is the default setting. (Note: If you enable encryption on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

WAN

Dynamic IP Address



WAN Settings

Please select the appropriate option to connect to your ISP.

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

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

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

○ Others — PPTP and BigPond Cable

○ PPTP — (for Europe use only)

Dynamic IP

Host Name: DI-624 (optional)

MAC Address: 00 - 03 - 2F - FF - F0 - 86 (optional)

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.

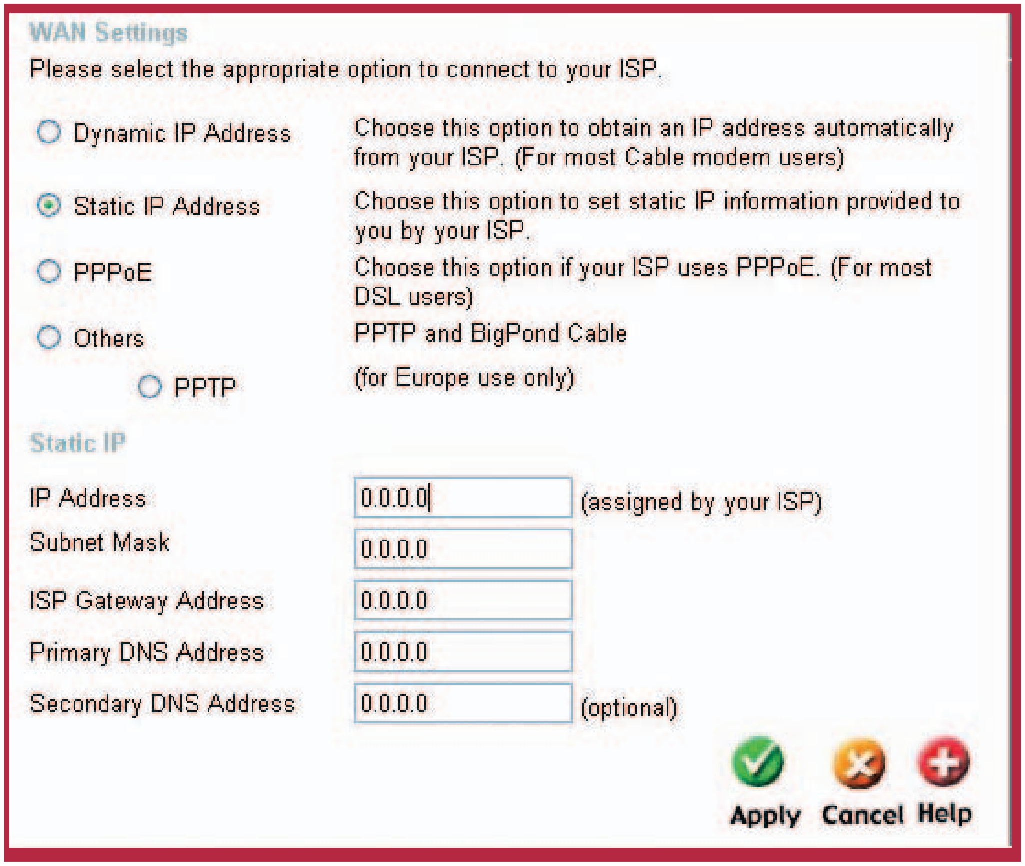
MAC Address: The default MAC Address is set to the WAN's physical interface MAC address on the Broadband Router. It is not recommended that you change the default MAC address unless required by your ISP.

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.

Primary/Secondary DNS Address: Enter a DNS Address if you do not wish to use the one provided by your ISP.

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

Static IP Address



WAN Settings

Please select the appropriate option to connect to your ISP.

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

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

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

○ Others — PPTP and BigPond Cable

○ PPTP — (for Europe use only)

Static IP

IP Address	0.0.0.0	(assigned by your ISP)
Subnet Mask	0.0.0.0	
ISP Gateway Address	0.0.0.0	
Primary DNS Address	0.0.0.0	
Secondary DNS Address	0.0.0.0	(optional)

Home > WAN > 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.)

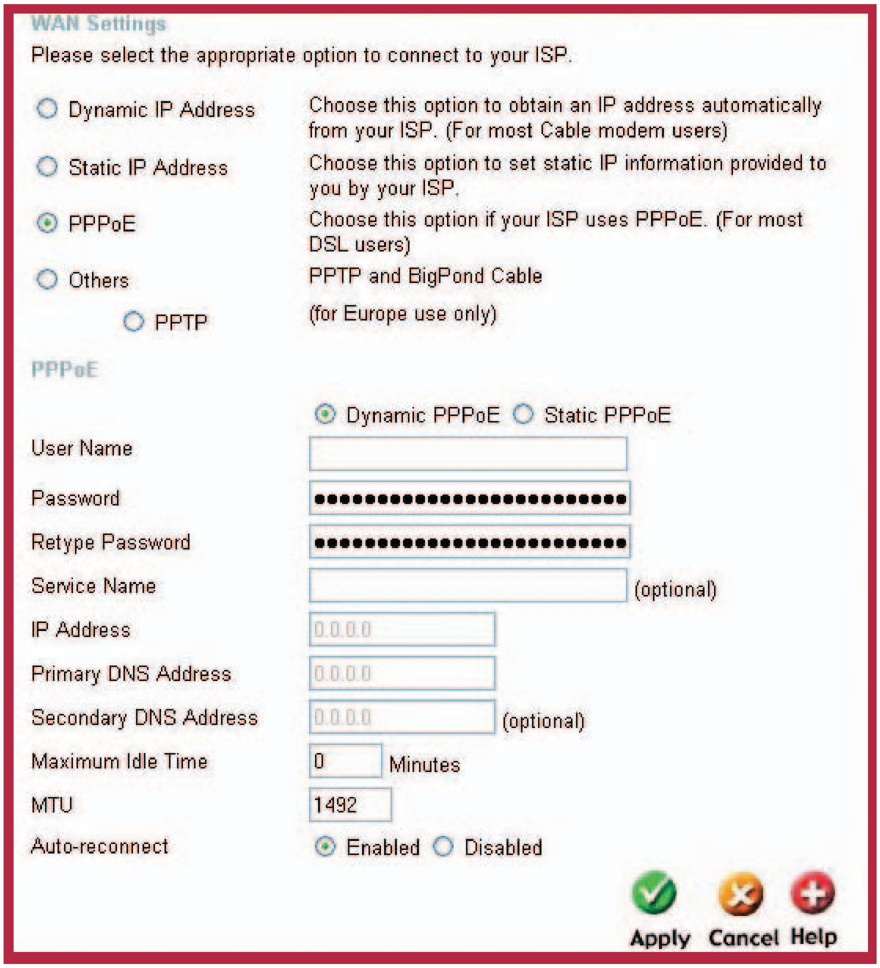
ISP Gateway Address: Input the public IP address of the ISP to which you are connecting.

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

Secondary DNS Address: This is optional.

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

PPPoE



WAN Settings

Please select the appropriate option to connect to your ISP.

○ Dynamic IP Address	Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)
○ Static IP Address	Choose this option to set static IP information provided to you by your ISP.
● PPPoE	Choose this option if your ISP uses PPPoE. (For most DSL users)
○ Others	PPTP and BigPond Cable
○ PPTP	(for Europe use only)

PPPoE

	● Dynamic PPPoE ○ Static PPPoE
User Name	
Password	••••••••••••••••••••••••••
Retype Password	••••••••••••••••••••••••••
Service Name	(optional)
IP Address	0.0.0.0
Primary DNS Address	0.0.0.0
Secondary DNS Address	0.0.0.0 (optional)
Maximum Idle Time	0 Minutes
MTU	1492
Auto-reconnect	● Enabled ○ Disabled

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.

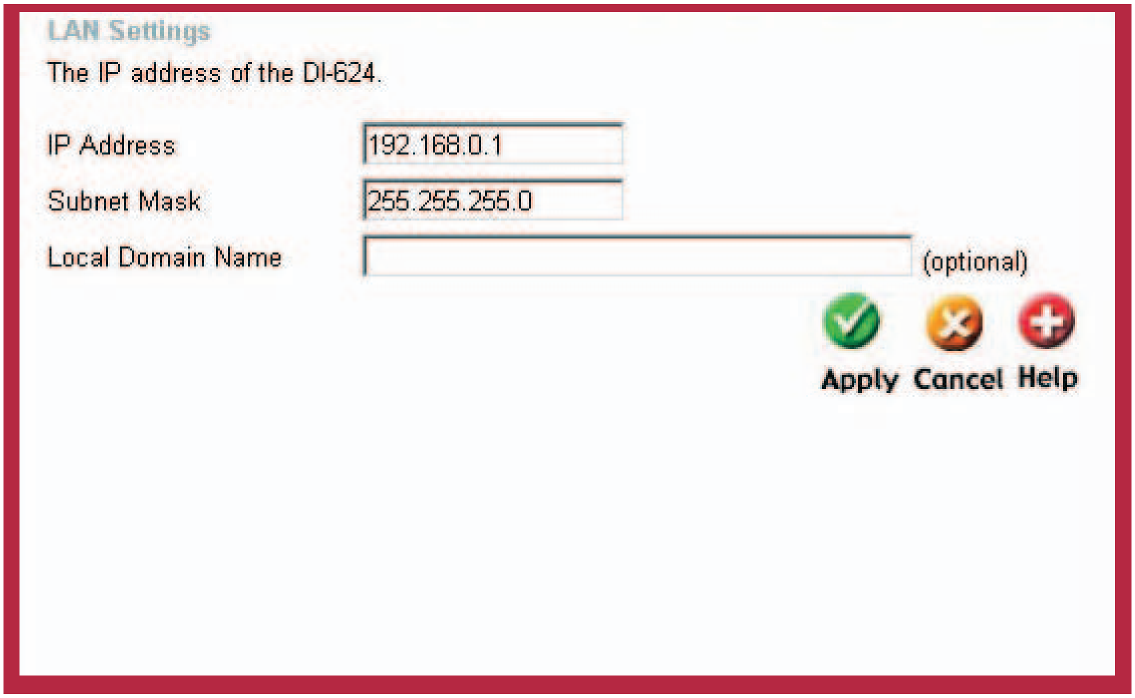
Primary DNS Address: Primary DNS IP address provided by our ISP.

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

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-624M will automatically connect to your ISP after your system is restarted or if the PPPoE connection is dropped.

LAN



LAN Settings

The IP address of the DI-624.

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Local Domain Name: (optional)

Home > LAN

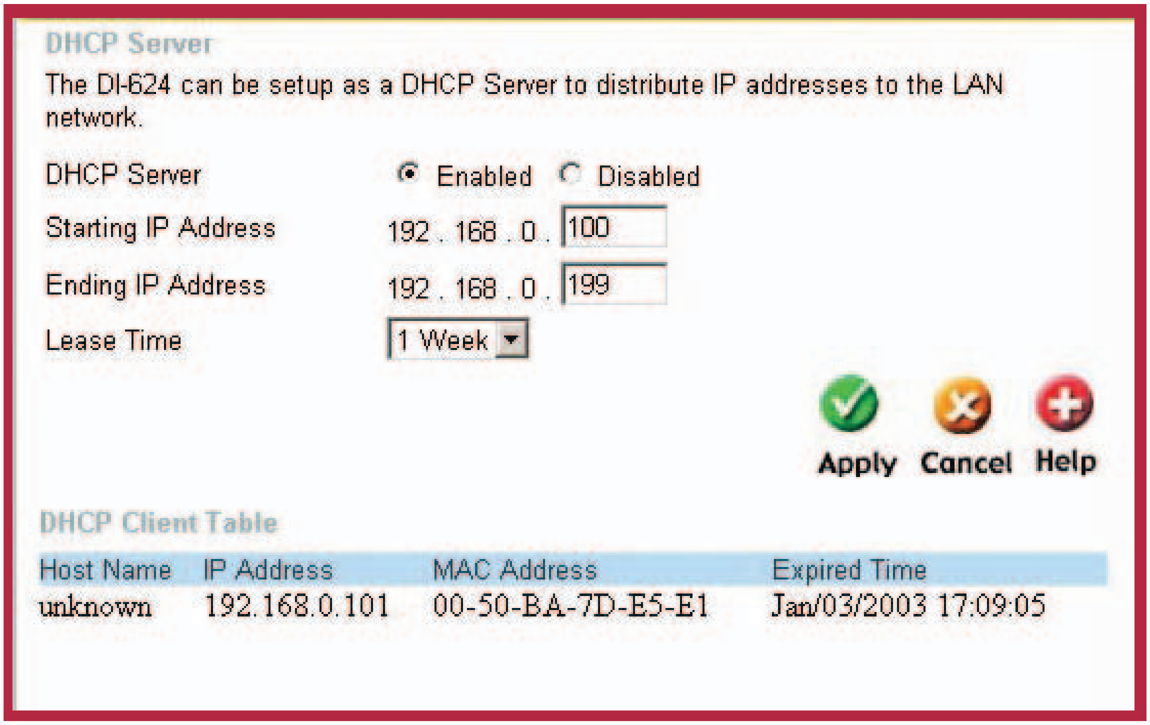
LAN is short for Local Area Networ... This is considered your internal network. These are the IP settings of the LAN interface for the DI-624M. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and 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.

DHCP



DHCP Server

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

DHCP Server	● Enabled ○ Disabled
Starting IP Address	192 . 168 . 0 . 100
Ending IP Address	192 . 168 . 0 . 199
Lease Time	1 Week

DHCP Client Table

Host Name	IP Address	MAC Address	Expired Time
unknown	192.168.0.101	00-50-BA-7D-E5-E1	Jan/03/2003 17:09:05

Home > DHCP

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

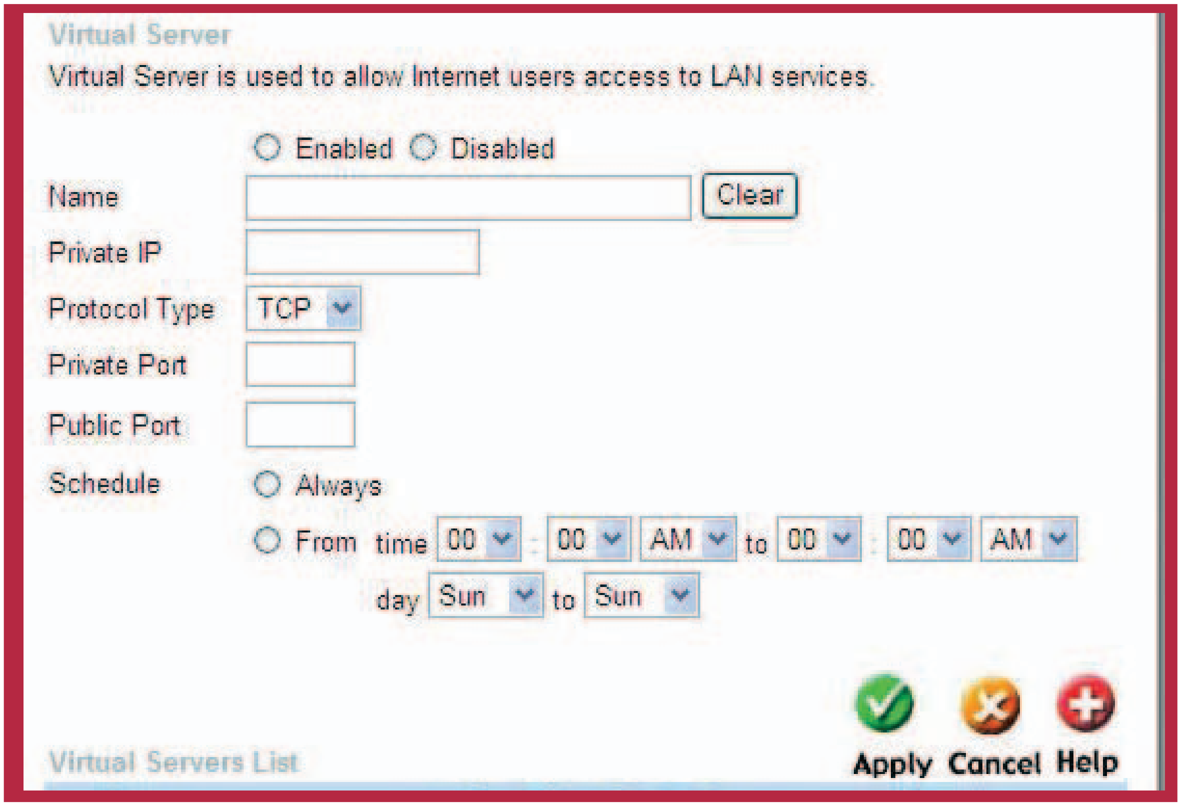
Ending IP Address: The ending IP address for the DHCP server's IP assignment.

Lease Time: The length of time for the IP lease. Enter the Lease time. The default setting is one hour.

Advanced

The Advanced tab provides the following configuration options: Virtual Server, Applications, Filters, Parental Control, Firewall, DMZ, and Performance.

Virtual Server



Virtual Server

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

Advanced > Virtual Server

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

The DI-624M 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.

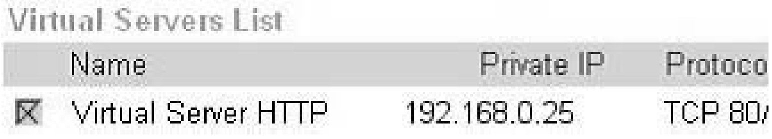
Private Port: The port number of the service used by the Private IP computer.

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.

Example #1: If you have a Web server that you wanted Internet users to access at all t , you would need to enable it. Web (HTTP) server is on L ocal Area Network) computer 192.168.0.25. HTTP uses po , TCP.

Name: Web Server
Private IP: 192.168.0.25
Protocol Type: TCP
Private Port: 80
Public Port: 80
Schedule: always



Virtual Servers List

	Name	Private IP	Protoco
☒	Virtual Server HTTP	192.168.0.25	TCP 80/

Click on this icon to edit the virtual service.

Click on this icon to delete the virtual service.

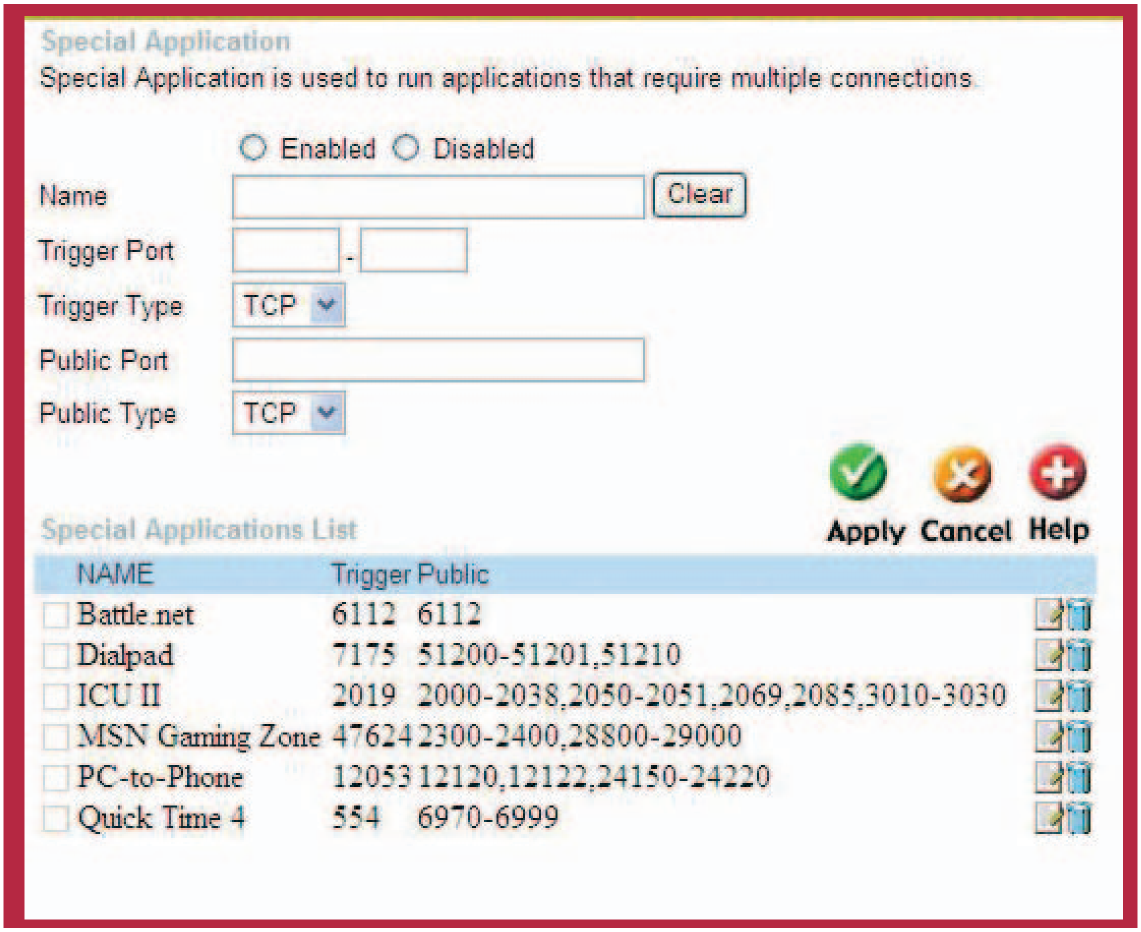
Example #2:

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.

Applications



Special Application

Special Application is used to run applications that require multiple connections

○ Enabled ○ Disabled

Name	
Trigger Port	-
Trigger Type	TCP
Public Port	
Public Type	TCP

Special Applications List

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

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-624M. 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-624M 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.

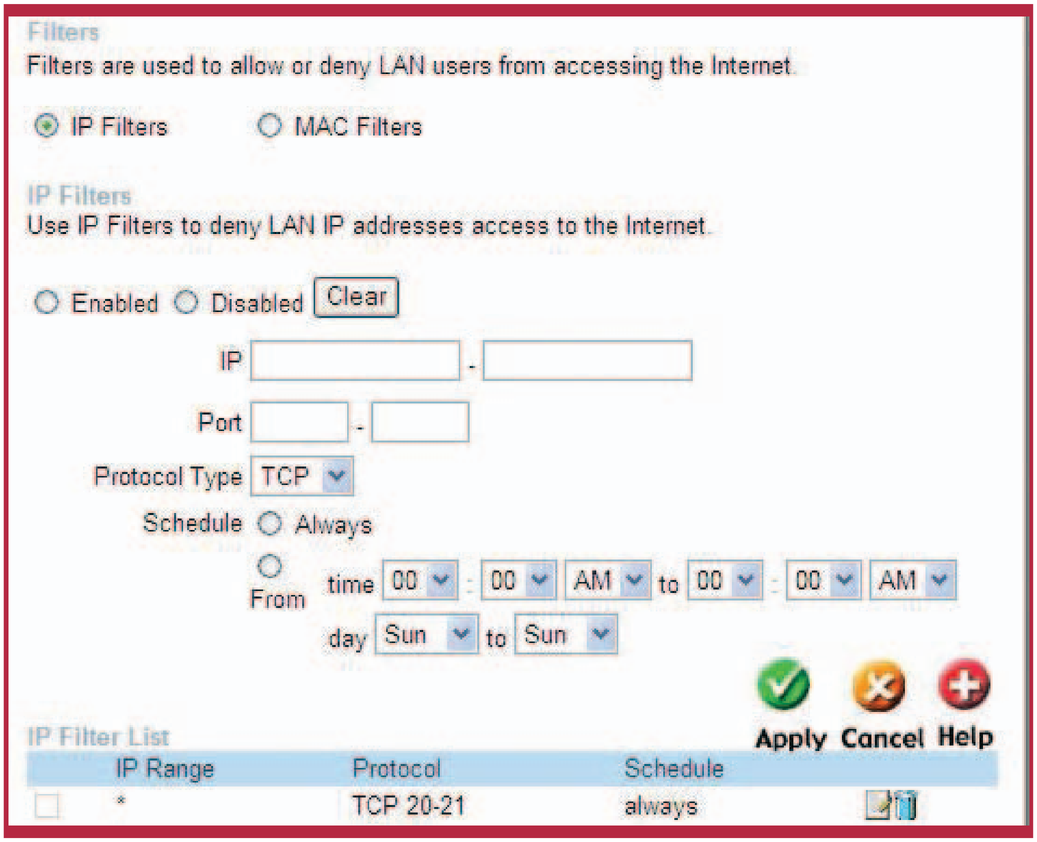
Trigger Type: This is the protocol used to trigger the special application.

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 to trigger the special application.

Filters

IP Filters



Filters

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

● IP Filters ○ MAC Filters

IP Filters

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

○ Enabled ○ Disabled

IP -

Port -

Protocol Type TCP

Schedule ○ Always

○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

IP Filter List

	IP Range	Protocol	Schedule
□	*	TCP 20-21	always

Advanced > Filters > IP Filters

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

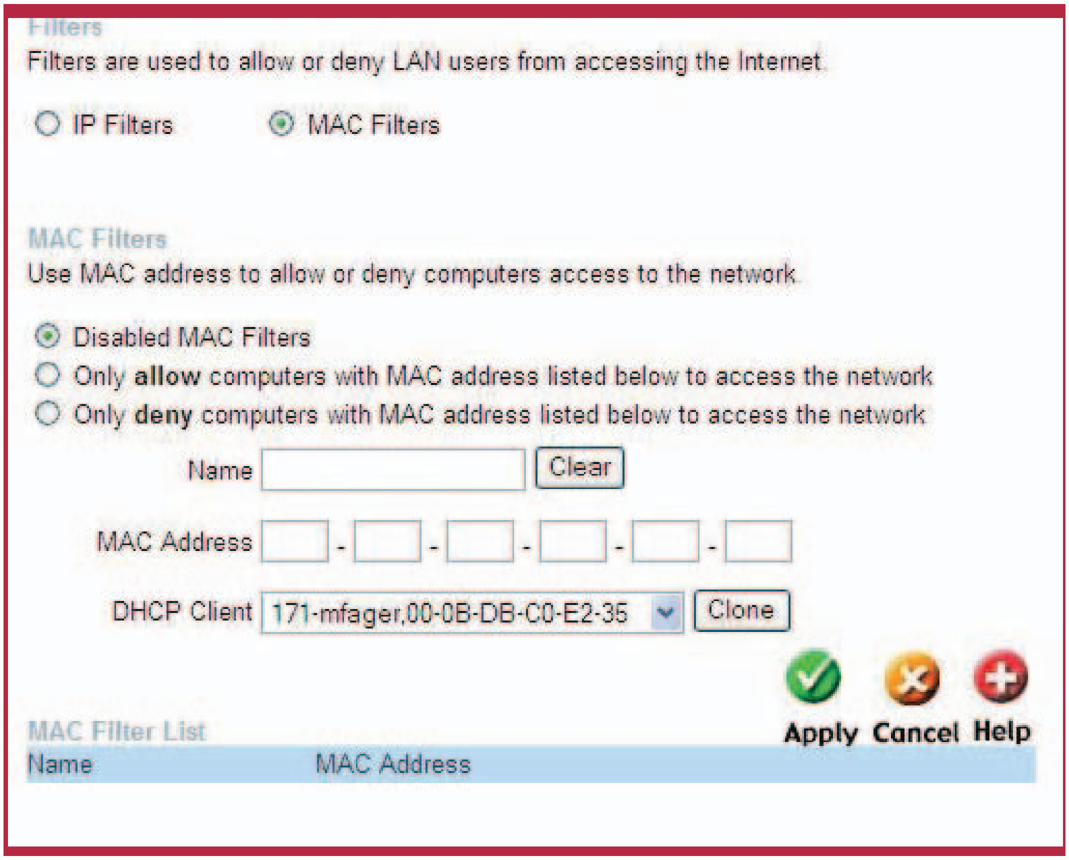
IP: The IP address of the LAN computer that will be denied access to the Internet.

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.

MAC Filters



Filters

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

○ IP Filters ● MAC Filters

MAC Filters

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

● Disabled MAC Filters

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

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

Name:

MAC Address: - - - - -

DHCP Client: 171-mfager,00-0B-DB-C0-E2-35

MAC Filter List

Name	MAC Address

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.

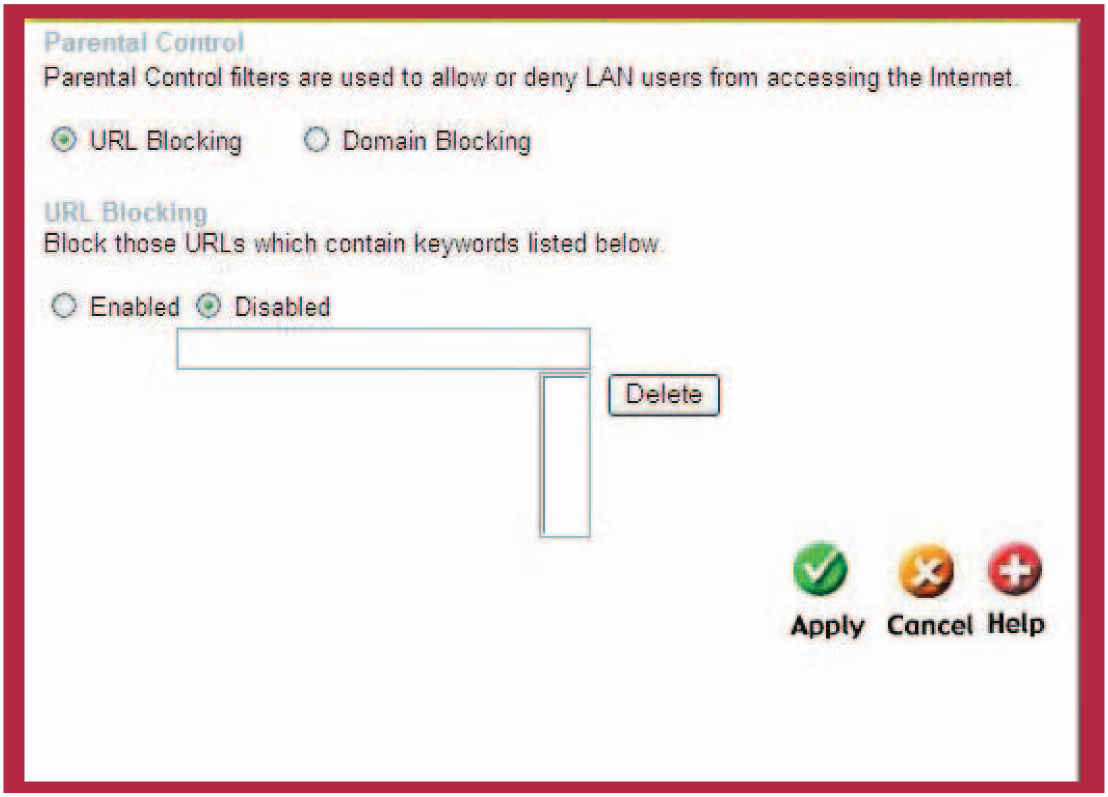
Name: Enter the name here.

MAC Address: Enter the MAC Address.

DHCP Client: Select a DHCP client from the pull-down list; click **Clone** to copy that MAC Address.

Parental Control

URL Blocking



Parental Control

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

● URL Blocking ○ Domain Blocking

URL Blocking

Block those URLs which contain keywords listed below.

○ Enabled ● Disabled

Advanced > Parental Control > URL Blocking

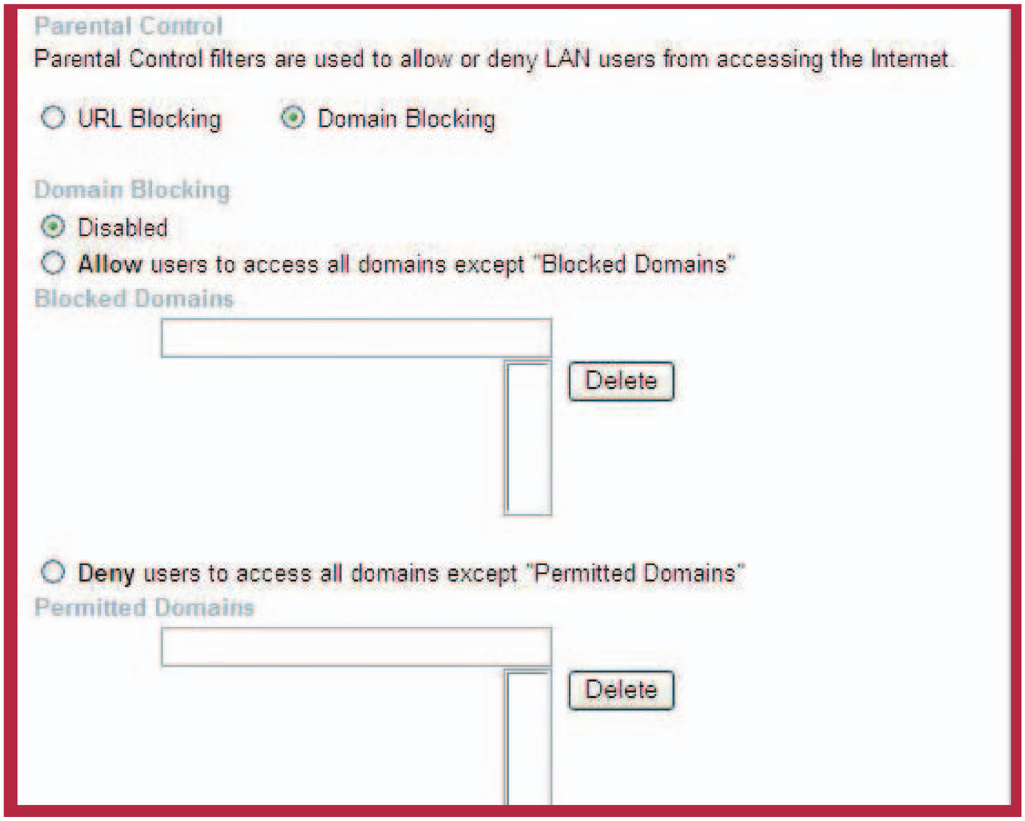
URL Blocking is used to deny LAN computers from accessing specific web sites by the URL. A URL is a specially formatted text string that defines a location on the Internet. If any part of the URL contains the blocked word, the site will not be accessible and the web page will not display. To use this 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**.

Parental Control 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.

Domain Blocking



Parental Control

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

○ URL Blocking ● Domain Blocking

Domain Blocking

● Disabled

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

Blocked Domains

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

Permitted Domains

Advanced > Parental Control > 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.

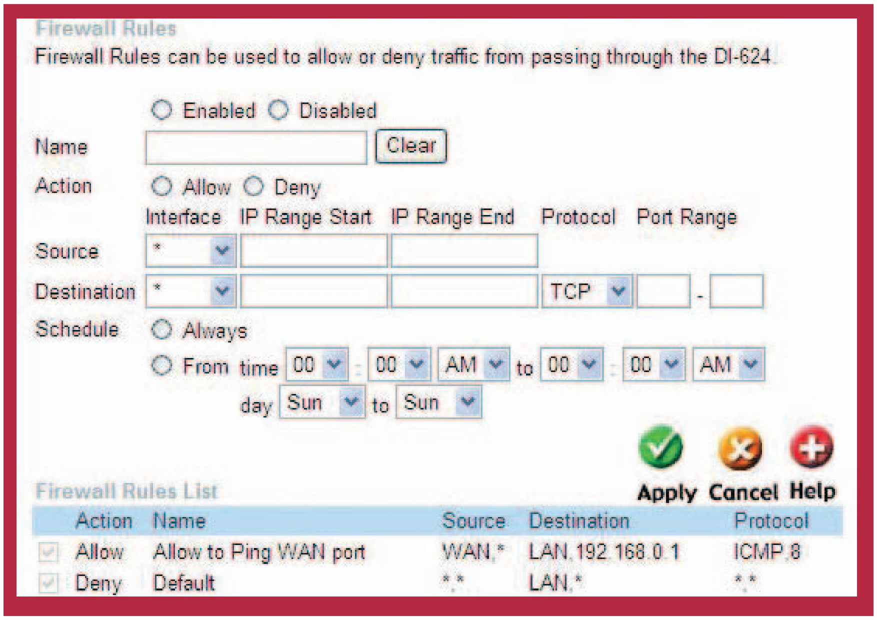
Parental ControlFilters: Select the filter you wish to use; in this case, **Domain Blocking** was chosen.

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.

Firewall



Firewall Rules

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

○ Enabled ○ Disabled

Name Clear

Action ○ Allow ○ Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	*				
Destination	*			TCP	-

Schedule ○ Always

○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

Firewall Rules List

	Action	Name	Source	Destination	Protocol
☑	Allow	Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,8
☑	Deny	Default	*,*	LAN,*	*,*

Advanced > Firewall

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

Firewall Rules: **Enable** or **disable** the Firewall.

Name: Enter the name.

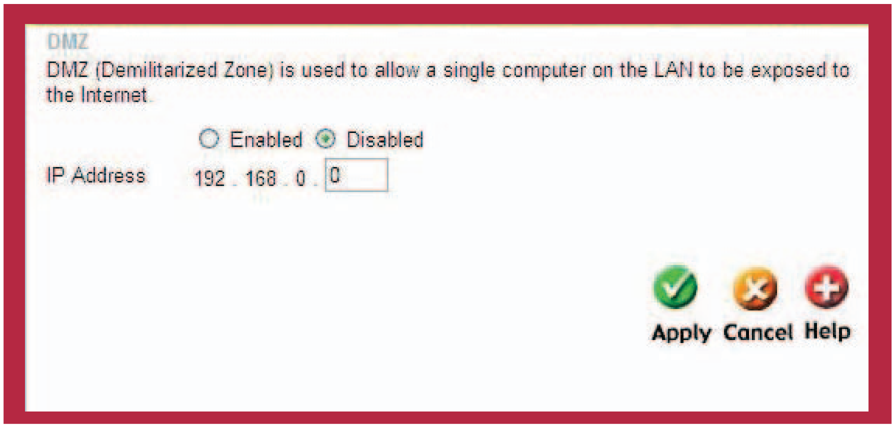
Action: Select **Allow** or **Deny**.

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**.

DMZ



DMZ

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

○ Enabled ● Disabled

IP Address 192 . 168 . 0 . 0

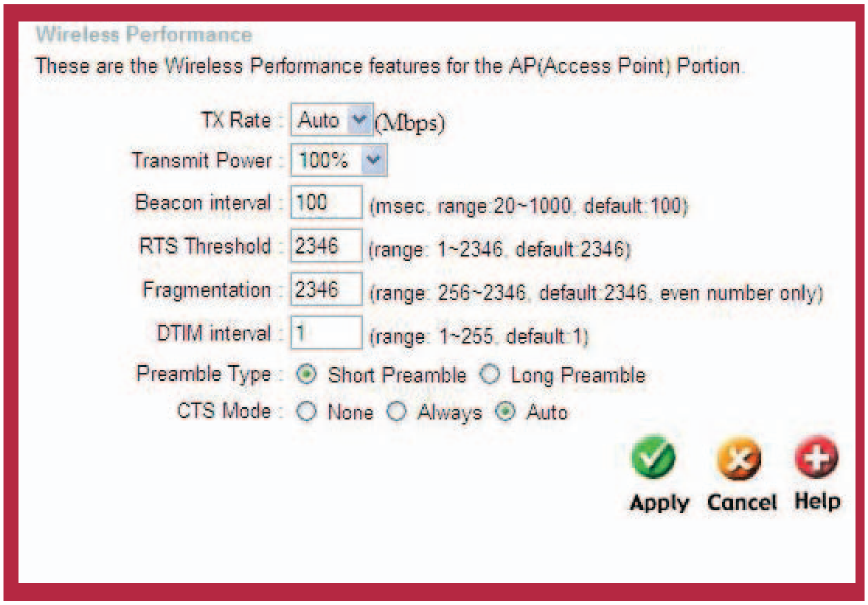
Advanced > DMZ

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

Performance



Wireless Performance

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

TX Rate : Auto (Mbps)

Transmit Power : 100%

Beacon interval : 100 (msec, range:20~1000, default:100)

RTS Threshold : 2346 (range: 1~2346, default:2346)

Fragmentation : 2346 (range: 256~2346, default:2346, even number only)

DTIM interval : 1 (range: 1~255, default:1)

Preamble Type : ● Short Preamble ○ Long Preamble

CTS Mode : ○ None ○ Always ● Auto

Advanced > Performance

Note: These features will be available in future firmware releases.

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

Transmit Power: **100%** is the default selection. Select from the drop down menu.

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. *Note: High network traffic areas should use the shorter preamble type.*

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

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

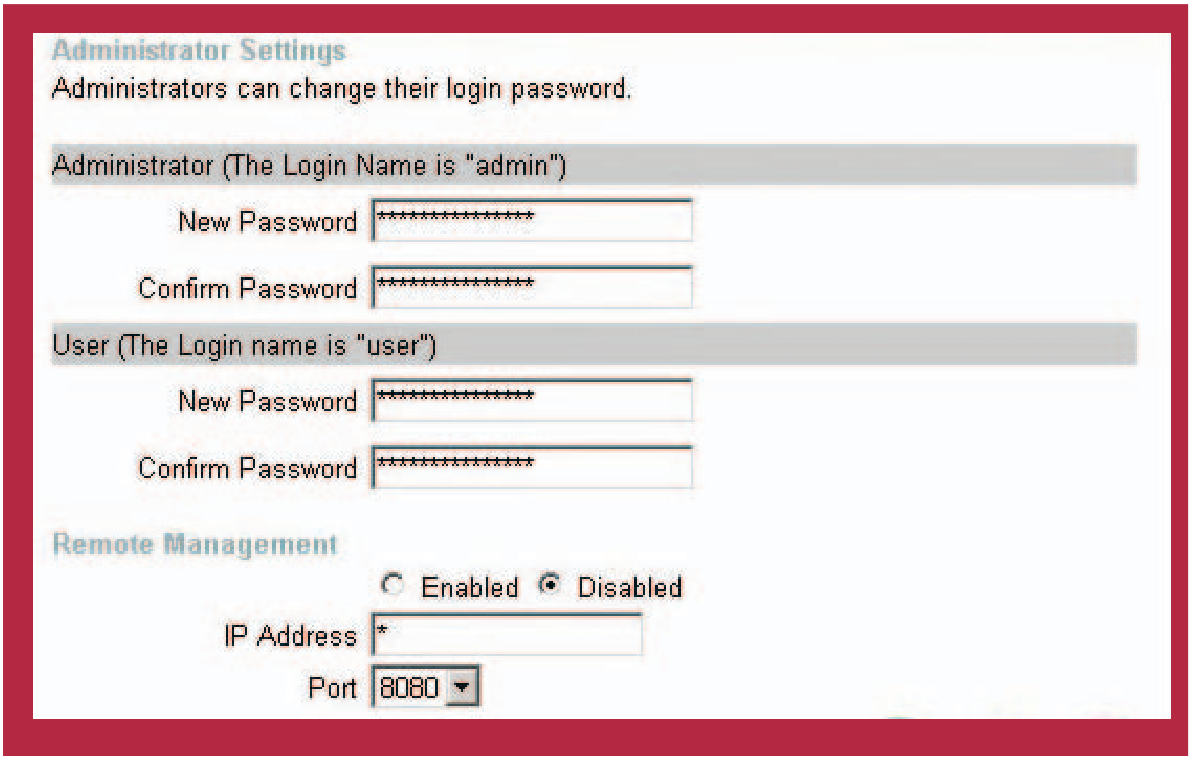
Always: CTS will always be used to make sure the wireless LAN is clear before sending data.

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

Tools

The Advanced tab provides the following options: Admin, Time, System, Firmware, and Misc.

Admin



Administrator Settings

Administrators can change their login password.

Administrator (The Login Name is "admin")

New Password: ****************

Confirm Password: ****************

User (The Login name is "user")

New Password: ****************

Confirm Password: ****************

Remote Management

○ Enabled ● Disabled

IP Address: *

Port: 8080

Tools > Admin

At this page, the DI-624M 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

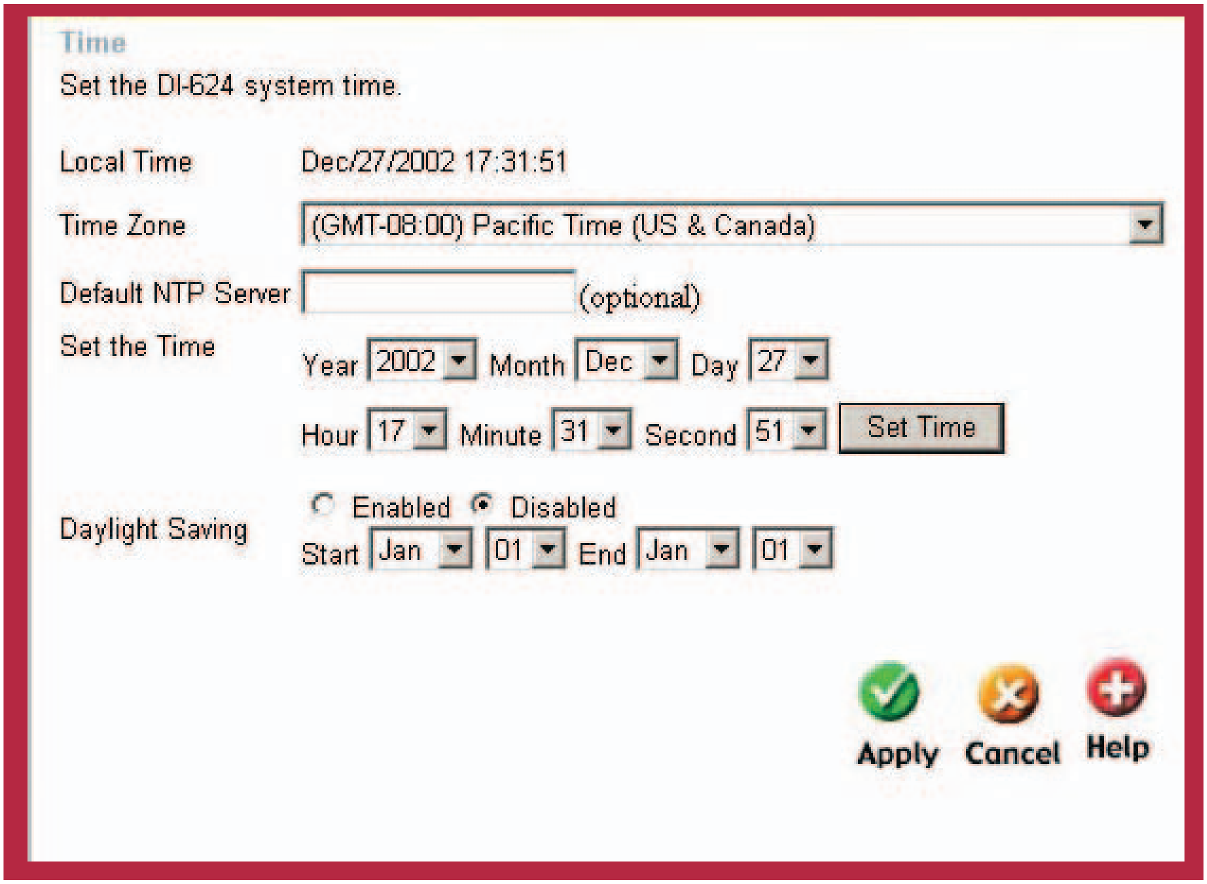
Remote Management: Remote management allows the DI-624M to be configured from the Internet by a web browser. A username and password is still required to access the Web-Management interface. In general, only a member of your network can browse the built-in web pages to perform **Administrator** tasks.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

Time



Time

Set the DI-624 system time.

Local Time Dec/27/2002 17:31:51

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

Default NTP Server (optional)

Set the Time Year 2002 Month Dec Day 27

Hour 17 Minute 31 Second 51

Daylight Saving ○ Enabled ● Disabled

Start Jan 01 End Jan 01

Tools > Time

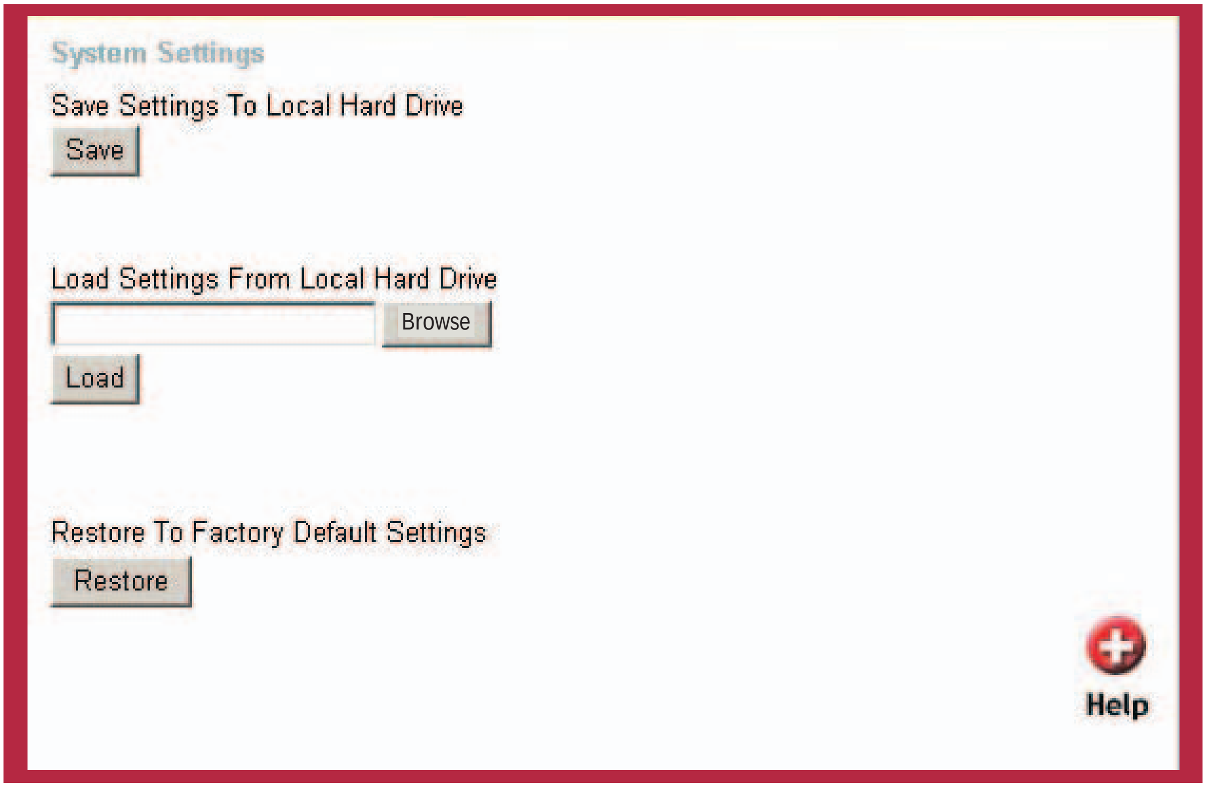
Time Zone: Select the Time Zone from the pull-down menu.

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.

System



System Settings

Save Settings To Local Hard Drive

Load Settings From Local Hard Drive

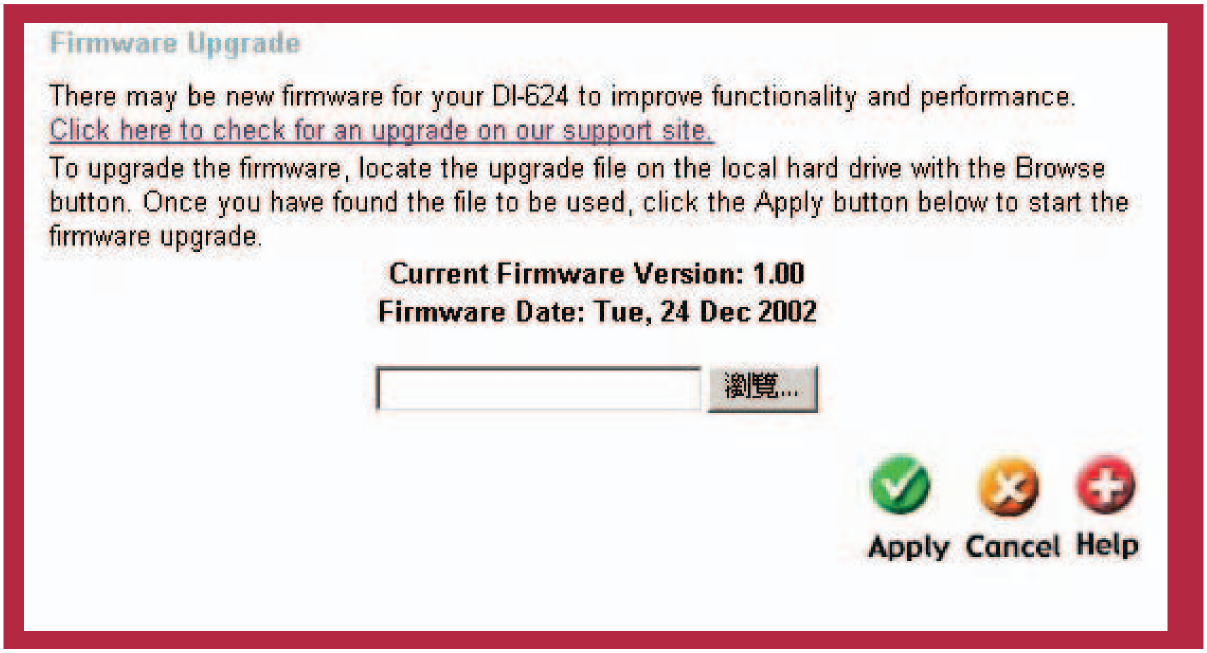
Restore To Factory Default Settings

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.

Firmware



Firmware Upgrade

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

Current Firmware Version: 1.00
Firmware Date: Tue, 24 Dec 2002

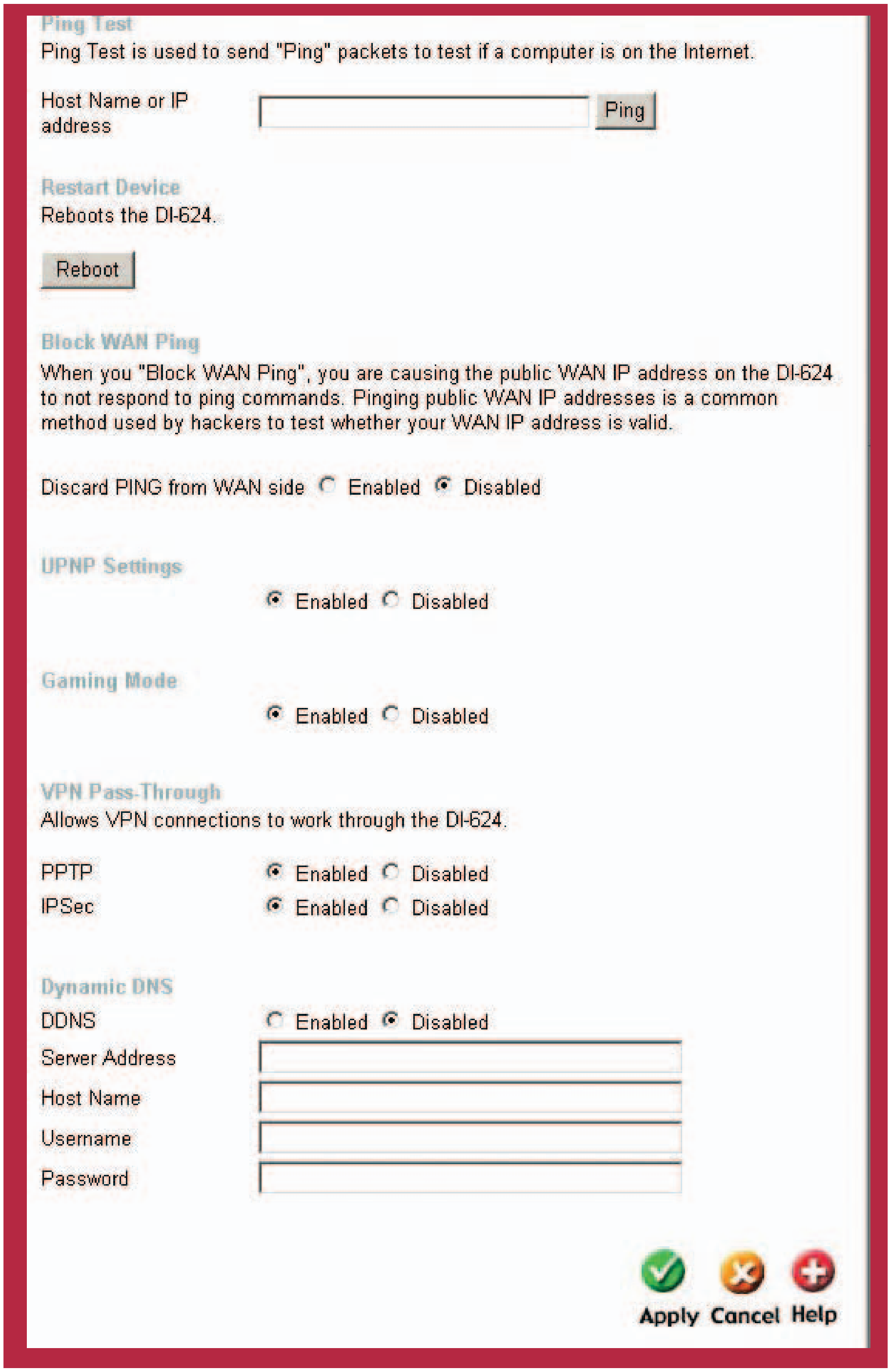
Tools > Firmware

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.

Misc.



Ping Test

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

Host Name or IP address [ ]

Restart Device

Reboots the DI-624.

Block WAN Ping

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

Discard PING from WAN side ○ Enabled ● Disabled

UPNP Settings

● Enabled ○ Disabled

Gaming Mode

● Enabled ○ Disabled

VPN Pass-Through

Allows VPN connections to work through the DI-624.

PPTP ● Enabled ○ Disabled

IPSec ● Enabled ○ Disabled

Dynamic DNS

DDNS ○ Enabled ● Disabled

Server Address [ ]

Host Name [ ]

Username [ ]

Password [ ]

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-624M.

Block WAN Ping: If you choose to block WAN Ping, the WAN IP Address of the DI-624M 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.

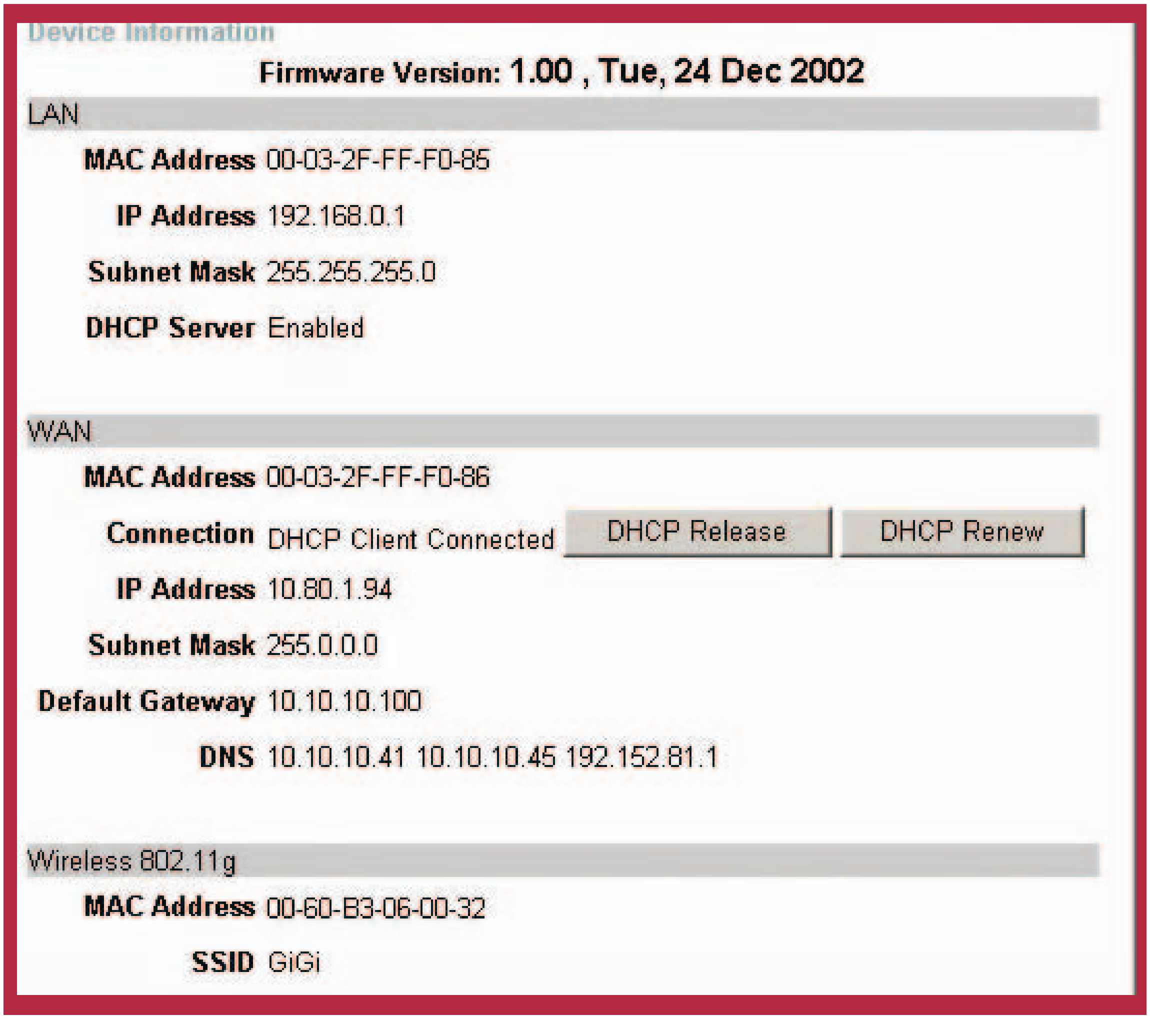
Dynamic DNS: Dynamic Domain Name System is a method of keeping a domain name linked to a changing IP Address. This is a useful feature since many computers do not use a static IP address.

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

Tools

The Advanced tab provides the following options: Device Info, Log, Stats, and Wireless.

Device Info



Device Information

Firmware Version: 1.00 , Tue, 24 Dec 2002

LAN

MAC Address 00-03-2F-FF-F0-85

IP Address 192.168.0.1

Subnet Mask 255.255.255.0

DHCP Server Enabled

WAN

MAC Address 00-03-2F-FF-F0-86

Connection DHCP Client Connected

IP Address 10.80.1.94

Subnet Mask 255.0.0.0

Default Gateway 10.10.10.100

DNS 10.10.10.41 10.10.10.45 192.152.81.1

Wireless 802.11g

MAC Address 00-60-B3-06-00-32

SSID GiGi

Status > Device Info

This page displays the current information for the DI-624M. 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-624M'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-624M

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

Wireless:

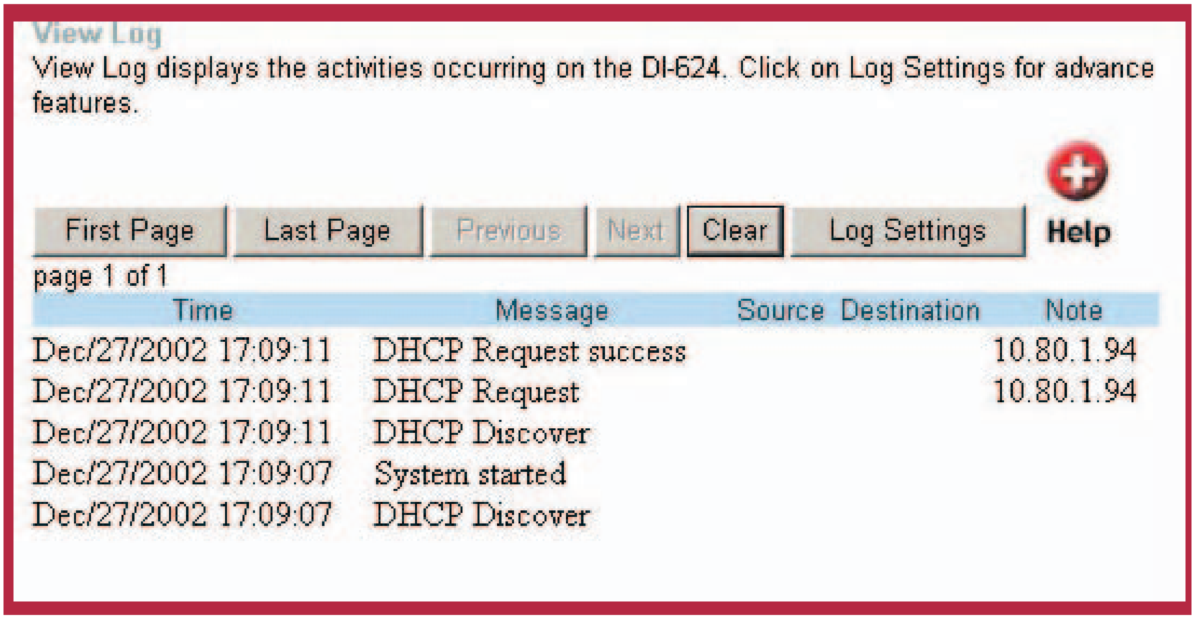
MAC Address: Displays the MAC address

SSID: Displays the current SSID

Channel: Displays the current channel

WEP: indicates whether WEP is enabled or disabled

Log



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

page 1 of 1

```
Time                   Message                 Source  Destination   Note
Dec/27/2002 17:09:11   DHCP Request success                          10.80.1.94
Dec/27/2002 17:09:11   DHCP Request                                  10.80.1.94
Dec/27/2002 17:09:11   DHCP Discover
Dec/27/2002 17:09:07   System started
Dec/27/2002 17:09:07   DHCP Discover
```

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.

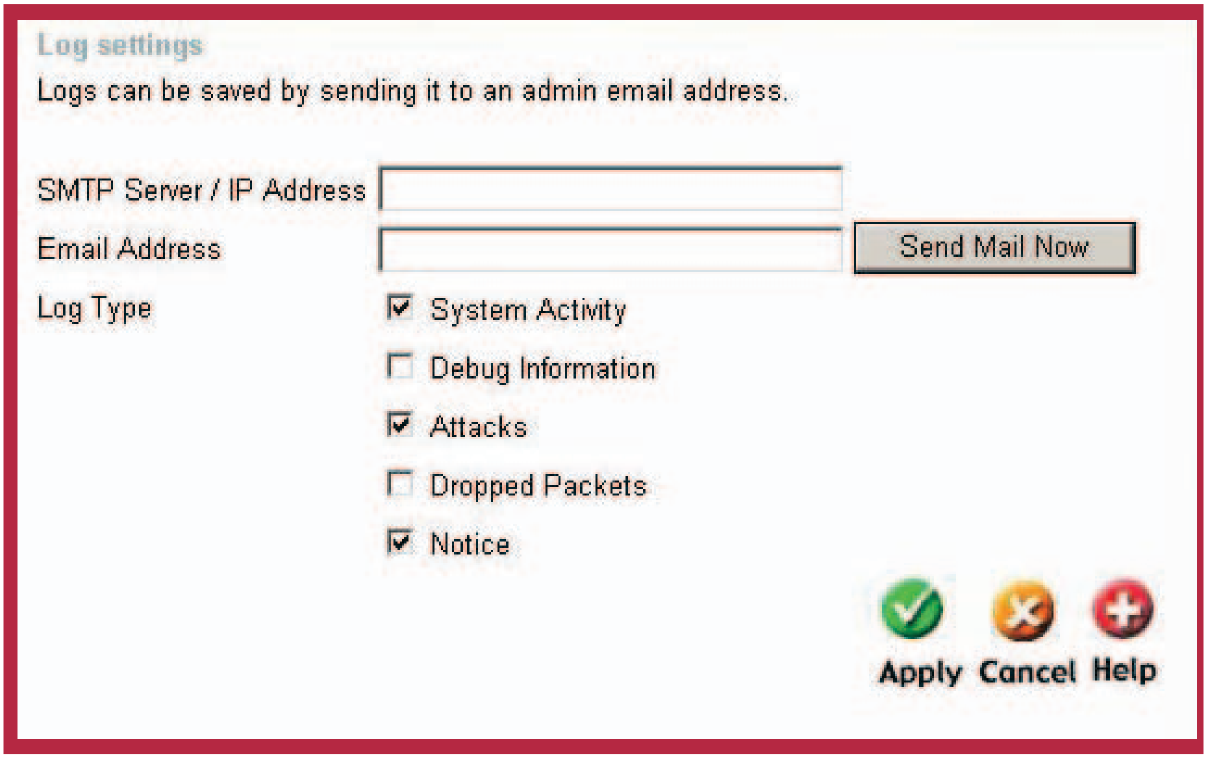
Previous - Moves back one log page.

Next - Moves forward one log page.

Clear - Clears the logs completely.

Log Settings - Brings up the page to configure the log.

Log Settings



Log settings

Logs can be saved by sending it to an admin email address.

SMTP Server / IP Address	
Email Address	
Log Type	☑ System Activity □ Debug Information ☑ Attacks □ Dropped Packets ☑ Notice

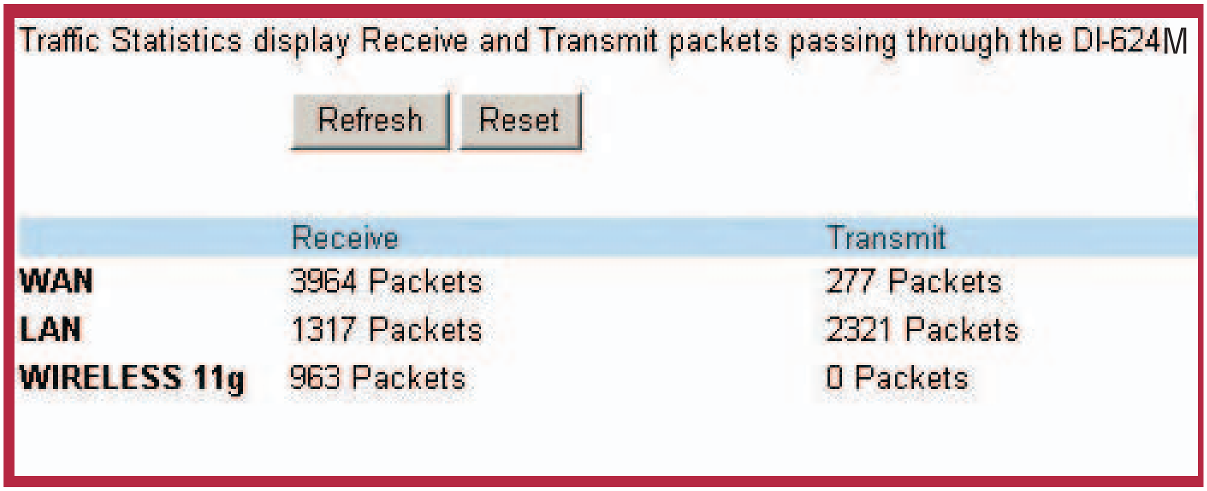
Status > Log > Log Settings

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.

Stats

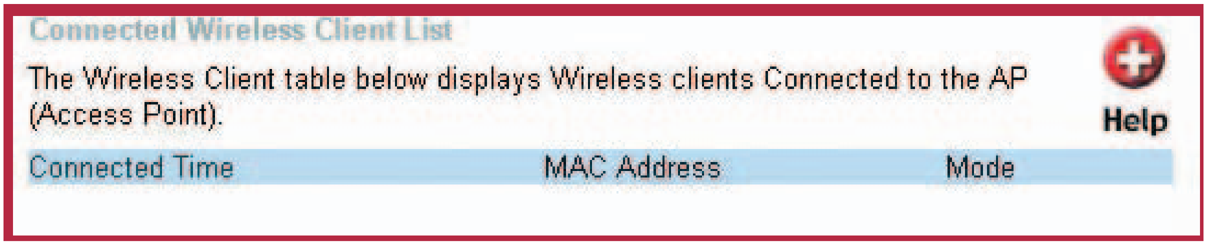

Traffic Statistics display Receive and Transmit packets passing through the DI-624M

	Receive	Transmit
WAN	3964 Packets	277 Packets
LAN	1317 Packets	2321 Packets
WIRELESS 11g	963 Packets	0 Packets

Status > Stats

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

Wireless


Connected Wireless Client List

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

Connected Time	MAC Address	Mode

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.

Troubleshooting

This Chapter provides solutions to problems that can occur during the installation and operation of the DI-624M 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-624M Wireless Broadband Router.

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

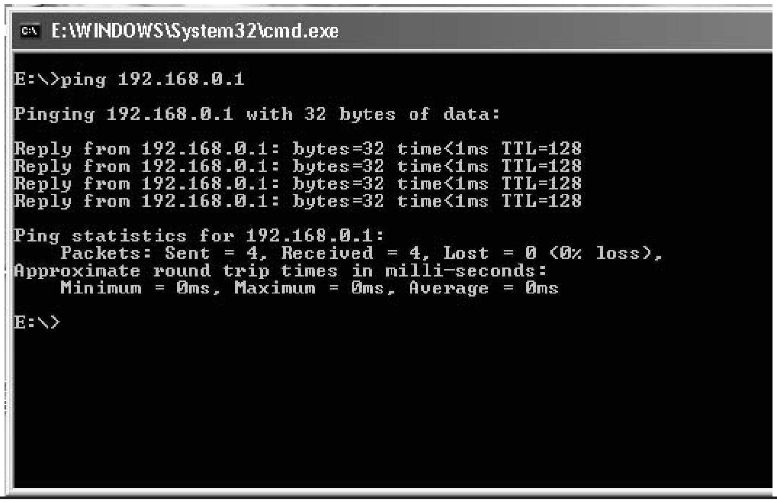
1. The computer used to configure the DI-624M cannot access the Configuration menu.

- Check that the **Ethernet LED** on the DI-624M 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-624M. Please see ***Checking the IP Address in Windows XP*** in the **Networking Basics** section of this manual.

Note: The IP Address of the DI-624M 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-624M is responding. Go to **Start**>**Run**>Type **Command**>Type **ping 192.168.0.1.** A successful ping will show four replies.

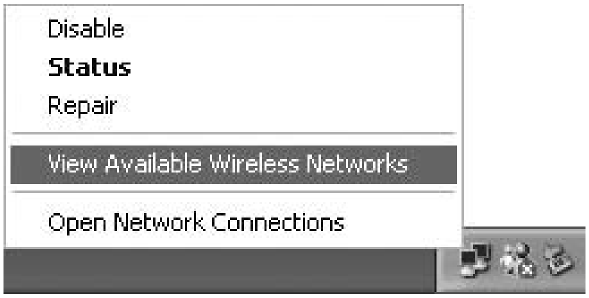
Note: If you have changed the default IP Address, make sure to ping the correct IP Address assigned to the DI-624M.

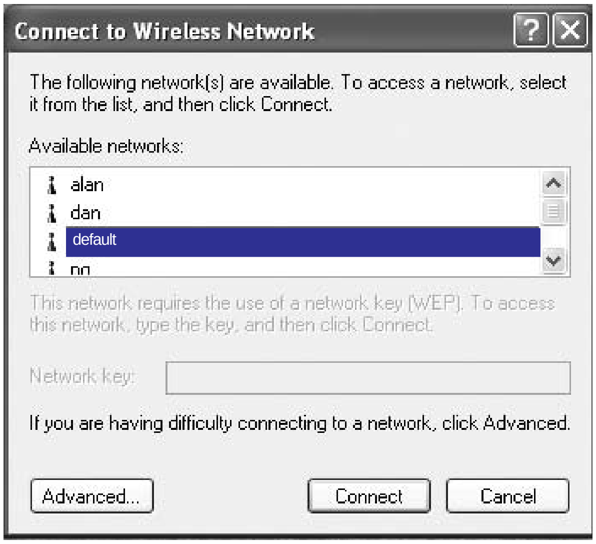


```
E:\>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128
Reply from 192.168.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

E:\>
```

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.




Connect to Wireless Network

The following network(s) are available. To access a network, select it from the list, and then click Connect.

Available networks:

This network requires the use of a network key (WEP). To access this network, type the key, and then click Connect.

Network key:

If you are having difficulty connecting to a network, click Advanced.

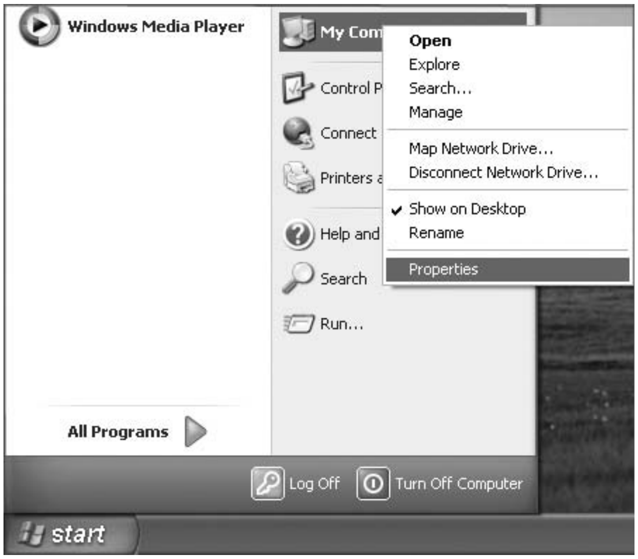
- Check that the **IP Address** assigned to the wireless adapter is within the same **IP Address range** as the access point and gateway. *(Since the DI-624M has an IP Address of 192.168.0.1, wireless adapters must have an IP Address in the same range, e.g., 192.168.0.x. Each device must have a unique 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**.)*

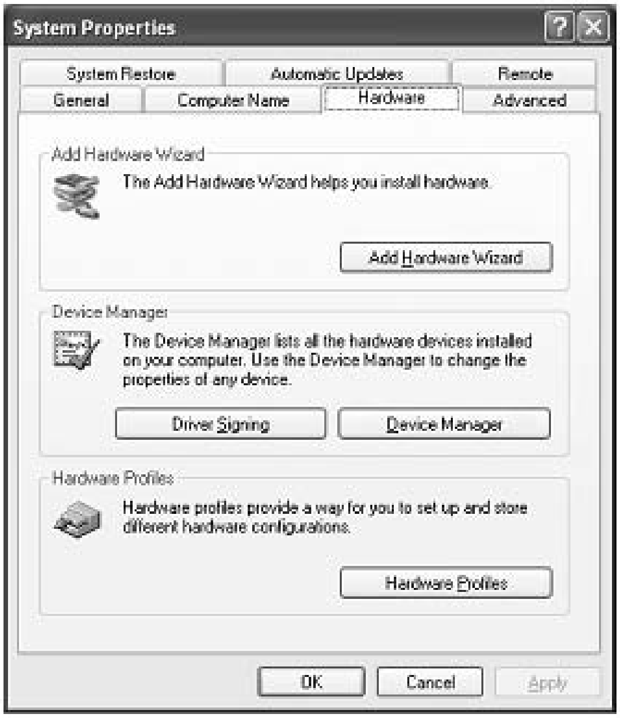
3. Check that the drivers for the network adapters are installed properly.

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 > Properties**.



- **Select** the **Hardware Tab**.
- Click **Device Manager**.



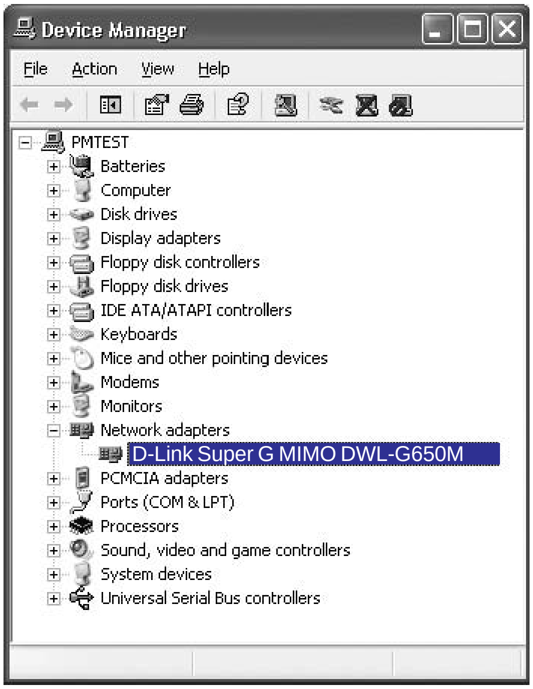
The Add Hardware Wizard helps you install hardware.

The Device Manager lists all the hardware devices installed on your computer. Use the Device Manager to change the properties of any device.

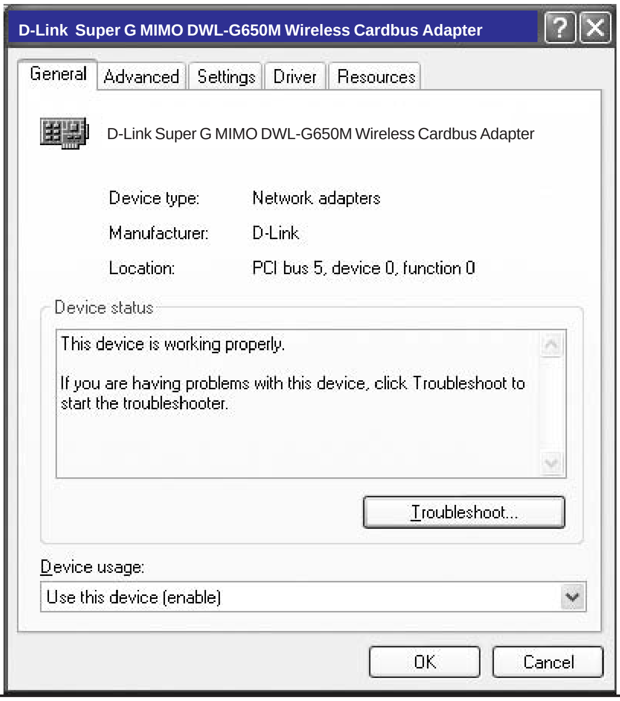
Hardware profiles provide a way for you to set up and store different hardware configurations.

- Double-click on **Network Adapters**.
- Right-click on **D-Link DWL-G650M Super G MIMO Wireless Notebook Adapter**. (In this example we use the DWL-G650M; 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**.



D-Link Super G MIMO DWL-G650M Wireless Cardbus Adapter

Device type: Network adapters

Manufacturer: D-Link

Location: PCI bus 5, device 0, function 0

Device status

This device is working properly.

If you are having problems with this device, click Troubleshoot to start the troubleshooter.

Device usage: Use this device (enable)

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-624M. 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-624M, you must also enable encryption on all wireless clients in order to establish a wireless connection.

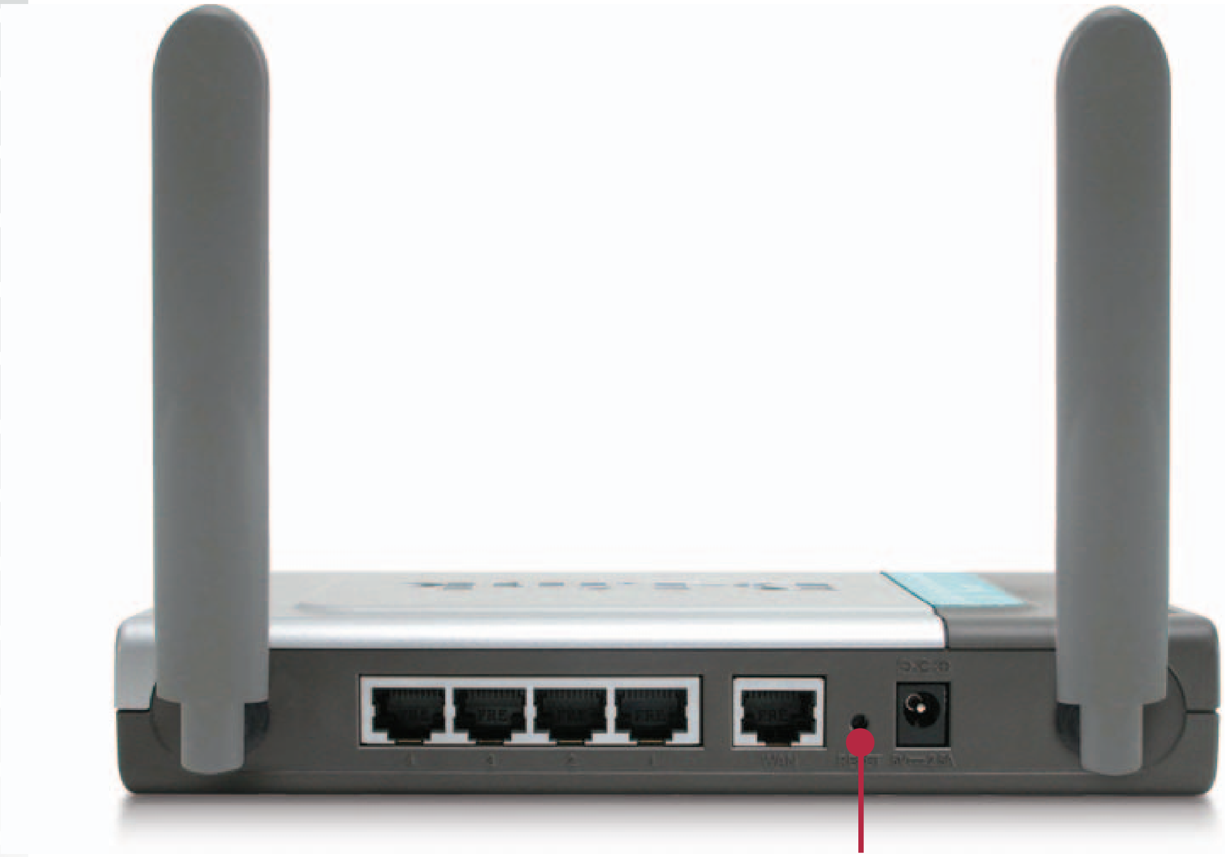
- For 802.11b, the Encryption settings are: 64, 128, or 256 bit. Make sure that the encryption bit level is the same on the Router and the Wireless Client.
- Make sure that the SSID on the Router and the Wireless Client are exactly the same. If they are not, wireless connection will not be established.
- Move the DI-624M and the wireless client into the same room and then test the wireless connection.
- Disable all security settings. (WEP, MAC Address Control)\
- Turn off your DI-624M and the client. Turn the DI-624M 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-624M, 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-624M 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-624M to Factory Default Settings

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



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

- Locate the **Reset** button on the back of the DI-624M.
- Use a paper clip to press the **Reset** button.
- Hold for about 10 seconds and then release.
- After the DI-62M 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

Wireless Frequency Range:

- 2.4GHz to 2.462GHz

LEDs:

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

Physical Dimensions:

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

Wireless Transmit Power:

- 15dBm ± 2dB

Security:

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

External Antenna Type:

- Dual non-detachable antennas

Modulation Technology:

- Orthogonal Frequency Division Multiplexing (OFDM)

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, -71dBm
- 48Mbps OFDM, 10% PER, -71dBm
- 36Mbps OFDM, 10% PER, -78dBm
- 24Mbps OFDM, 10% PER, -82dBm
- 18Mbps OFDM, 10% PER, -85dBm
- 12Mbps OFDM, 10% PER, -87dBm
- 11Mbps CCK, 8% PER, -85dBm
- 9Mbps OFDM, 10% PER, -90dBm
- 6Mbps OFDM, 10% PER, -91dBm
- 5.5Mbps CCK, 8% PER, -88dBm
- 2Mbps QPSK, 8% PER, -89dBm
- 1Mbps BPSK, 8% PER, -92dBm

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

Frequently Asked Questions

1 Why can´t I access the Web based configuration?

When entering the IP Address of the DI-624M (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.

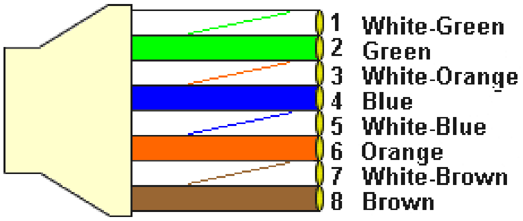
What type of cable should I be using?

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)

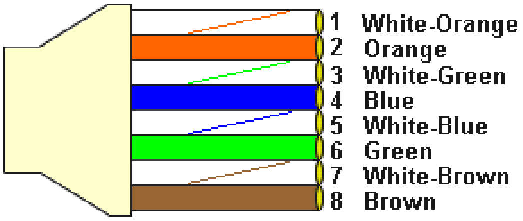
The following connections require a Straight-through Cable:
Computer to Residential Gateway/Router
Computer to Normal Port (hub/switch)
Access Point to Normal Port (hub/switch)
Print Server to Normal Port (hub/switch)
Uplink Port to Normal Port (hub/switch)

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

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

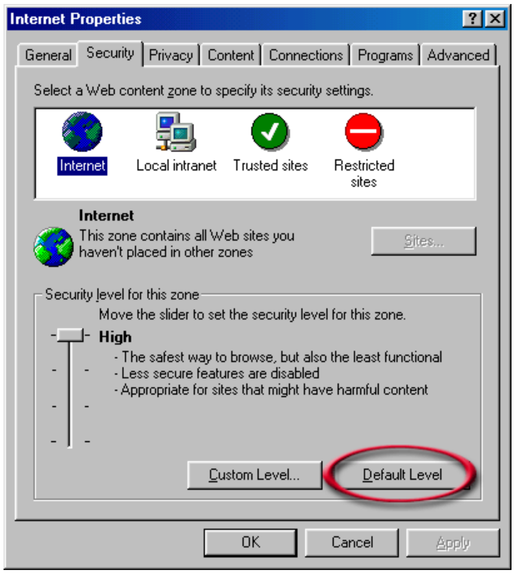
Hub/Switch uplink port to another Hub/Switch uplink port – Crossover

Hub/Switch uplink port to another Hub/Switch normal port - Straight-through

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.



Internet Properties

Select a Web content zone to specify its security settings.

Internet

This zone contains all Web sites you haven't placed in other zones

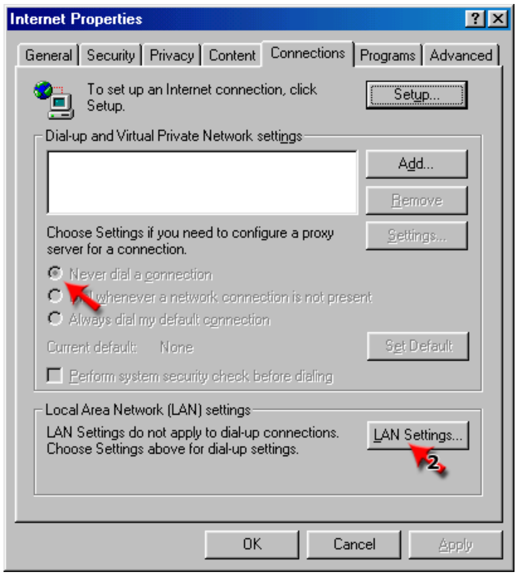
Security level for this zone

Move the slider to set the security level for this zone.

High

- The safest way to browse, but also the least functional
- Less secure features are disabled
- Appropriate for sites that might have harmful content

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



Internet Properties

To set up an Internet connection, click Setup.

Dial-up and Virtual Private Network settings

Choose Settings if you need to configure a proxy server for a connection.

○ Never dial a connection

○ whenever a network connection is not present

○ Always dial my default connection

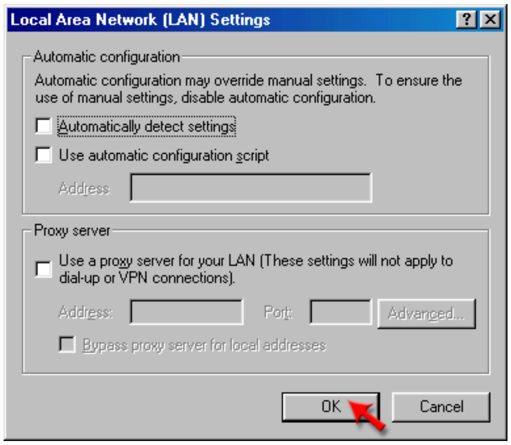
Current default: None

□ Perform system security check before dialing

Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

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



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

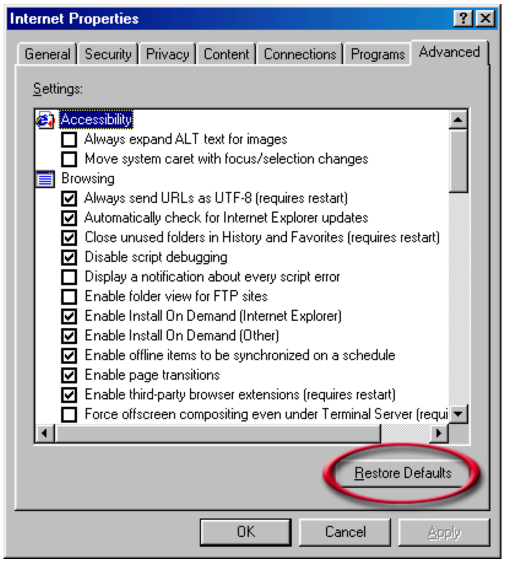
□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: Advanced...

□ Bypass proxy server for local addresses

OK Cancel

- 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.



Internet Properties

General | Security | Privacy | Content | Connections | Programs | Advanced

Settings:

Accessibility

□ Always expand ALT text for images

□ Move system caret with focus/selection changes

Browsing

☑ Always send URLs as UTF-8 (requires restart)

☑ Automatically check for Internet Explorer updates

☑ Close unused folders in History and Favorites (requires restart)

☑ Disable script debugging

□ Display a notification about every script error

□ Enable folder view for FTP sites

☑ Enable Install On Demand (Internet Explorer)

☑ Enable Install On Demand (Other)

☑ Enable offline items to be synchronized on a schedule

☑ Enable page transitions

☑ Enable third-party browser extensions (requires restart)

□ Force offscreen compositing even under Terminal Server (requi

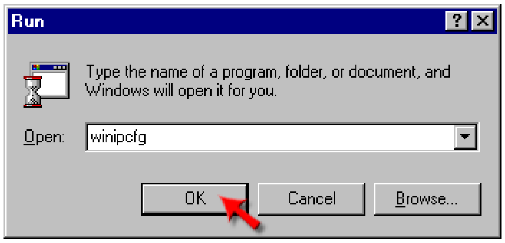
Restore Defaults

OK Cancel Apply

Step 4: 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 95, 98, or ME?

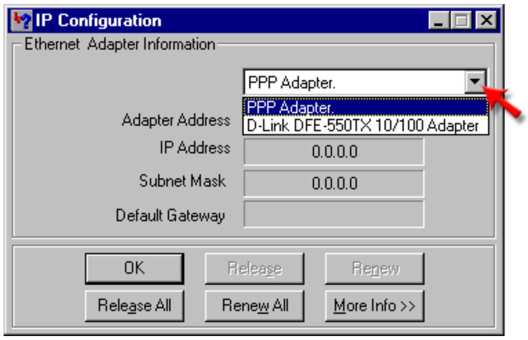
- Click on **Start**, then click on **Run**.
- The Run Dialogue Box will appear. Type **winipcfg** in the window as shown then click **OK**.



Type the name of a program, folder, or document, and Windows will open it for you.

Open: winipcfg

- The **IP Configuration** window will appear, displaying your **Ethernet Adapter Information**.
- Select your adapter from the drop down menu.
- If you do not see your adapter in the drop down menu, your adapter is not properly installed.



Ethernet Adapter Information

PPP Adapter.

PPP Adapter.
D-Link DFE-550TX 10/100 Adapter

Adapter Address

IP Address 0.0.0.0

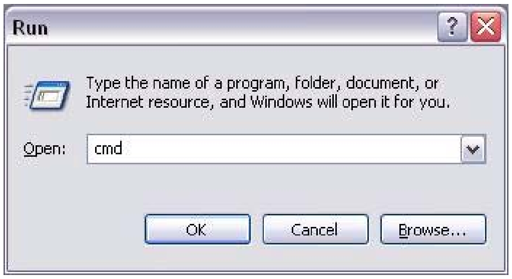
Subnet Mask 0.0.0.0

Default Gateway

- After selecting your adapter, it will display your IP Address, subnet mask, and default gateway.
- Click **OK** to close the IP Configuration window.

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

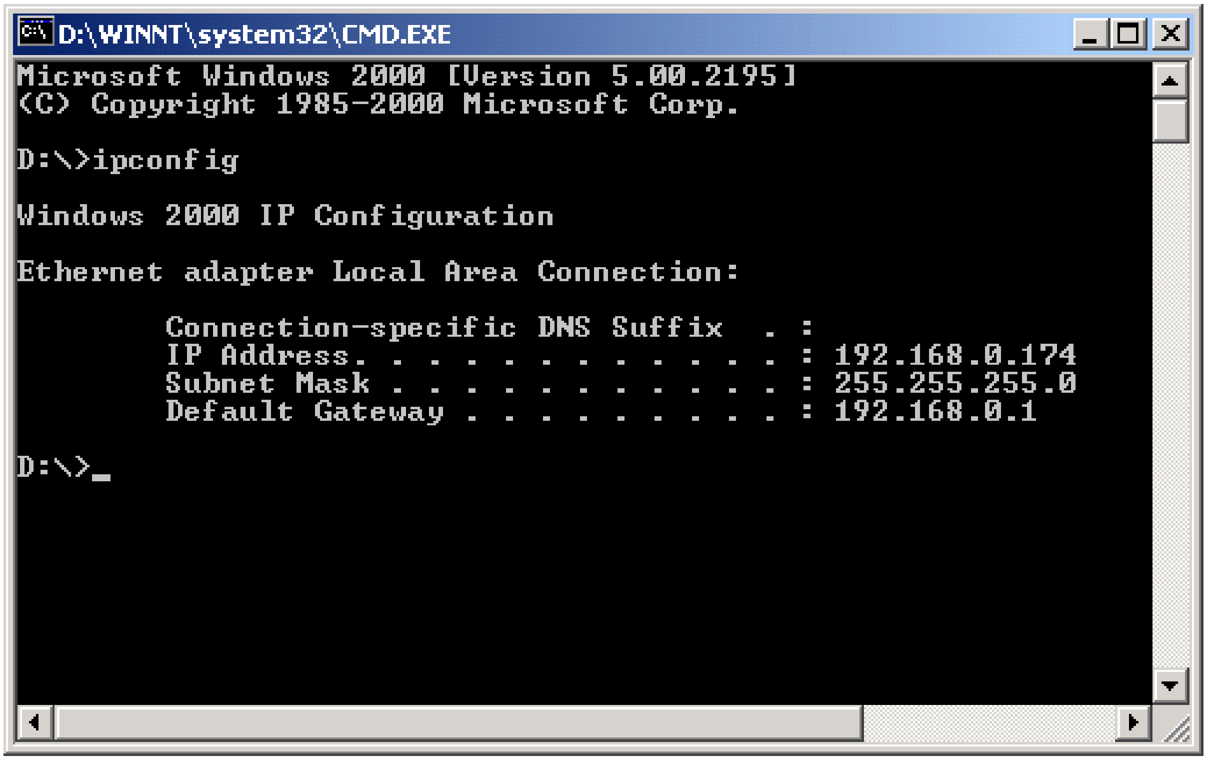
- Click on **Start** and select **Run**.
- Type **cmd** then click **OK**.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: cmd

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



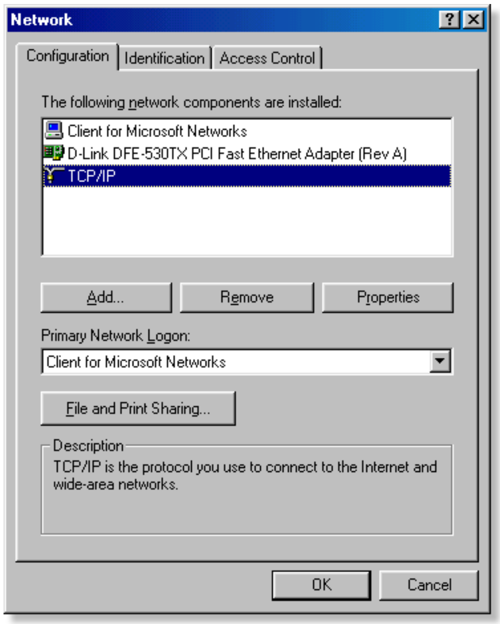
```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

D:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.174
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

D:\>_
```

- Type **exit** to close the command prompt.

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 98/Me?

- From the desktop, right-click on the **Network Neigborhood** icon (Win ME - My Network Places) and select **Properties**.
- Highlight **TCP/IP** and click the **Properties** button. If you have more than 1 adapter, then there will be a TCP/IP "Binding" for each adapter. Highlight **TCP/IP > (your network adapter)** and then click **Properties**.



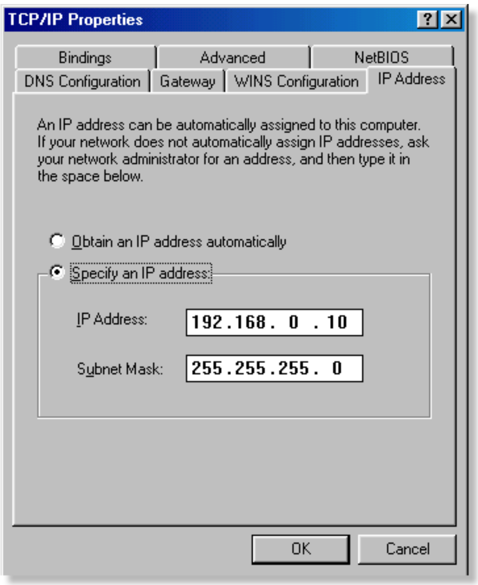
The following network components are installed:

- Client for Microsoft Networks
- D-Link DFE-530TX PCI Fast Ethernet Adapter (Rev A)
- TCP/IP

Primary Network Logon: Client for Microsoft Networks

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

- Click **Specify an IP Address**.
- Enter in 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 is between 2-99. Make sure that the number you choose is not in use on the network.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

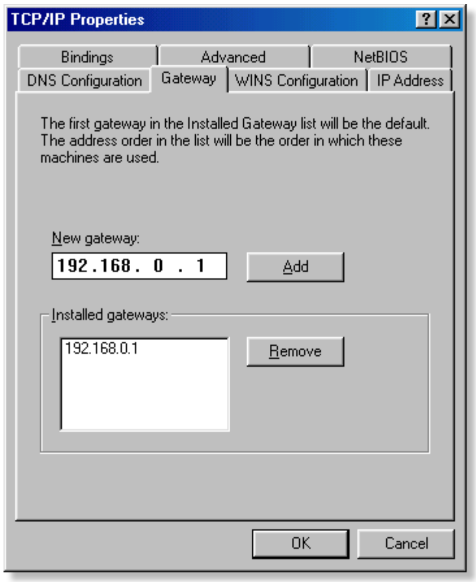
○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 192.168. 0 . 10

Subnet Mask: 255.255.255. 0

- Click on the **Gateway** tab.
- Enter the LAN IP Address of your router here (192.168.0.1).
- Click **Add** when finished.

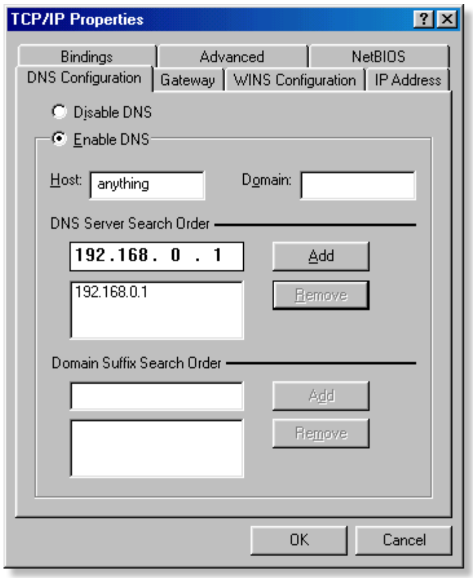


The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168.0.1

Installed gateways: 192.168.0.1

- Click on the **DNS Configuration** tab.
- Click **Enable DNS**. Type in a **Host** (can be any word). Under DNS server search order, enter the LAN IP Address of your router (192.168.0.1). Click **Add**.



○ Disable DNS

● Enable DNS

Host: anything Domain:

DNS Server Search Order

192.168.0.1

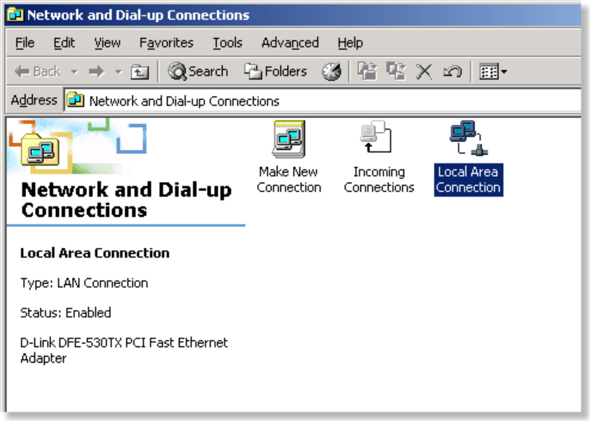
192.168.0.1

Domain Suffix Search Order

- Click **OK** twice.
- When prompted to reboot your computer, click **Yes**. After you reboot, the computer will now have a static, private IP Address.

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

- Right-click on **My Network Places** and select **Properties**.
- Right-click on the **Local Area Connection** which represents your network card and select **Properties**.


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders
Address Network and Dial-up Connections
Network and Dial-up Connections
Make New Connection
Incoming Connections
Local Area Connection

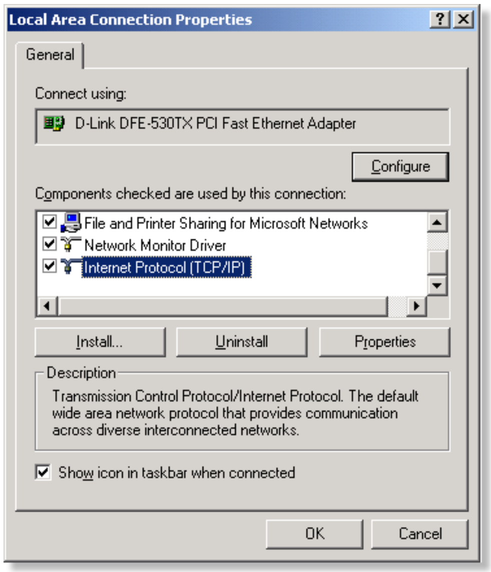
Local Area Connection

Type: LAN Connection

Status: Enabled

D-Link DFE-530TX PCI Fast Ethernet Adapter

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



Connect using:

D-Link DFE-530TX PCI Fast Ethernet Adapter

Components checked are used by this connection:

☑ File and Printer Sharing for Microsoft Networks
☑ Network Monitor Driver
☑ Internet Protocol (TCP/IP)

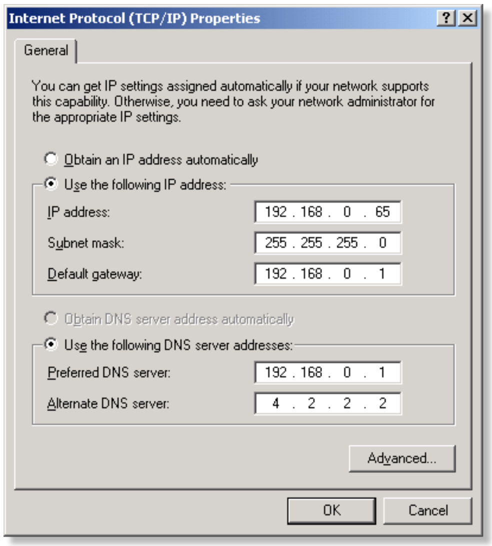
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☑ Show icon in taskbar when connected

- 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**.



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:	192 . 168 . 0 . 65
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	192 . 168 . 0 . 1

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server:	192 . 168 . 0 . 1
Alternate DNS server:	4 . 2 . 2 . 2

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

- Click on **Start > Control Panel > Network and Internet Connections > Network connections**.
- See the second step for assigning a static IP address in Windows 2000 and continue from there.

Step 5: Access the Web management. Open your Web browser and enter the IP Address of your D-Link device in the address bar. This should open the login page for the Web management. Follow instructions to login and complete the configuration.

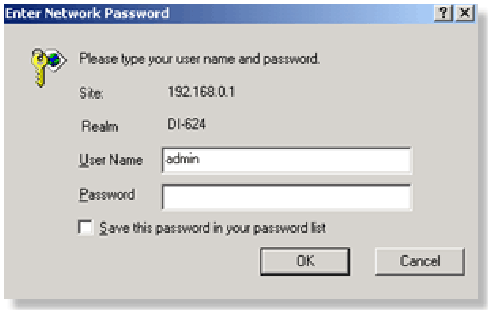
2 How can I setup my router to work with a Cable modem connection?

Dynamic Cable connection

(IE 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).



Enter Network Password

Please type your user name and password.

Site: 192.168.0.1

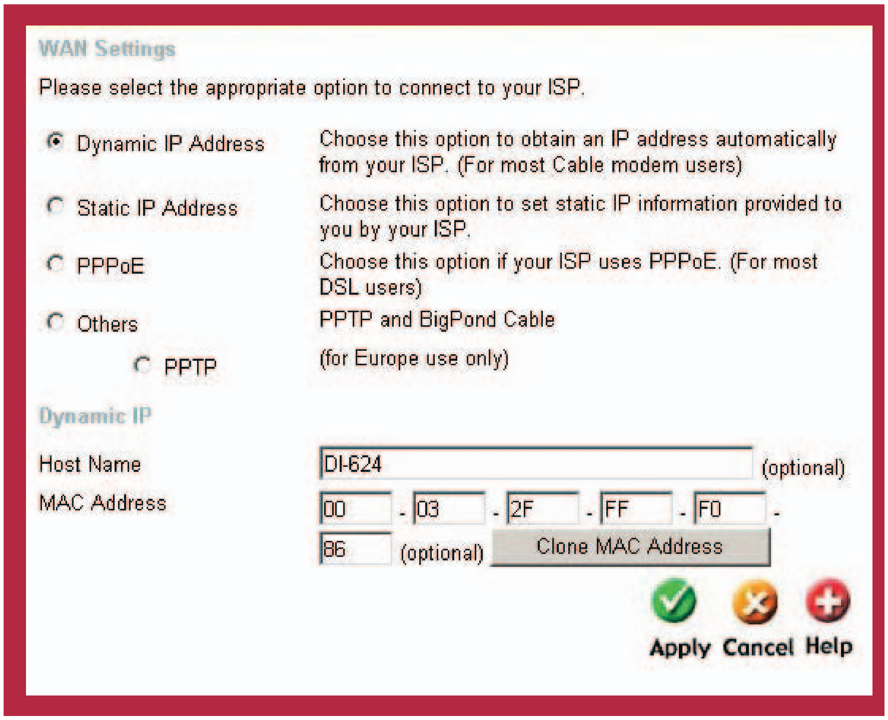
Realm DI-624

User Name admin

Password

□ Save this password in your password list

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.



WAN Settings

Please select the appropriate option to connect to your ISP.

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

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

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

○ Others — PPTP and BigPond Cable

○ PPTP — (for Europe use only)

Dynamic IP

Host Name DI-624 (optional)

MAC Address 00 - 03 - 2F - FF - F0 - 86 (optional)

Step 3: Power cycle the cable modem and router.

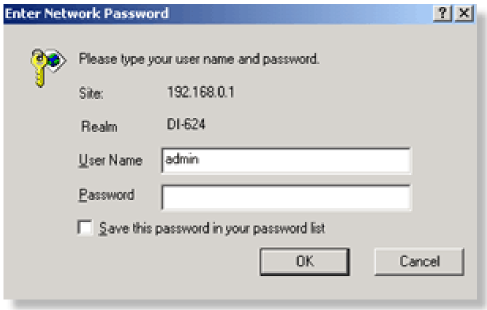
Turn the cable modem off (first) . Turn the router off Leave them off for 2 minutes.** Turn the cable modem on (first). Wait until you get a solid cable light on the cable modem. Turn the router on. Wait 30 seconds.

** 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).



Please type your user name and password.

Site: 192.168.0.1

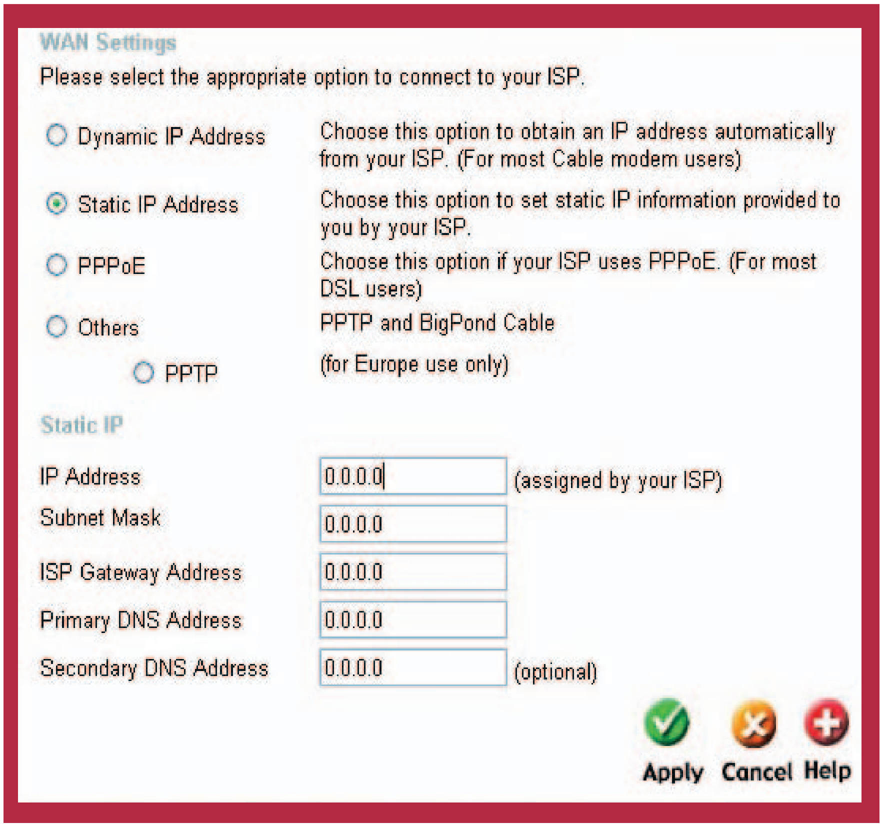
Realm DI-624

User Name admin

Password

□ Save this password in your password list

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.



WAN Settings

Please select the appropriate option to connect to your ISP.

○ Dynamic IP Address	Choose this option to obtain an IP address automatically from your ISP. (For most Cable modem users)
● Static IP Address	Choose this option to set static IP information provided to you by your ISP.
○ PPPoE	Choose this option if your ISP uses PPPoE. (For most DSL users)
○ Others	PPTP and BigPond Cable
○ PPTP	(for Europe use only)

Static IP

IP Address	0.0.0.0	(assigned by your ISP)
Subnet Mask	0.0.0.0	
ISP Gateway Address	0.0.0.0	
Primary DNS Address	0.0.0.0	
Secondary DNS Address	0.0.0.0	(optional)

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.

3 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.

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.

4 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.

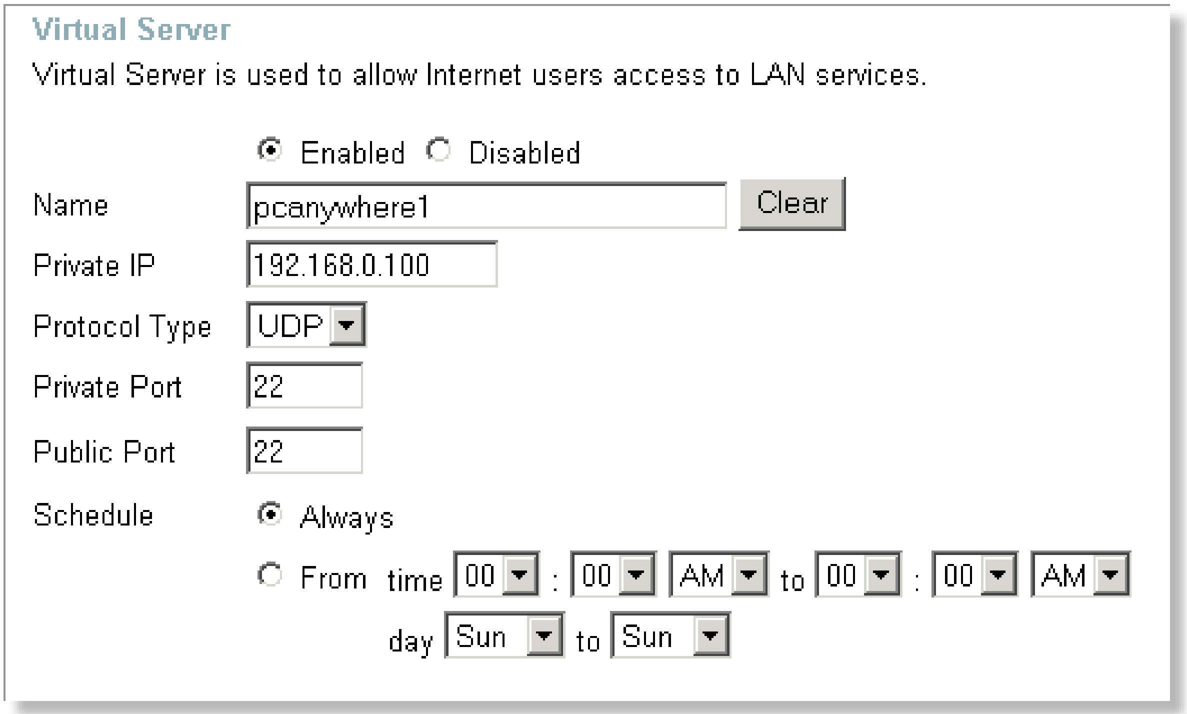
Go to http://www.aol.com for more specific configuration information of their software.

5 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 **Advanced** on top and then click **Virtual Server** on the left side.



Virtual Server

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

	● Enabled ○ Disabled
Name	pcanywhere1
Private IP	192.168.0.100
Protocol Type	UDP
Private Port	22
Public Port	22
Schedule	● Always ○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

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.

6 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

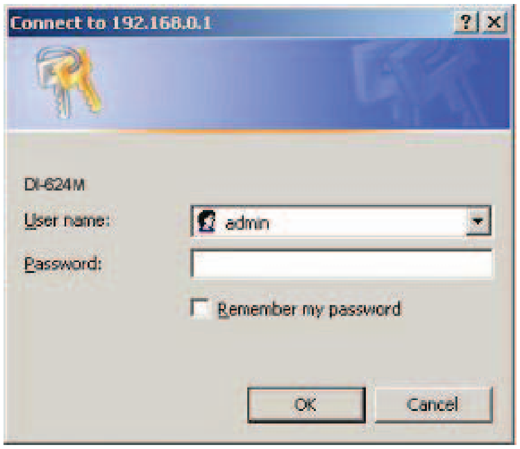
7 How do I configure the DMZ Host?

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/ME/9x or Macintosh operating systems please refer to Step 4 of the first question in this section (Frequently Asked Questions).

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)



Connect to 192.168.0.1

DI-624M

User name: admin

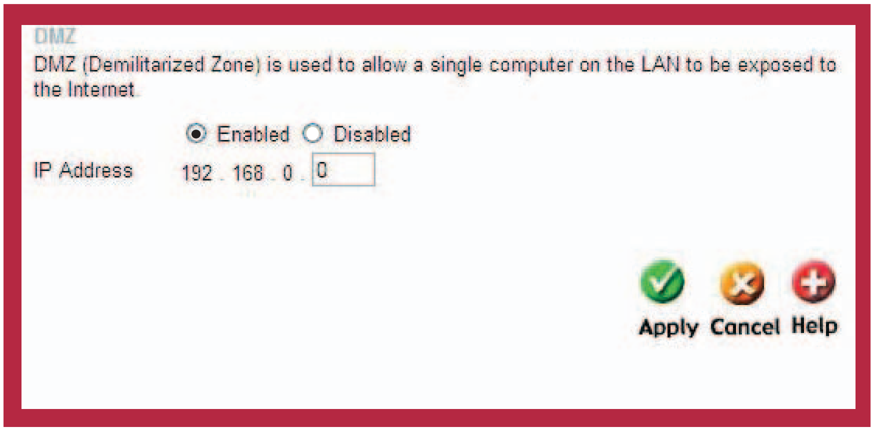
Password:

☐ Remember my password

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.



DMZ

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

● Enabled ○ Disabled

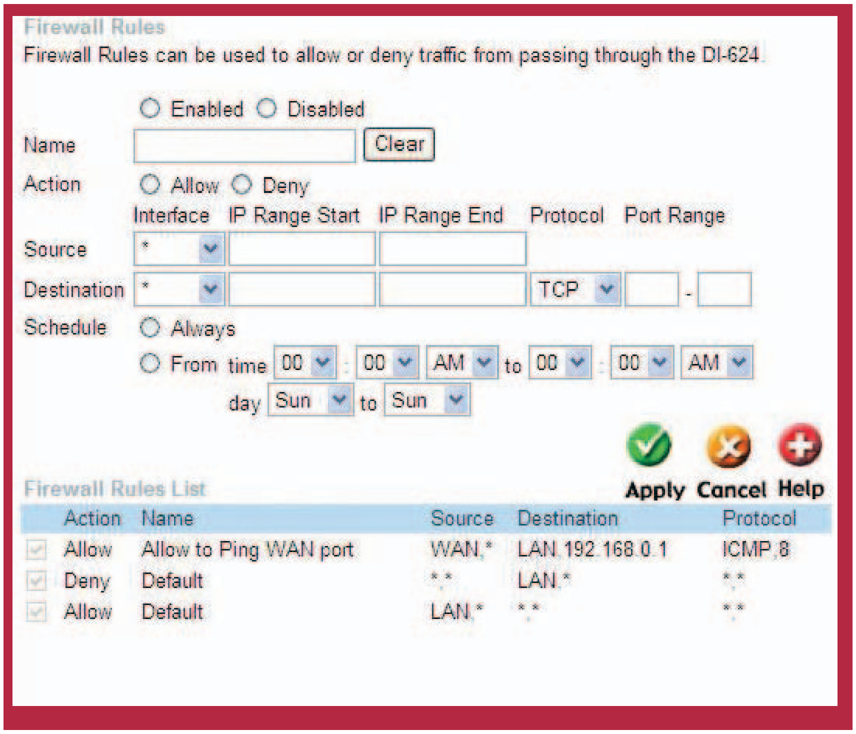
IP Address 192 . 168 . 0 . 0

8 How do I open a range of ports on my DI-624M 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.



Firewall Rules

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

○ Enabled ○ Disabled

Name [ ] Clear

Action ○ Allow ○ Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	*				
Destination	*			TCP	-

Schedule ○ Always

○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

Firewall Rules List

	Action	Name	Source	Destination	Protocol
☑	Allow	Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,8
☑	Deny	Default	*,*	LAN,*	*,*
☑	Allow	Default	LAN,*	*,*	*,*

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.

9 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

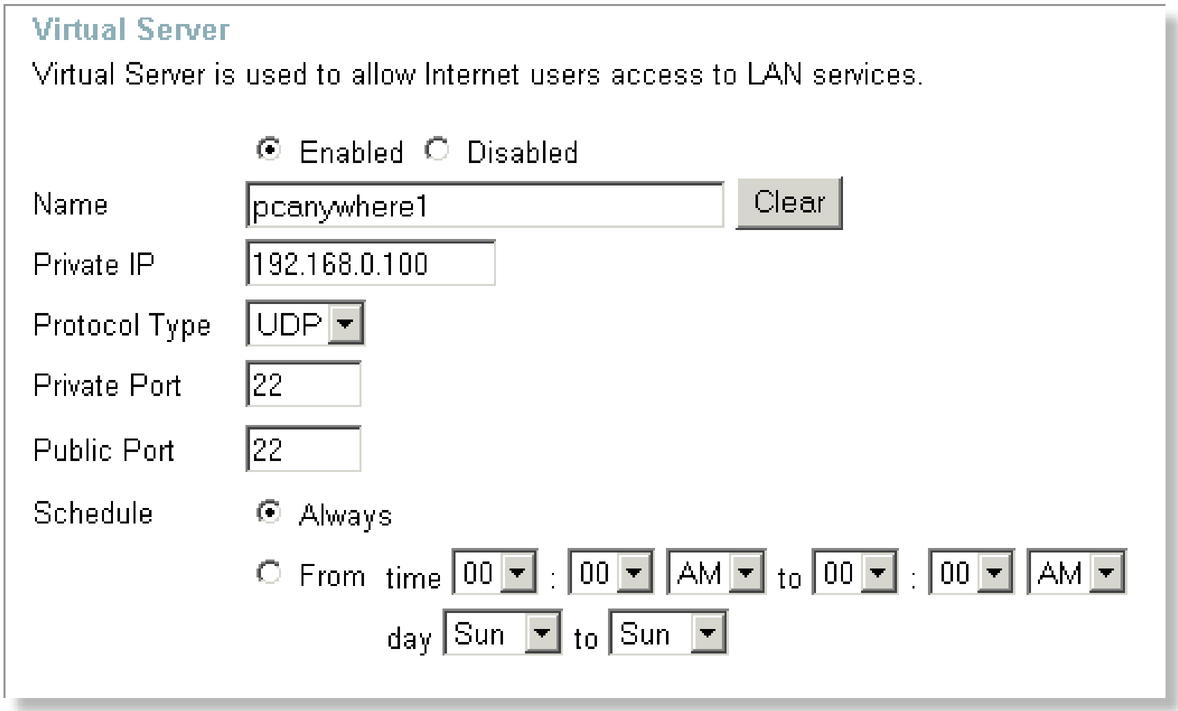
10 How do I use *PC Anywhere* with my DI-624M router?

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.



Virtual Server

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

● Enabled ○ Disabled

Name: pcanywhere1 [Clear]

Private IP: 192.168.0.100

Protocol Type: UDP

Private Port: 22

Public Port: 22

Schedule: ● Always

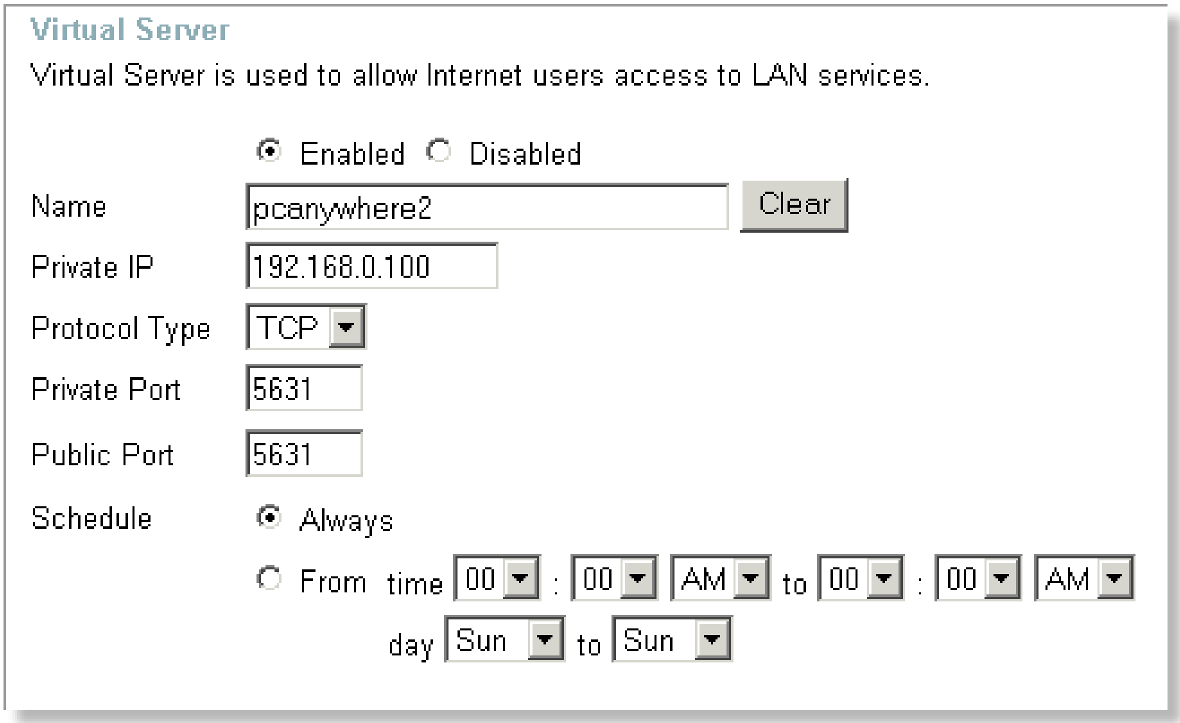
○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

Step 4: The first entry will read as shown above.

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

Step 6: Create a second entry as shown below:



Virtual Server

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

● Enabled ○ Disabled

Name: pcanywhere2 [Clear]

Private IP: 192.168.0.100

Protocol Type: TCP

Private Port: 5631

Public Port: 5631

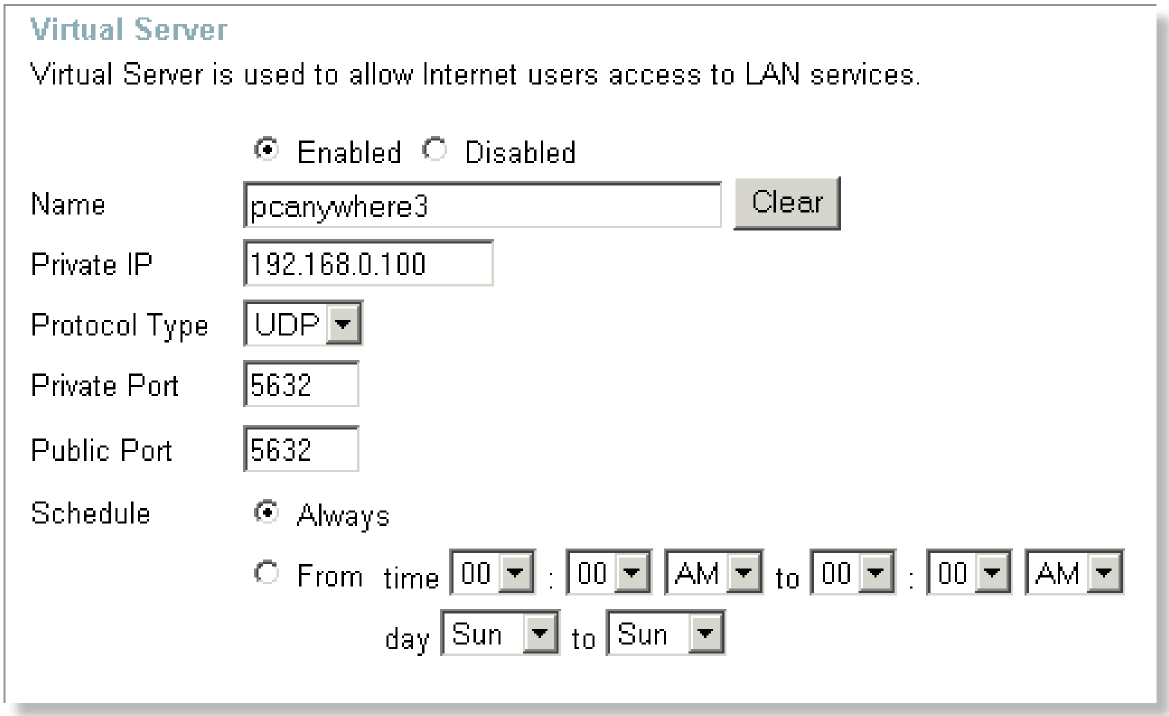
Schedule: ● Always

○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

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

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



Virtual Server

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

	● Enabled ○ Disabled
Name	pcanywhere3
Private IP	192.168.0.100
Protocol Type	UDP
Private Port	5632
Public Port	5632
Schedule	● Always ○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

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.

11 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):

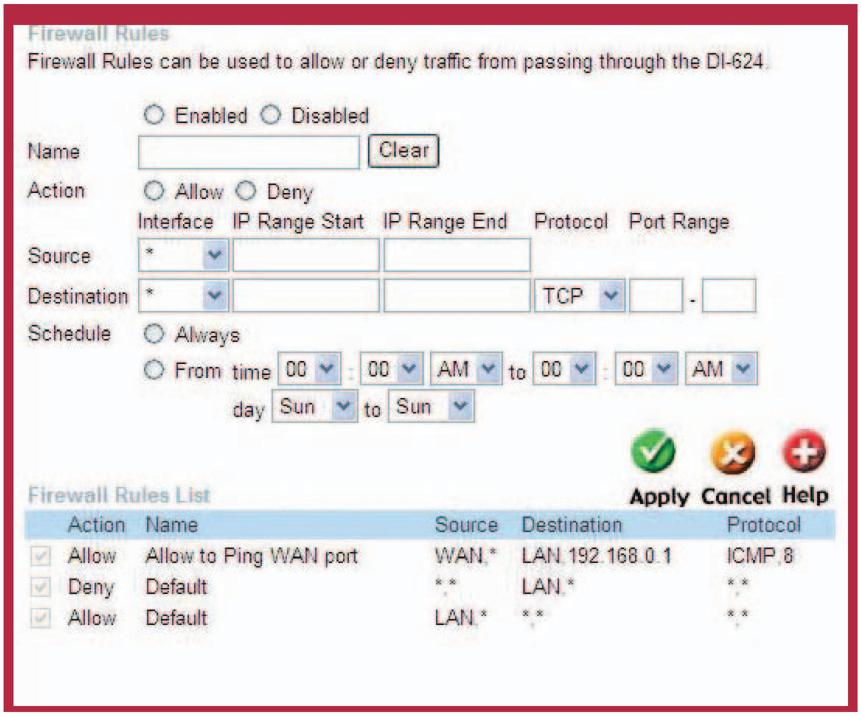
4661 (TCP) To connect with a server

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**.



Firewall Rules

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

	○ Enabled ○ Disabled				
Name	Clear				
Action	○ Allow ○ Deny				
	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	*				
Destination	*			TCP	-
Schedule	○ Always				
	○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun				

Firewall Rules List

	Action	Name	Source	Destination	Protocol
☑	Allow	Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,8
☑	Deny	Default	*,*	LAN,*	*,*
☑	Allow	Default	LAN,*	*,*	*,*

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**.

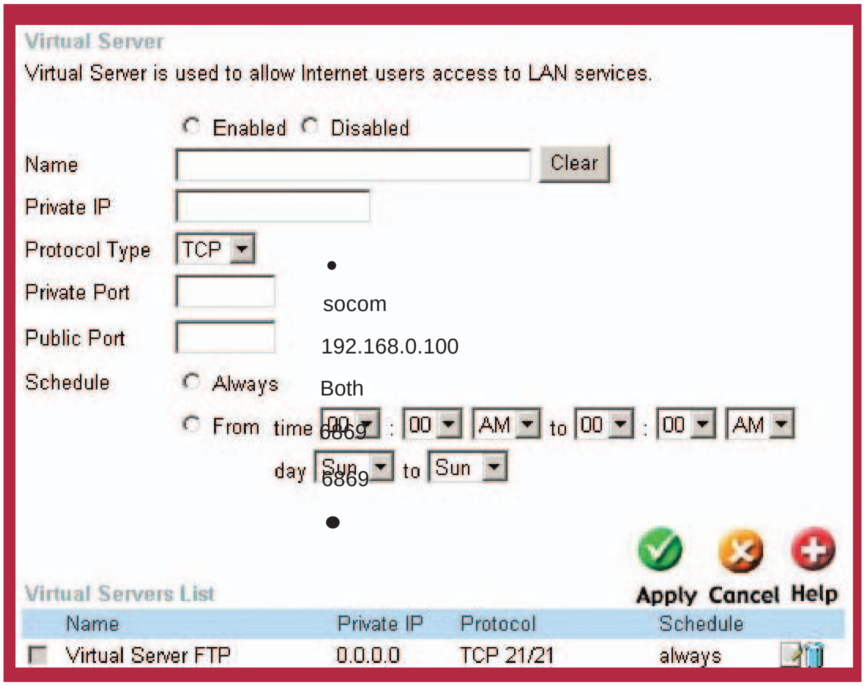
12 How do I set up my router for SOCOM on my Playstation 2?

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.



Virtual Server

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

○ Enabled ○ Disabled

- Name: socom   Clear
- Private IP: 192.168.0.100
- Protocol Type: TCP   Both
- Private Port: 6869
- Public Port: 6869
- Schedule: ○ Always
  ○ From time 00 : 00 AM to 00 : 00 AM
  day Sun to Sun

Virtual Servers List

	Name	Private IP	Protocol	Schedule
□	Virtual Server FTP	0.0.0.0	TCP 21/21	always

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**.

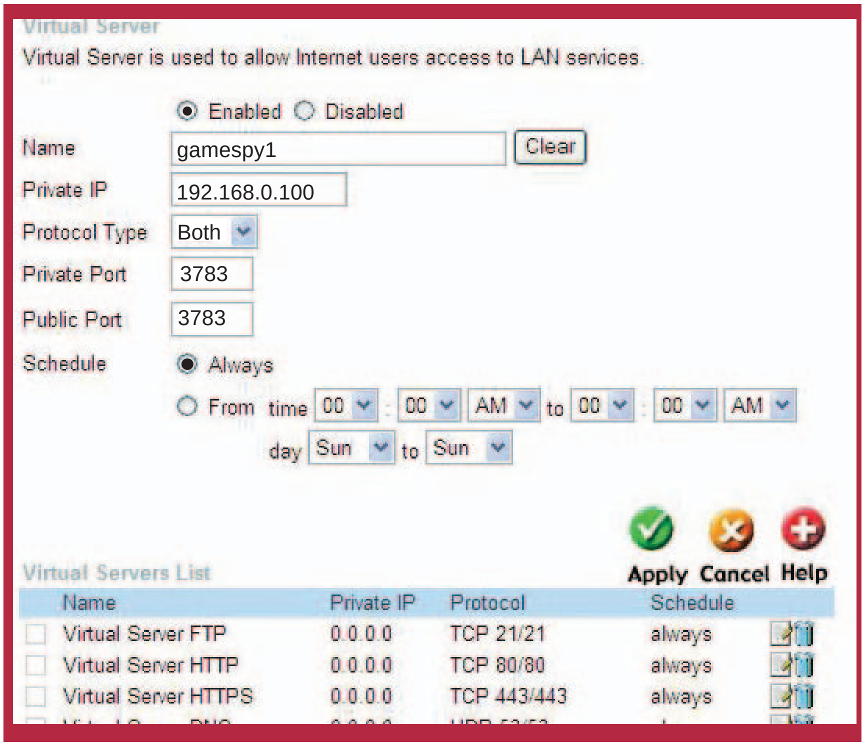
Step 6: Click on the **Tools** tab and then **Misc** on the left side.

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

13 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.



Virtual Server

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

● Enabled ○ Disabled

Name	gamespy1
Private IP	192.168.0.100
Protocol Type	Both
Private Port	3783
Public Port	3783
Schedule	● Always ○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Virtual Servers List

	Name	Private IP	Protocol	Schedule
□	Virtual Server FTP	0.0.0.0	TCP 21/21	always
□	Virtual Server HTTP	0.0.0.0	TCP 80/80	always
□	Virtual Server HTTPS	0.0.0.0	TCP 443/443	always

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.

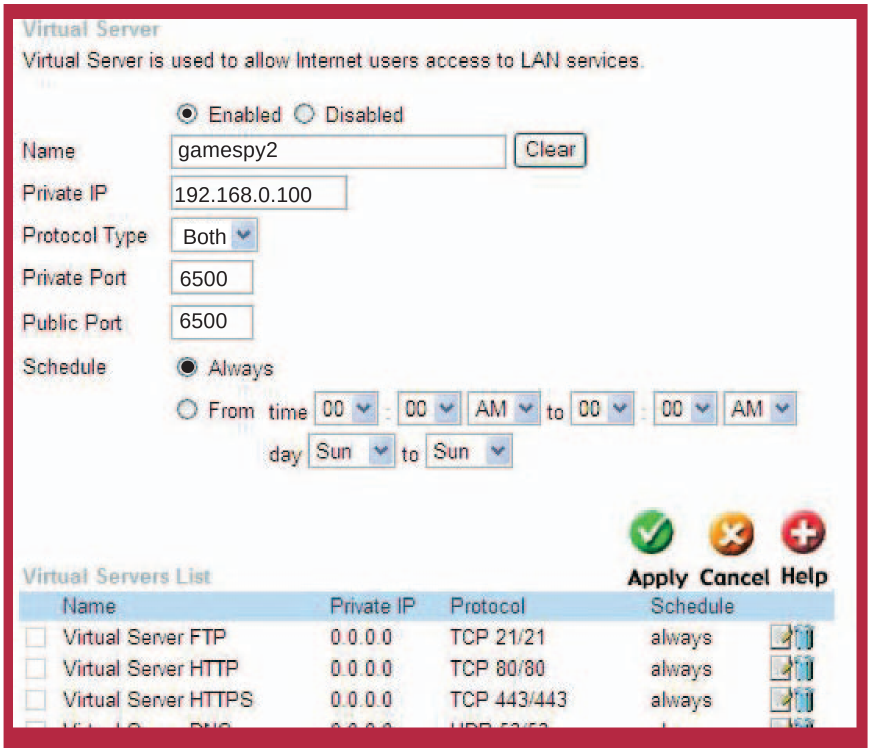
PROTOCOL TYPE - Both

PRIVATE PORT - 3783

PUBLIC PORT - 3783

SCHEDULE - Always.

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



Virtual Server

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

● Enabled ○ Disabled

Name	gamespy2
Private IP	192.168.0.100
Protocol Type	Both
Private Port	6500
Public Port	6500
Schedule	● Always ○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Virtual Servers List

	Name	Private IP	Protocol	Schedule
□	Virtual Server FTP	0.0.0.0	TCP 21/21	always
□	Virtual Server HTTP	0.0.0.0	TCP 80/80	always
□	Virtual Server HTTPS	0.0.0.0	TCP 443/443	always

Step 5: Enter 2nd entry:

Click Enabled.

Enter the following information:

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**.

14 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).

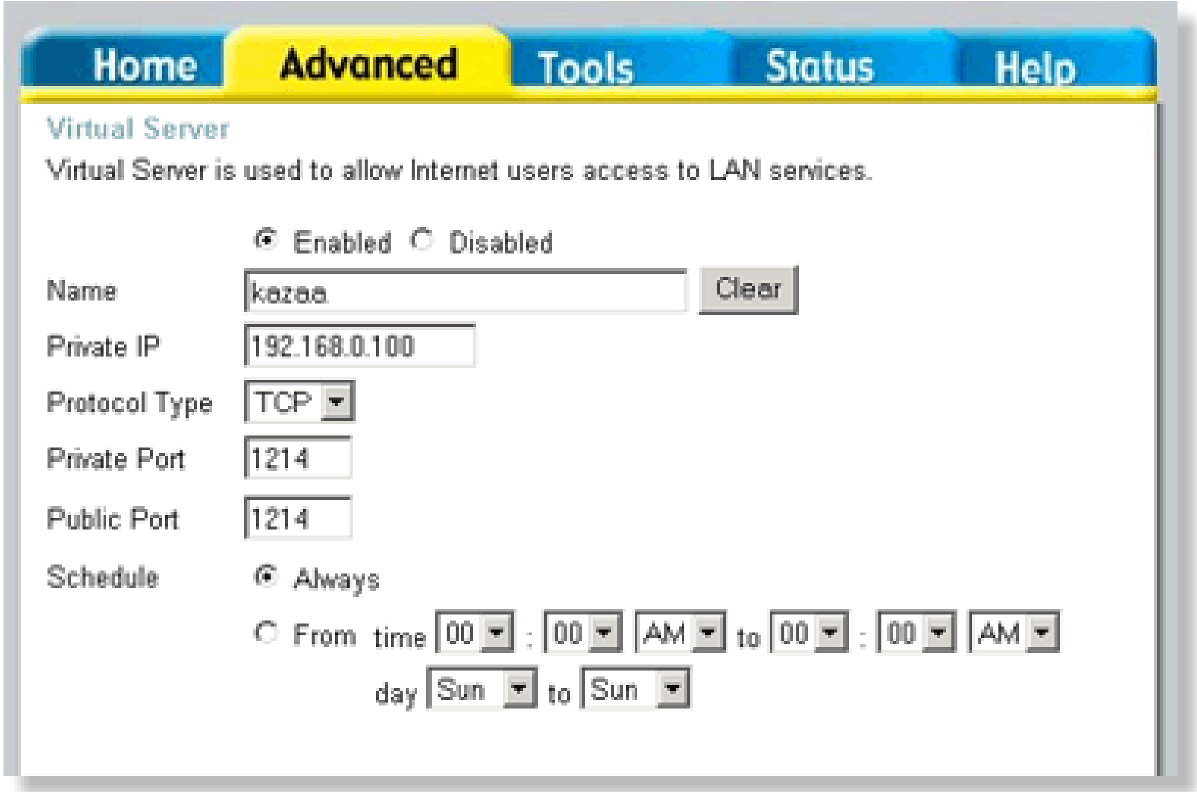
Step 2: Enter your username (admin) and your password (blank by default).

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.



Virtual Server

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

● Enabled ○ Disabled

Name: kazaa

Private IP: 192.168.0.100

Protocol Type: TCP

Private Port: 1214

Public Port: 1214

Schedule: ● Always

○ From time 00 : 00 AM to 00 : 00 AM

day Sun to Sun

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

15 How do I configure my router to play Warcraft 3?

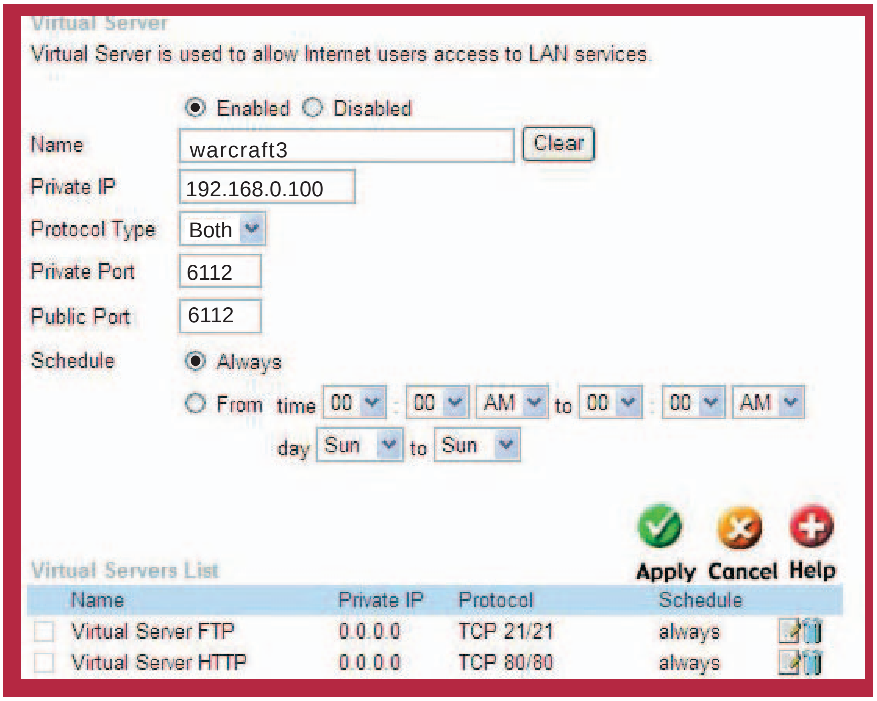
You must open ports on your router to allow incoming traffic while hosting a game in Warcraft 3. To play a game, you do not have to configure your router.

Warcraft 3 (Battlenet) uses port 6112.

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.



Virtual Server

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

● Enabled ○ Disabled

Name	warcraft3 [Clear]
Private IP	192.168.0.100
Protocol Type	Both
Private Port	6112
Public Port	6112
Schedule	● Always ○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Virtual Servers List

	Name	Private IP	Protocol	Schedule
□	Virtual Server FTP	0.0.0.0	TCP 21/21	always
□	Virtual Server HTTP	0.0.0.0	TCP 80/80	always

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.

16 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.

17 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**.

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 *****.

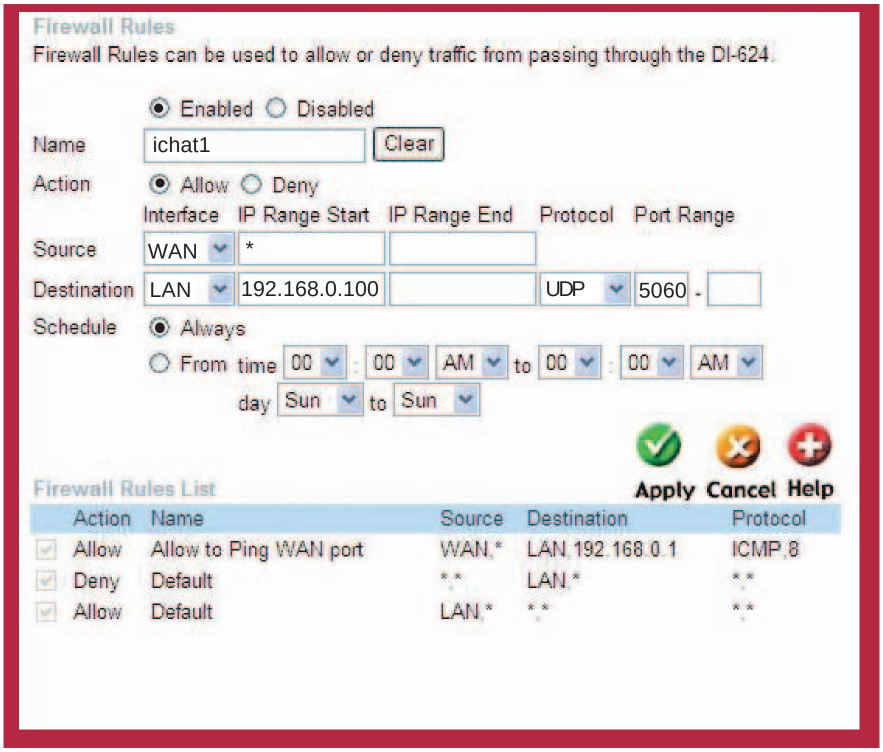
Leave the second box empty.

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.



Firewall Rules

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

● Enabled ○ Disabled

Name ichat1 Clear

Action ● Allow ○ Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	WAN	*			
Destination	LAN	192.168.0.100		UDP	5060 -

Schedule ● Always

○ From time 00 : 00 AM to 00 : 00 AM

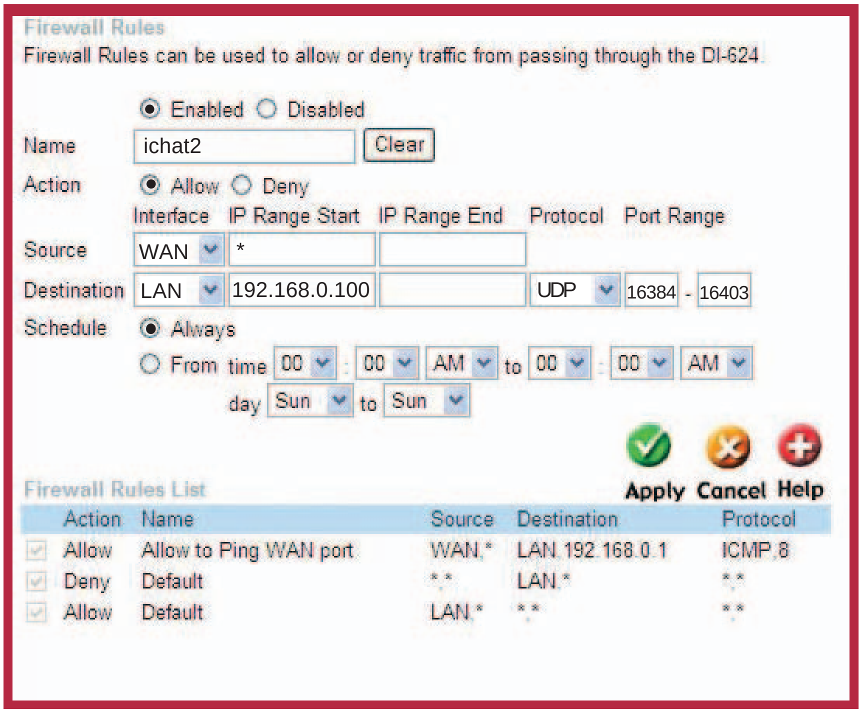
day Sun to Sun

Firewall Rules List

	Action	Name	Source	Destination	Protocol
☑	Allow	Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,8
☑	Deny	Default	*,*	LAN,*	*,*
☑	Allow	Default	LAN,*	*,*	*,*

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

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



Firewall Rules

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

● Enabled ○ Disabled

Name: ichat2 [Clear]

Action: ● Allow ○ Deny

	Interface	IP Range Start	IP Range End	Protocol	Port Range
Source	WAN	*			
Destination	LAN	192.168.0.100		UDP	16384 - 16403

Schedule: ● Always
○ From time 00 : 00 AM to 00 : 00 AM
day Sun to Sun

Firewall Rules List

	Action	Name	Source	Destination	Protocol
☑	Allow	Allow to Ping WAN port	WAN,*	LAN,192.168.0.1	ICMP,8
☑	Deny	Default	*,*	LAN,*	*,*
☑	Allow	Default	LAN,*	*,*	*,*

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).

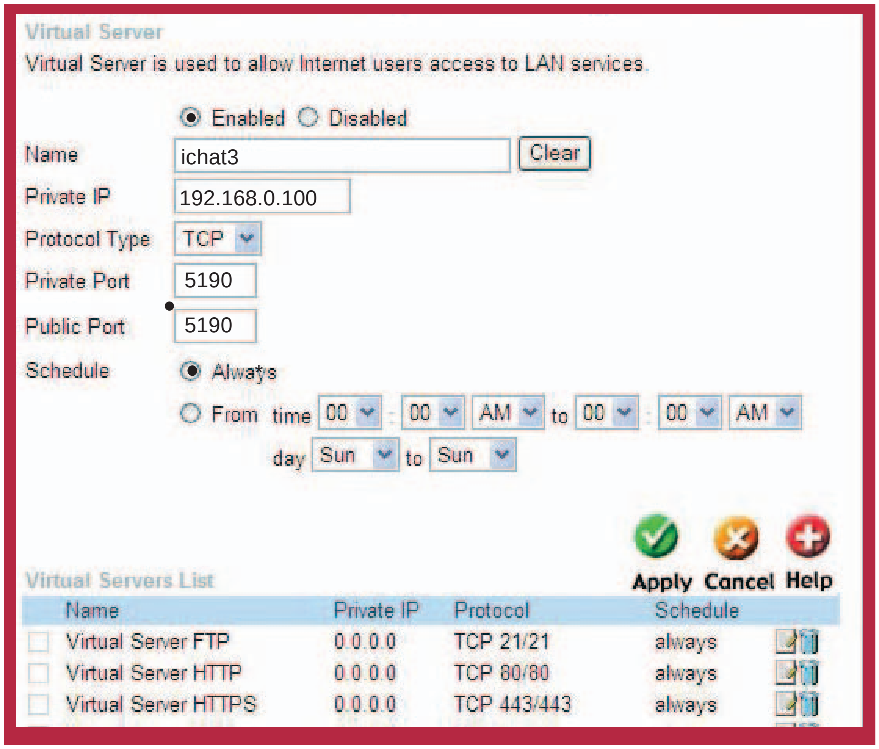
Step 4: Next to Private IP, enter the IP Address of the computer on your local network that you want to allow the incoming service to.

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

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

Step 7: Click **Always** or configure a schedule.

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



Virtual Server

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

● Enabled ○ Disabled

Name	ichat3
Private IP	192.168.0.100
Protocol Type	TCP
Private Port	5190
Public Port	5190
Schedule	● Always ○ From time 00 : 00 AM to 00 : 00 AM day Sun to Sun

Virtual Servers List

	Name	Private IP	Protocol	Schedule
□	Virtual Server FTP	0.0.0.0	TCP 21/21	always
□	Virtual Server HTTP	0.0.0.0	TCP 80/80	always
□	Virtual Server HTTPS	0.0.0.0	TCP 443/443	always

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**.

17 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.

18 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-624M) 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.

Appendix

Securing Your Network

1. **Change Admin Password**

Changing the password to access your new router is the first step in securing your network. This can done through the Wizard or on the Admin Page of the Tools tab. There is no password by default and hackers will know this when trying to access your network. Make sure that the password you choose is not commonly known or something that is easy to guess such as your last name or your pet's name. Try using a combination of letters and numbers to deter intruders from hacking into your network. Your private information should be kept private.

2. **Disable DHCP and use Static IP addresses or Use Static DHCP and limit scope to the amount of users on your network.**

In the event that an intruder manages to gain access to your network, having DHCP enabled makes it easier for the intruder to access other computers on your network. There are two methods for getting around this. One is to disable DHCP and use static IP addressing on all the devices connected to your network. This would mean that the intruder would have to know what IP network your devices are on in order to access them. The second way is to change the scope of the DHCP server to only include enough IP addresses for the devices in your network. You can then use the Static DHCP feature of the router to assign an IP address to each device on your network. Static DHCP still dynamically assigns an IP address to your network devices but only allows for those defined devices to obtain an IP address.

3. **Change the default LAN IP address**

Change the default LAN IP address from 192.168.0.1 to an alternate IP address. There are 3 ranges of IP addresses that have been reserved for use on Private Networks.

10.0.0.0	**-**	**10.255.255.255 (10.0.0.0/8)**
172.16.0.0	**-**	**172.31.255.255 (172.16.0.0/12)**
192.168.0.0	**-**	**192.168.255.255 (192.168.0.0/16)**

D-Link routers use 192.168.0.1 as their default LAN IP address. Choosing an alternate IP address lessens the probabilty of an intruders knowing what IP network your devices are on.

4. **Set up MAC Filtering**

Each networking device (router, network card, etc) on a network contains a unique hexadecimal number that identifies that specific product. This number is referred to as a MAC address. MAC filtering allows you to create a list of the MAC address of each device on your network and only allows these specific devices to associate with your network. With this feature enabled, devices attempting to connect to your network with a MAC address that is not in the list you created, will be denied access.

Glossary

A

Access Control List - ACL. Database of network devices that are allowed to access resources on the network.

Access Point - AP. Device that allows wireless clients to connect to it and access the network

Ad-hoc network - Peer-to-Peer network between wireless clients

Address Resolution Protocol - ARP. Used to map MAC addresses to IP addresses so that conversions can be made in both directions.

ADSL - Asymmetric Digital Subscriber Line

Advanced Encryption Standard - AES. Government encryption standard

Alphanumeric - Characters A-Z and 0-9

Antenna - Used to transmit and receive RF signals.

AppleTalk – A set of Local Area Network protocols developed by Apple for their computer systems

AppleTalk Address Resolution Protocol – AARP. Used to map the MAC addresses of Apple computers to their AppleTalk network addresses, so that conversions can be made in both directions.

Application layer - 7th Layer of the OSI model. Provides services to applications to ensure that they can communicate properly with other applications on a network.

ASCII - American Standard Code for Information Interchange. This system of characters is most commonly used for text files

Attenuation – The loss in strength of digital an analog signals. The loss is greater when the signal is being transmitted over long distances.

Authentication –To provide credentials, like a Password, in order to verify that the person or device is really who they are claiming to be

Automatic Private IP Addressing - APIPA. An IP address that a Windows computer will assign itself when it is configured to obtain an IP address automatically but no DHCP server is available on the network

B

Backward Compatible - The ability for new devices to communicate and interact with older legacy devices to guarantee interoperability

Bandwidth - The maximum amount of bytes or bits per second that can be transmitted to and from a network device

Basic Input/Output System – BIOS. A program that the processor of a computer uses to startup the system once it is turned on

Baud – Data transmission speed

Bit rate – The amount of bits that pass in given amount of time

bit/sec – bits per second

BOOTP – Bootstrap Protocol. Allows for computers to be booted up and given an IP address with no user intervention

Bottleneck – A time during processes when something causes the process to slowdown or stop all together

Broadband – A wide band of frequencies available for transmitting data

Broadcast – Transmitting data in all directions at once

Browser – A program that allows you to access resources on the web and provides them to you graphically

C

Cable modem – A device that allows you to connect a computer up to a coaxial cable and receive Internet access from your Cable provider

CardBus – A newer version of the PC Card or PCMCIA interface. It supports a 32-bit data path, DMA, and consumes less voltage

Carrier Sense Multiple Access/Collision Avoidance – CSMA/CA

Carrier Sense Multiple Access/Collision Detect – CSMA/CD

CAT 5 – Category 5. Used for 10/100 Mbps or 1Gbps Ethernet connections

Client – A program or user that requests data from a server

Collision – When do two devices on the same Ethernet network try and transmit data at the exact same time.

Cookie – Information that is stored on the hard drive of your computer that holds your preferences to the site that gave your computer the cookie

CSMA/CA – Carrier Sense Multiple Access/Collision Avoidance

CSMA/CD – Carrier Sense Multiple Access/Collision Detection

D

Data – Information that has been translated into binary do that it can be processed or moved to another device

Data Encryption Standard – Uses a randomly selected 56-bit key that must be known by both the sender and the receiver when information is exchanged

Data-Link layer – The second layer of the OSI model. Controls the movement of data on the physical link of a network

Database – Organizes information so that it can be managed updated, as well as easily accessed by users or applications

DB-25 – A 25 ping male connector for attaching External modems or RS-232 serial devices

DB-9 – A 9 pin connector for RS-232 connections

dBd - decibels related to dipole antenna

dBi - decibels relative to isotropic radiator

dBm - decibels relative to one milliwatt

Decrypt – To unscramble an encrypted message back into plain text

Default – A predetermined value or setting that is used by a program when no user input has been entered for this value or setting

Demilitarized zone – DMZ. A single computer or group of computers that can be accessed by both users on the Internet as well as users on the Local Network, but that is not protected by the same security as the Local Network.

DHCP – Dynamic Host Configuration Protocol. Used to automatically assign IP addresses from a predefined pool of addresses to computers or devices that requests them

Digital certificate – An electronic method of providing credentials to a server in order to have access to it or a network

Direct Sequence Spread Spectrum – DSSS. Modulation technique used by 802.11b wireless devices

DNS – Domain Name System. Translates Domain Names to IP addresses

DOCSIS – Data Over Cable Service Interface Specifications. The standard interface for cable modems

Domain name – A name that is associated with an IP address

Download – To send a request from one computer to another and have the file transmitted back to the requesting computer

DSL – Digital Subscriber Line. High bandwidth Internet connection over telephone lines

Duplex – Sending and Receiving data transmissions at the sane time

Dynamic DNS service – DDNS is provided by companies to allow users with Dynamic IP addresses to obtain a Domain Name that will always by linked to their changing IP address. The IP address is updated by either client software running on a computer or by a router that supports DDNS, whenever the IP address changes.

Dynamic IP address – IP address that is assigned by a DHCP server and that may change. Cable Internet providers usually use this method to assign IP addresses to their customers.

E

EAP – Extensible Authentication Protocol

Email – Electronic Mail is a computer-stored message that is transmitted over the Internet

Encryption – Converting data into cyphertext so that it cannot be easily read

Enterprise – Large organizations that use computers

Ethernet – The most widely used technology for Local Area Networks.

F

Fiber optic – A way of sending data through light impulses over glass or plastic wire or fiber

File server – A computer on a network that stores data so that the other computers on the network can all access it

File sharing – Allowing data from computers on a network to be accessed by other computers on the network will different levels of access rights

Firewall – A device that protects resources of the Local Area Network from unauthorized users outside of the local network

Firmware – Programming that is inserted into a hardware device that tells it how to function

Fragmentation – Breaking up data into smaller pieces to make it easier to store

FTP – File Transfer Protocol. Easiest way to transfer files between computers on the Internet

Full-duplex – Sending and Receiving data at the same time

G

Gain – The amount an amplifier boosts the wireless signal

Gateway – A device that connects your network to another, like the internet

Gbps – Gigabits per second

Gigabit Ethernet – Transmission technology that provides a data rate of 1 billion bits per second

Graphical user interface – GUI

H

H.323 – A standard that provides consistency of voice and video transmissions and compatibility for videoconferencing devices

Half-duplex – Data cannot be transmitted and received at the same time

Hashing – Transforming a string of characters into a shorter string with a predefined length

Hexadecimal – Characters 0-9 and A-F

HomePNA – Networking over telephone lines

HomeRF – Networking standard that combines 802.11b and DECT (digital Enhanced Cordless Telecommunication) that provides speeds up to 1.6 Mbps and a distance of 150 ft using a Frequency Hopping transmission method

Hop – The action of data packets being transmitted from one router to another

Host – Computer on a network

HTTP – Hypertext Transfer Protocol is used to transfer files from HTTP servers (web servers) to HTTP clients (web browsers)

HTTPS – HTTP over SSL is used to encrypt and decrypt HTTP transmissions

Hub – A networking device that connects multiple devices together

I

ICMP – Internet Control Message Protocol

IEEE – Institute of Electrical and Electronics Engineers

IETF – Internet Engineering Task Force

IGMP – Internet Group Management Protocol is used to make sure that computers can report their multicast group membership to adjacent routers

IIS – Internet Information Server is a WEB server and FTP server provided by Microsoft

IKE – Internet Key Exchange is used to ensure security for VPN connections

Infrastructure – In terms of a wireless network, this is when wireless clients use an Access Point to gain access to the network

Internet – A system of worldwide networks which use TCP/IP to allow for resources to be accessed from computers around the world

Internet Explorer – A World Wide Web browser created and provided by Microsoft

Internet Protocol – The method of transferring data from one computer to another on the Internet

Internet Protocol Security – IPsec provides security at the packet processing layer of network communication

Internet Service Provider – An ISP provides access to the Internet to individuals or companies

Interoperability – The ability for products to interact with other products without much customer interaction

Intranet – A private network

Intrusion Detection – A type of security that scans a network to detect attacks coming from inside and outside of the network

IP – Internet Protocol

IP address – A 32-bit number, when talking about Internet Protocol Version 4, that identifies each computer that transmits data on the Internet or on an Intranet

IPsec **–** Internet Protocol Security

IPv6 **–** Internet Protocol Version 6 uses 128-bit addresses and was developed to solve the problem that we face of running our of IP version 4 addresses

IPX **–** Internetwork Packet Exchange is a networking protocol developed by Novel to enable their Netware clients and servers to communicate

ISP **–** Internet Service Provider

J

Java **–** A programming language used to create programs and applets for web pages

K

Kbps **–** Kilobits per second

Kbyte **-** Kilobyte

Kerberos **–** A method of securing and authenticating requests for services on a network

L

LAN **–** Local Area Network

Latency – The amount of time that it takes a packet to get from the one point to another on a network. Also referred to as delay

LED - Light Emitting Diode

Legacy – Older devices or technology

Local Area Network – A group of computers in a building that usually access files from a server

M

MAC address – A unique hardware address for devices on a Local Area Network

MDI – Medium Dependent Interface is an Ethernet port for a connection to a straight-through cable

MDIX - Medium Dependent Interface Crossover, is an Ethernet port for a connection to a crossover cable

Megabit - Mb

Megabyte - MB

Megabits per second - Mbps

MIB – Management Information Base is a set of objects that can be managed by using SNMP

Modem – A device that Modulates digital signals from a computer to an analog signal in order to transmit the signal over phone lines. It also Demodulates the analog signals coming from the phone lines to digital signals for your computer

MPPE – Microsoft Point-to-Point Encryption is used to secure data transmissions over PPTP connections

MTU – Maximum Transmission Unit is the largest packet that can be transmitted on a packet-based network like the Internet

Multicast – Sending data from one device to many devices on a network

N

NAT – Network Address Translation allows many private IP addresses to connect to the Internet, or another network, through one IP address

NetBEUI – NetBIOS Extended User Interface is a Local Area Network communication protocol. This is an updated version of NetBIOS

NetBIOS – Network Basic Input/Output System

Netmask – Determines what portion of an IP address designates the Network and which part designates the Host

NetWare – A Server Software developed by Novell

Network Interface Card – A card installed in a computer or built onto the motherboard that allows the computer to connect to a network

Network later – The third layer of the OSI model which handles the routing of traffic on a network

Network Time Protocol – Used to synchronize the time of all the computers in a network

NIC – Network Interface Card

NTP – Network Time Protocol

O

OFDM – Orthogonal Frequency-Division Multiplexing is the modulation technique for both 802.11a and 802.11g

OSI – Open Systems Interconnection is the reference model for how data should travel between two devices on a network

OSPF – Open Shortest Path First is a routing protocol that is used more than RIP in larger scale networks because only changes to the routing table are sent to all the other routers in the network as opposed to sending the entire routing table at a regular interval, which is how RIP functions

P

Password - A sequence of characters that is used to authenticate requests to resources on a network

Personal Area Network – The interconnection of networking devices within a range of 10 meters

Physical layer – The first layer of the OSI model. Provides the hardware means of transmitting electrical signals on a data carrier

PoE – Power over Ethernet is the means of transmitting electricity over the unused pairs in a category 5 Ethernet cable

POP 3 – Post Office Protocol 3 is used for receiving email

PPP – Point-to-Point Protocol is used for two computers to communicate with each over a serial interface, like a phone line

PPPoE – Point-to-Point Protocol over Ethernet is used to connect multiple computers to a remote server over Ethernet

PPTP – Point-to-Point Tunneling Protocol is used for creating VPN tunnels over the Internet between two networks

Preamble – Used to synchronize communication timing between devices on a network

Q

QoS – Quality of Service

R

RADIUS – Remote Authentication Dial-In User Service allows for remote users to dial into a central server and be authenticated in order to access resources on a network

Rendezvous – Apple's version of UPnP, which allows for devices on a network to discover each other and be connected without the need to configure any settings

Repeater – Retransmits the signal of an Access Point in order to extend it's coverage

RIP – Routing Information Protocol is used to synchronize the routing table of all the routers on a network

RJ-11 – The most commonly used connection method for telephones

RJ-45 - The most commonly used connection method for Ethernet

RS-232C – The interface for serial communication between computers and other related devices

RSA – Algorithm used for encryption and authentication

S

Samba – A freeware program that allows for resources to be shared on a network. Mainly used in Unix based Operating Systems

Server – A computer on a network that provides services and resources to other computers on the network

Session key – An encryption and decryption key that is generated for every communication session between two computers

Session layer – The fifth layer of the OSI model which coordinates the connection and communication between applications on both ends

Simple Mail Transfer Protocol – Used for sending and receiving email

Simple Network Management Protocol – Governs the management and monitoring of network devices

SMTP – Simple Mail Transfer Protocol

SNMP – Simple Network Management Protocol

SOHO – Small Office/Home Office

SPI – Stateful Packet Inspection

SSH – Secure Shell is a command line interface that allows for secure connections to remote computers

SSID – Service Set Identifier is a name for a wireless network

Stateful inspection – A feature of a firewall that monitors outgoing and incoming traffic to make sure that only valid responses to outgoing requests for incoming packets are allowed to pass though the firewall

Subnet mask – Determines what portion of an IP address designates the Network and which part designates the Host

T

TCP – Transmission Control Protocol

TCP/IP – Transmission Control Protocol/Internet Protocol

TFTP – Trivial File Transfer Protocol is a utility used for transferring files that is simpler to use than FTP but with less features

Throughput – The amount of data that can be transferred in a given time period

Traceroute – A utility displays the routes between you computer and specific destination

U

UDP – User Datagram Protocol

UNC – Universal Naming Convention allows for shares on computers to be identified without having to know what storage device it's on

Unicast – Communication between a single sender and receiver

Universal Plug and Play – A standard that allows network devices to discover each other and configure themselves to be a part of the network

UPnP – Universal Plug and Play

URL – Uniform Resource Locator is a unique address for files accessible on the Internet

UTP – Unshielded Twisted Pair

V

Virtual LAN -

Virtual Private Network – A secure tunnel over the Internet to connect remote offices or users to their company's network

VLAN – Virtual LAN

Voice over IP – Sending voice information over the Internet as opposed to the PSTN

VoIP – Voice over IP

W

Wake on LAN – Allows you to power up a computer though it's Network Interface Card

WAN – Wide Area Network

Web browser – A utility that allows you to view content and interact will all of the information on the World Wide Web

WEP – Wired Equivalent Privacy is security for wireless networks that is supposed to be comparable to that of a wired network

Wi-Fi – Wireless Fidelity

Wi-Fi Protected Access – An updated version of security for wireless networks that provides authentication as well as encryption

Wide Area Network - A network spanning a large geographical area or consisting of more than one LAN.

Wireless ISP – A company that provides a broadband Internet connection over a wireless connection

Wireless LAN – Connecting to a Local Area Network over one of the 802.11 wireless standards

WISP – Wireless Internet Service Provider

WLAN – Wireless Local Area Network

Y

Yagi antenna – A directional antenna used to concentrate wireless signals on a specific location

Contacting 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 8:30am to 9:00pm 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 for its product only to the person or entity that originally purchased the product from:

- D-Link or its authorized reseller or distributor and

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

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

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

- Hardware (excluding power supplies and fans) One (1) Year

- Power Supplies and Fans One (1) Year

- Spare parts and spare kits Ninety (90) days

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

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

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

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

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

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

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

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

· Return Merchandise Ship-To Address

USA: 17595 Mt. Herrmann, Fountain Valley, CA 92708

Canada: 2180 Winston Park Drive, Oakville, ON, L6H 5W1 (Visit http://www.dlink.ca for detailed warranty information within Canada)

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

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

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

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

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

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

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

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

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

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

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

FCC Caution:

The manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment; such modifications could void the user's authority to operate the equipment.

(1) The devices are restricted to indoor operations within the 5.15 to 5.25GHz range. (2) For this device to operate in the 5.15 to 5.25GHz range, the devices must use integral antennas.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE:

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. The antenna(s) used for this equipment must be installed to provide a separation distance of at least eight inches (20 cm) from all persons.

This equipment must not be operated in conjunction with any other antenna.

Registration

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

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

(12/27/04)