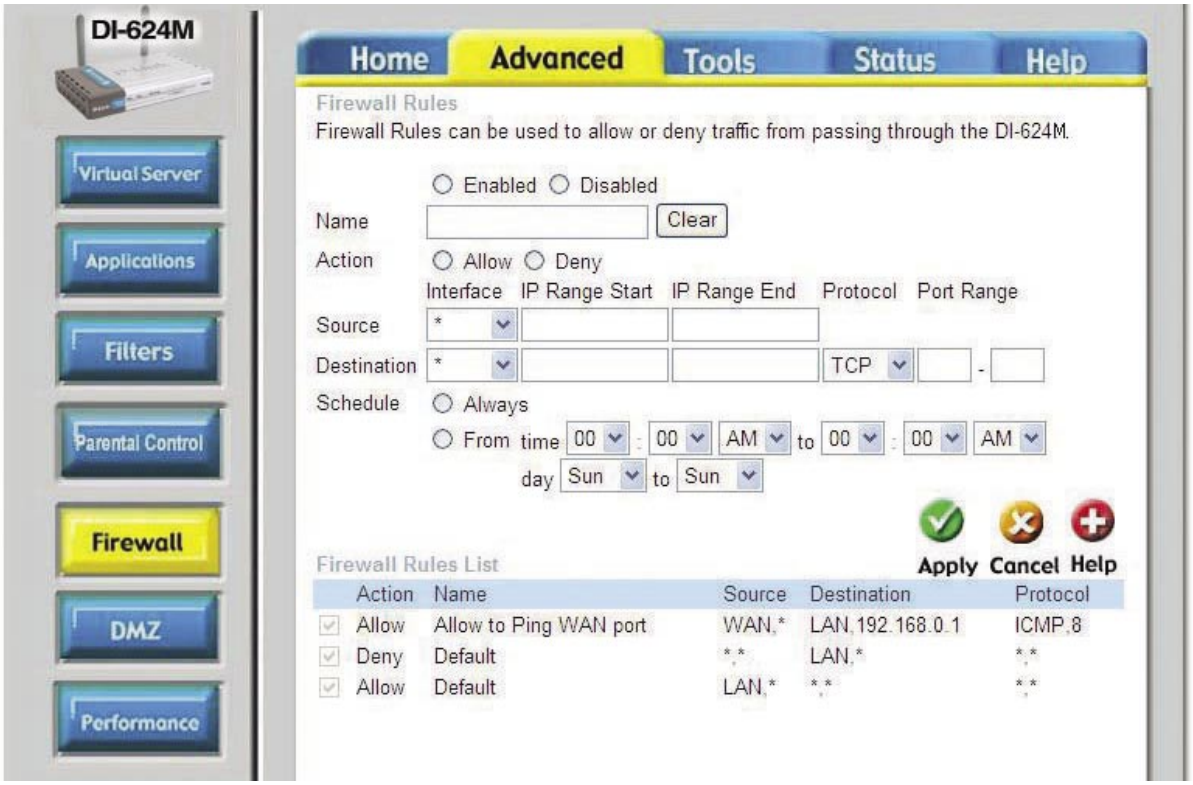
8 How do I open a range of ports on my DI-624M using Firewall rules?

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.



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:

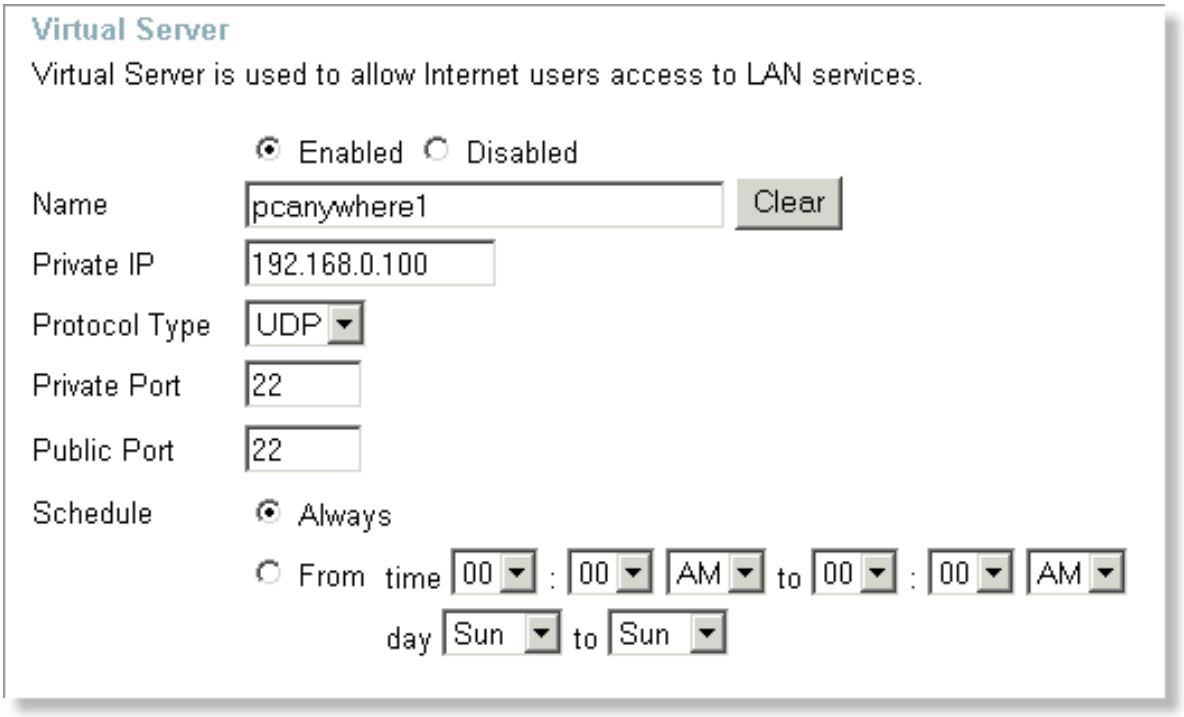
Server Port	Server IP	Enable
21	192.168.0.5	X
80	192.168.0.6	X
1723	192.168.0.7	X

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).

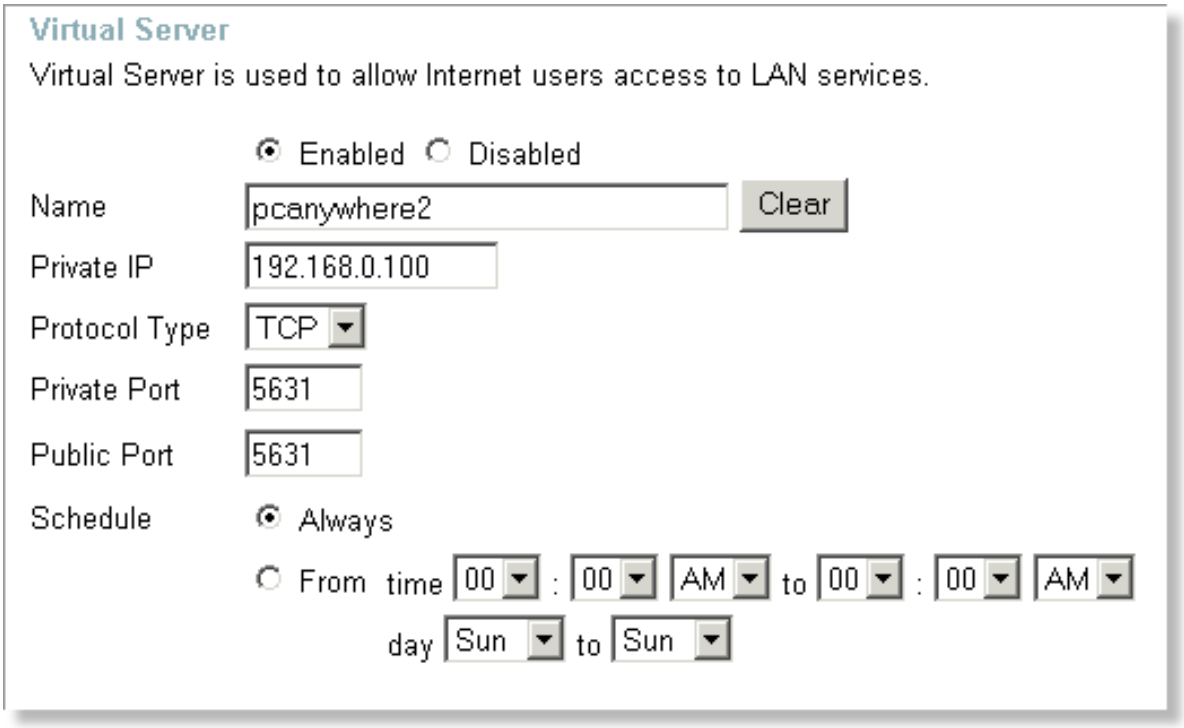
Step 3: Enter the information as seen below. The **Private IP** is the IP Address of the computer on your local network that you want to connect to.



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

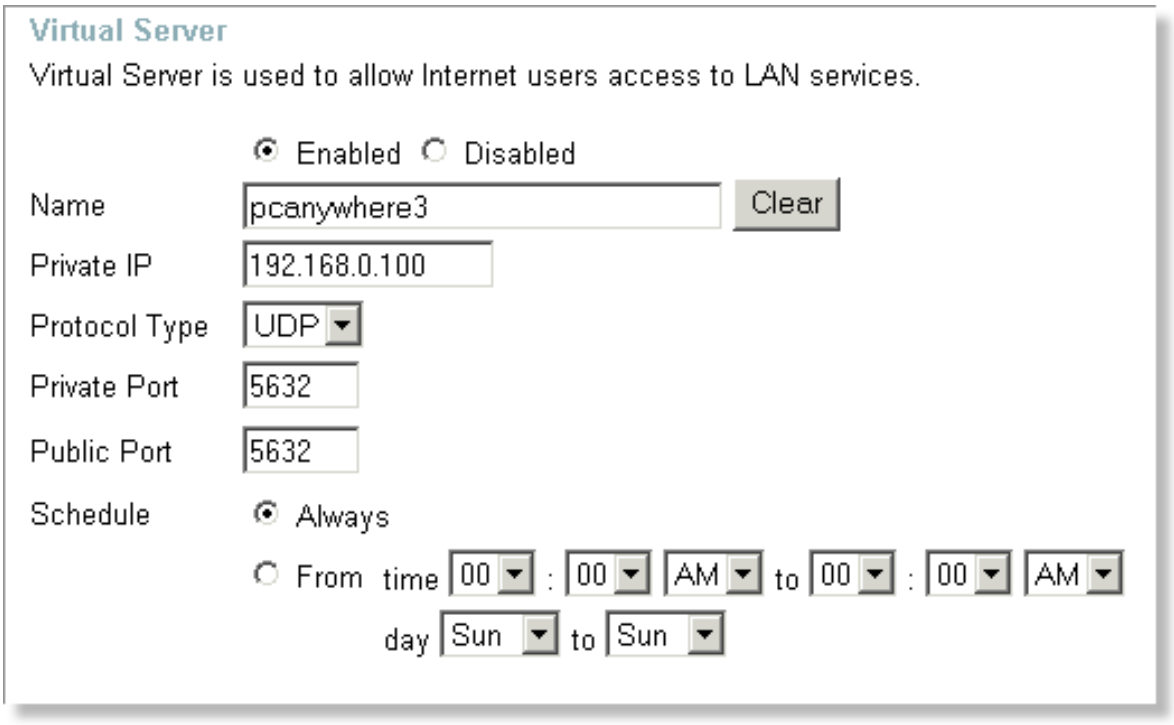
Step 5: Click **Apply** and then click **Continue**.

Step 6: Create a second entry as shown below:



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

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



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):

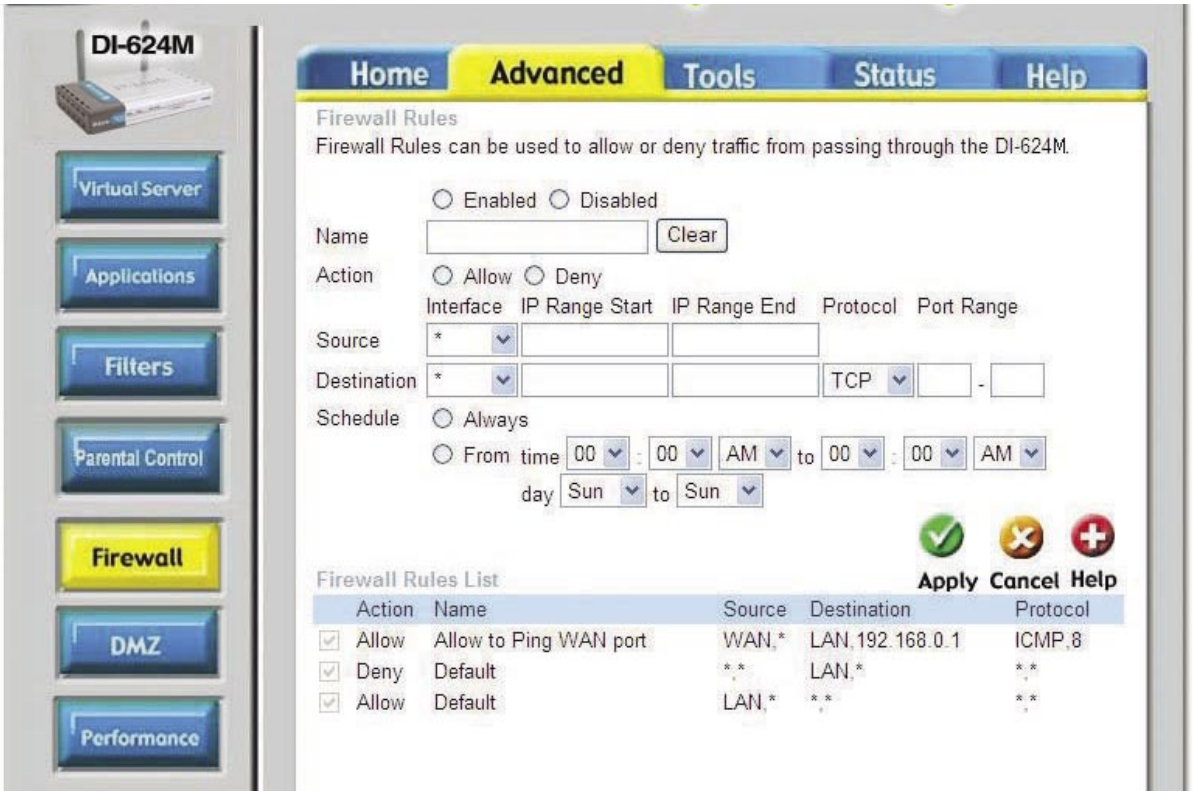
4661 (TCP) To connect with a server

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**.



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**.

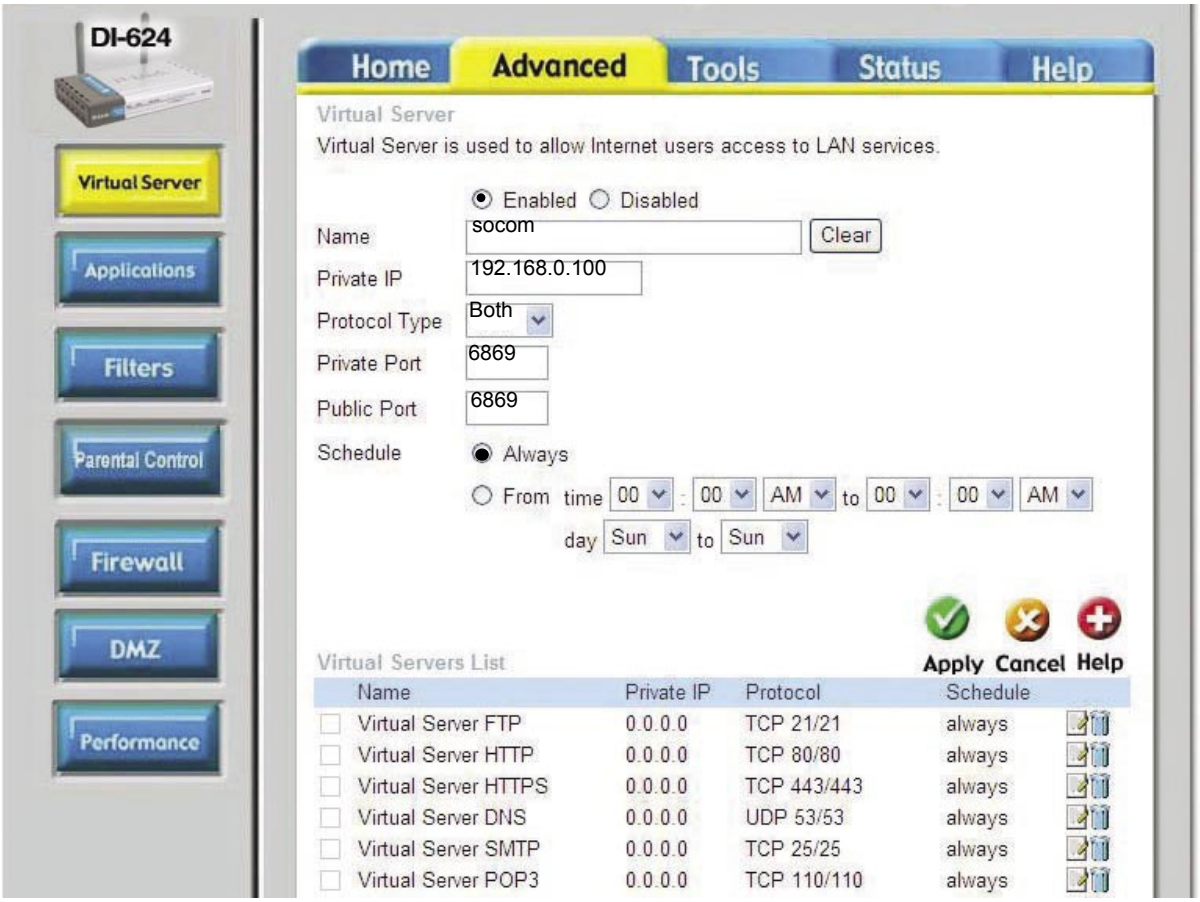
12 How do I set up my router for SOCOM on my Playstation 2?

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.



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**.

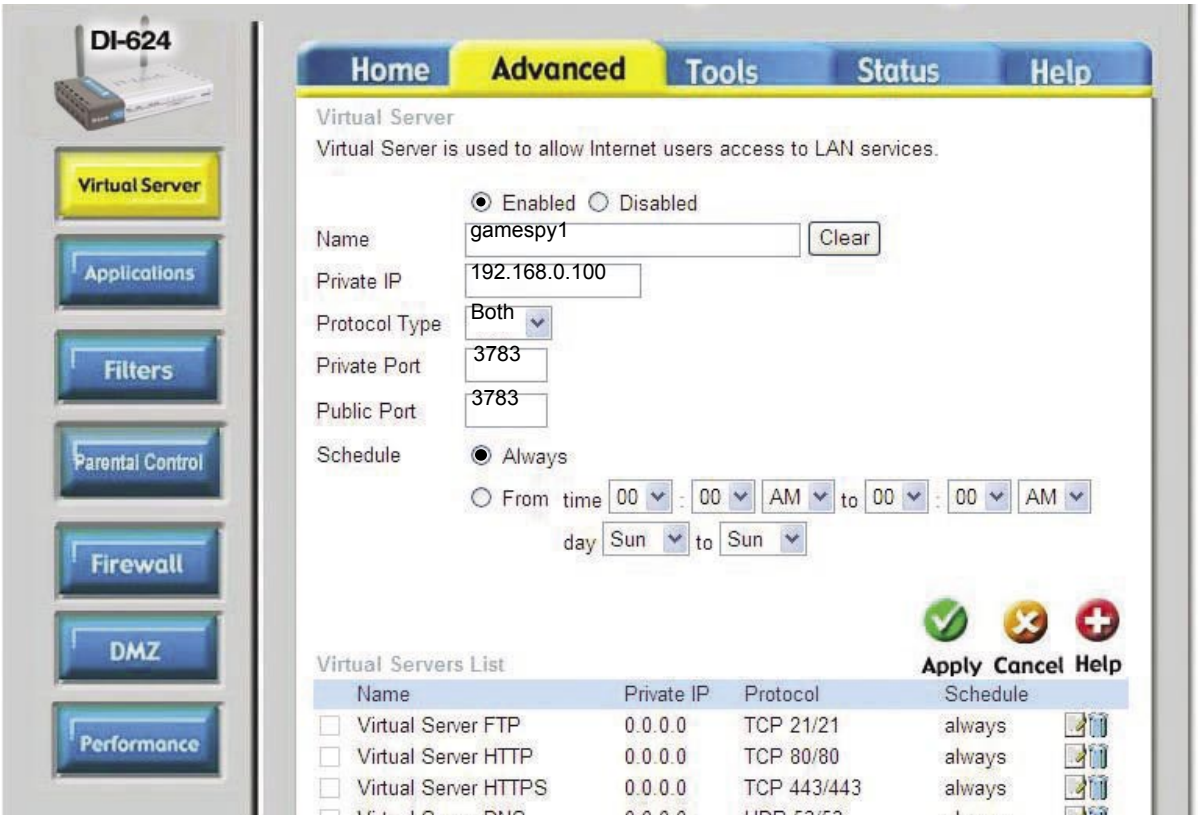
Step 5: For **Protocol Type** select Both. Enter **6869** for both the **Private Port** and **Public Port**. Click **Always**. Click **Apply** to save changes and then **Continue**.

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 3: You will create 2 entries.

Step 4: Click Enabled and enter Settings:

NAME - Gamespy1

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

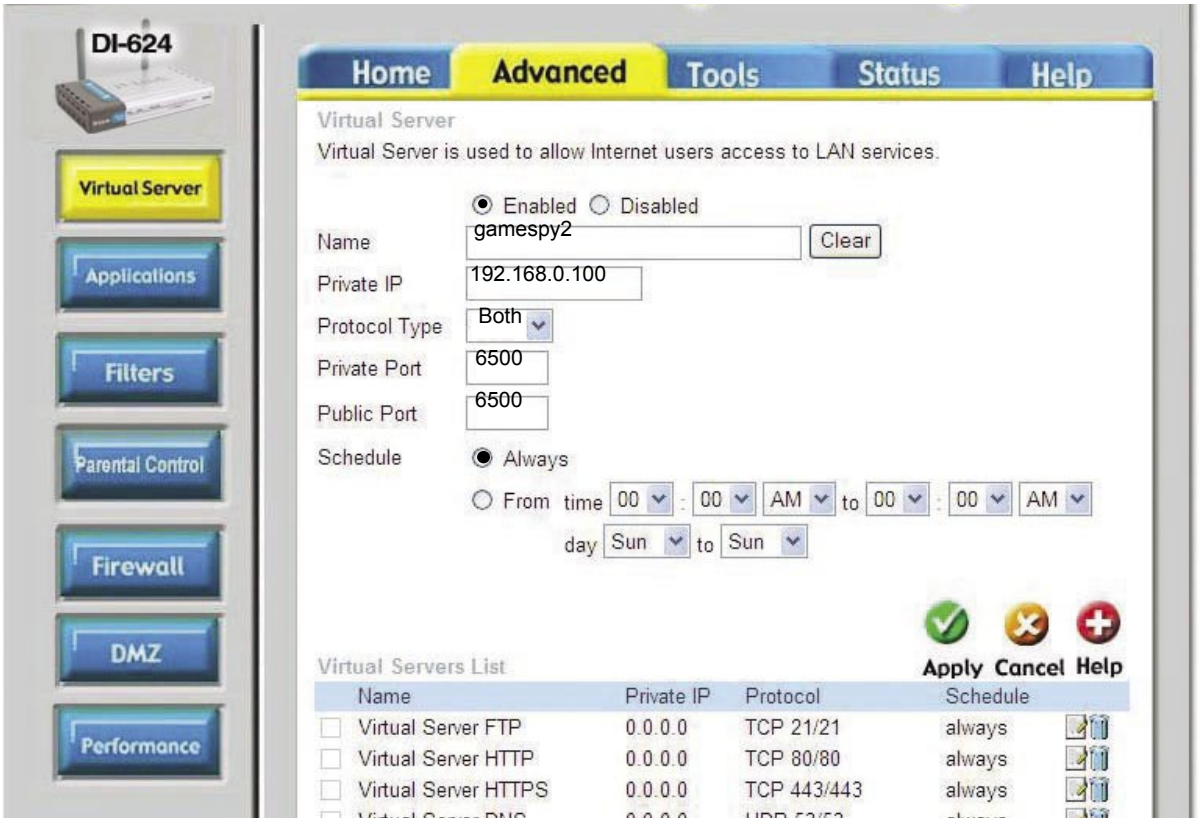
PROTOCOL TYPE - Both

PRIVATE PORT - 3783

PUBLIC PORT - 3783

SCHEDULE - Always.

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



Step 5: 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).

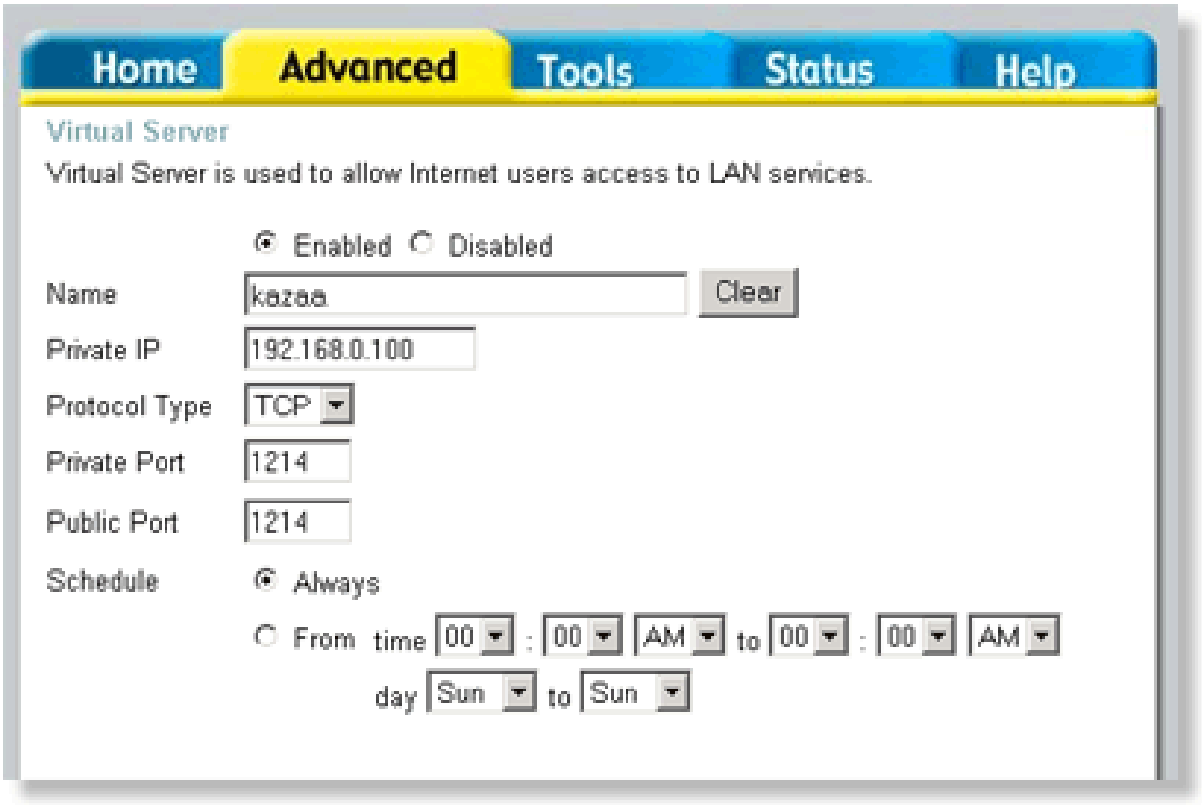
Step 2: Enter your username (admin) and your password (blank by default).

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.



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

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

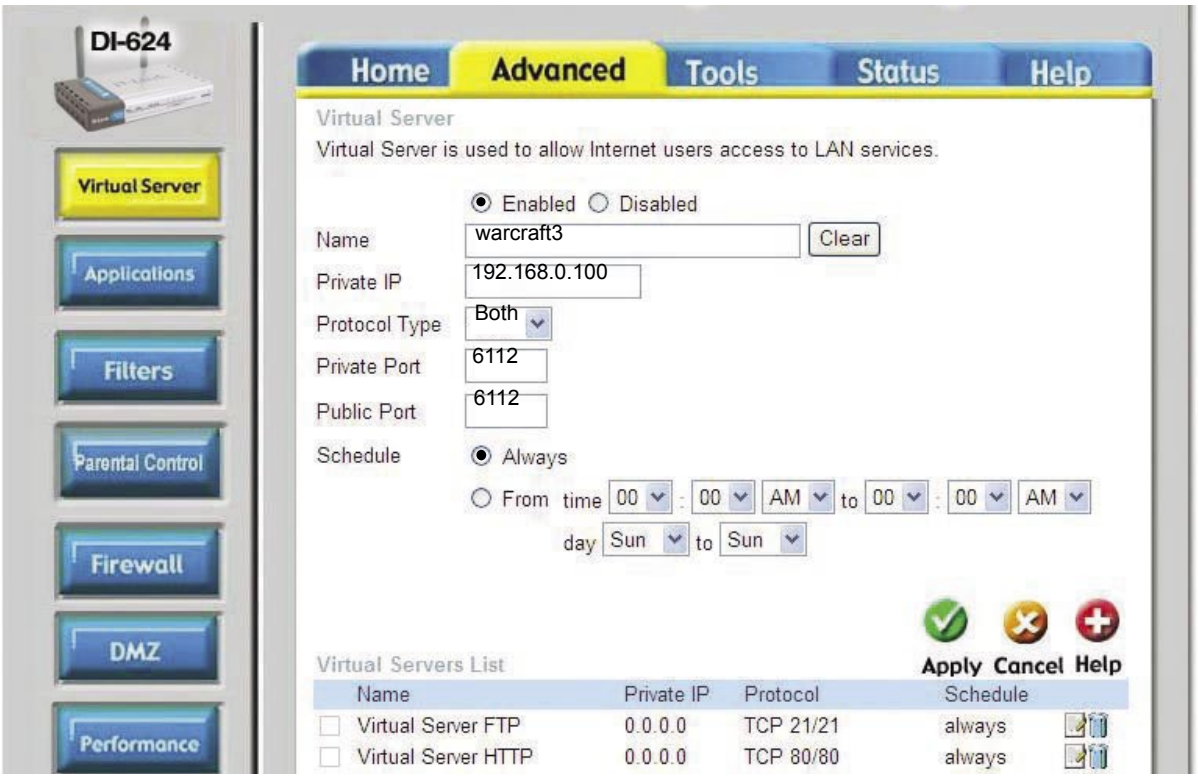
You must open ports on your router to allow incoming traffic while hosting a game in Warcraft 3. To play a game, you do not have to configure your router.

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.



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 *****.

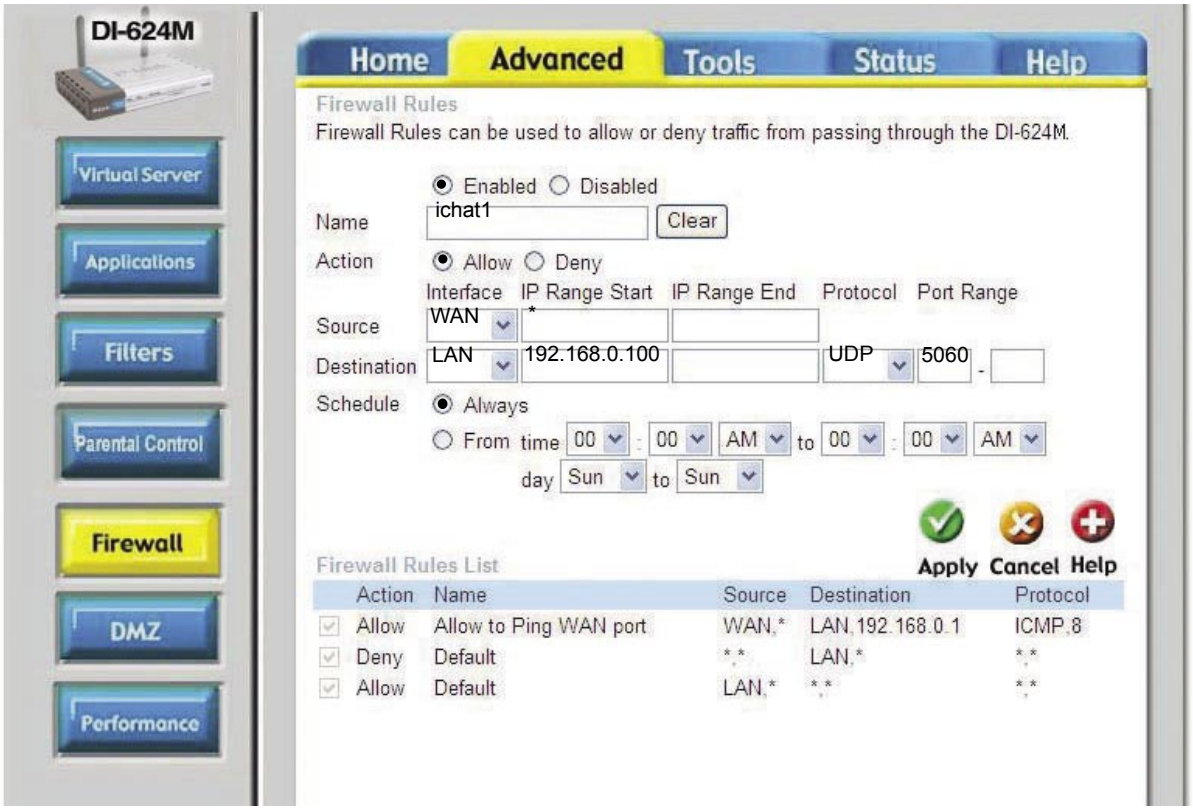
Leave the second box empty.

Next to Destination, select **LAN** under interface.

Enter the IP Address of the computer you are running iChat from.

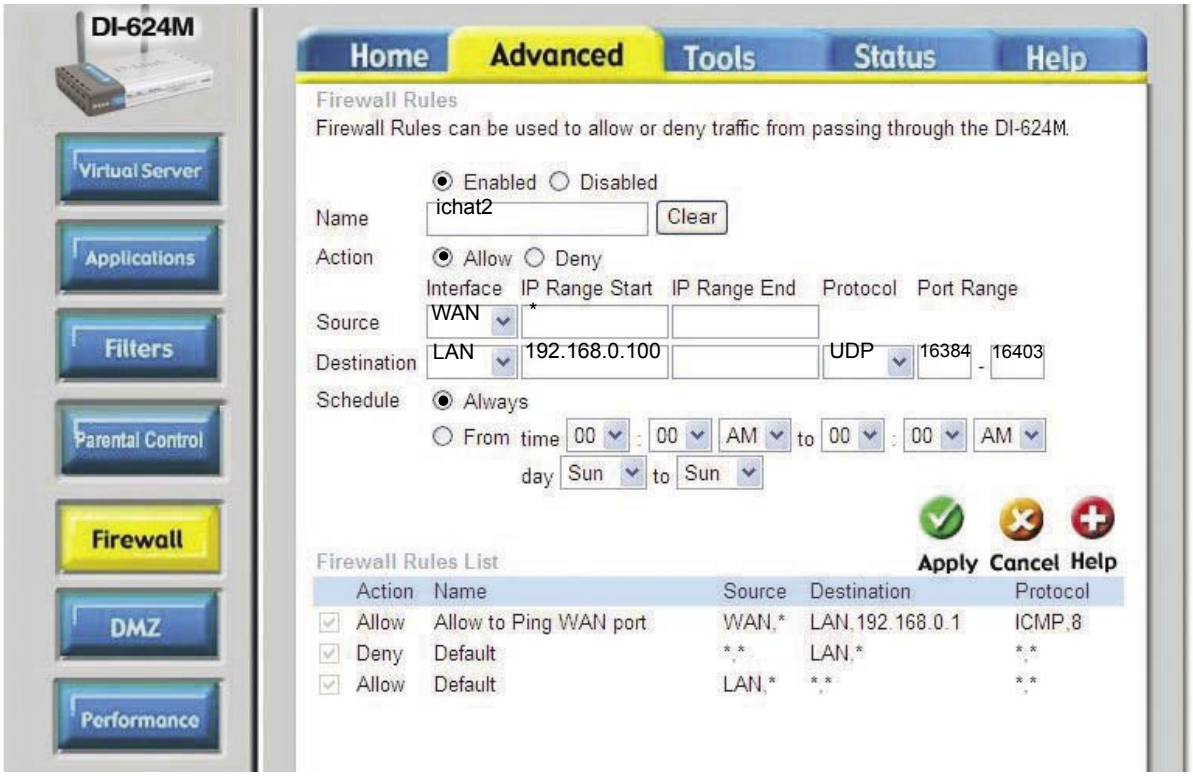
Leave the second box empty. Under Protocol, select **UDP**. In the port range boxes, enter **5060** in the first box and leave the second box empty.

Click **Always** or set a schedule.



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

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



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).

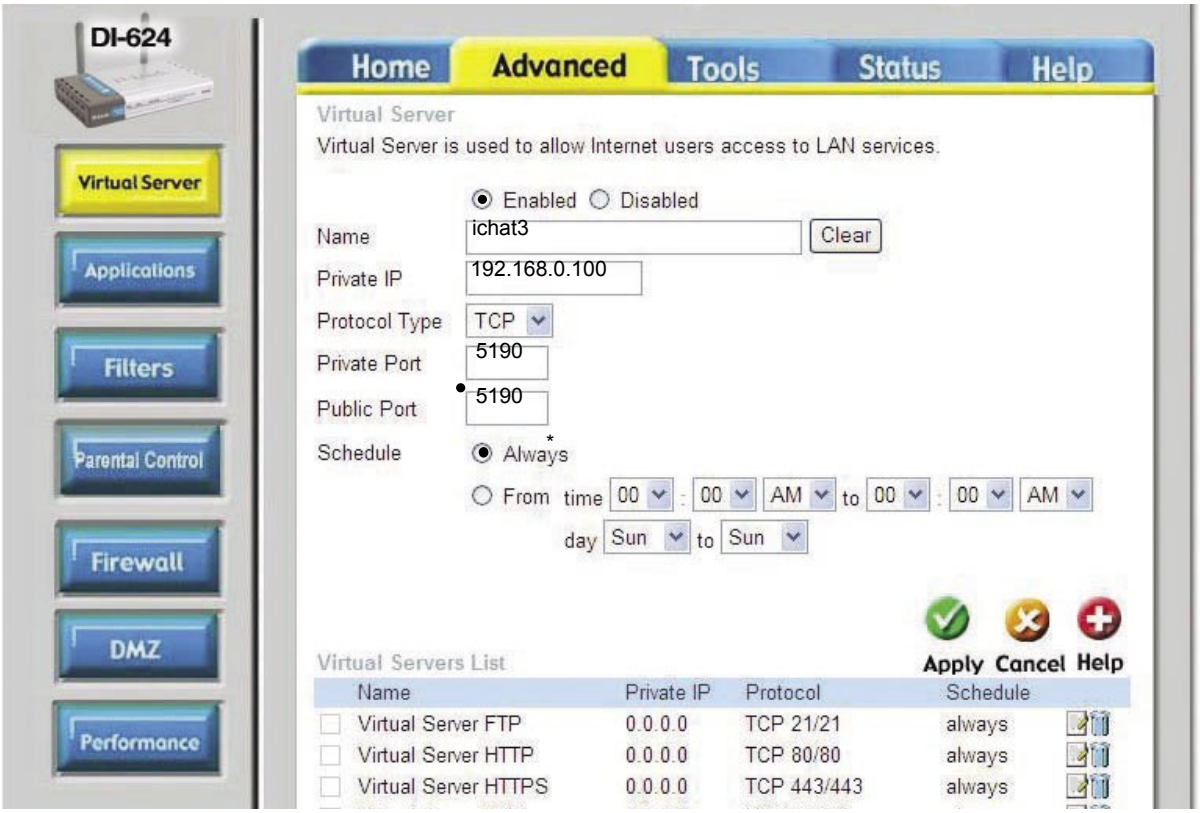
Step 4: Next to Private IP, enter the IP Address of the computer on your local network that you want to allow the incoming service to.

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**.



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.

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.

USA-Federal Communications Commission (FCC)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of 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. If not installed and used in accordance with the instructions, it may cause harmful interference to radio communications. 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 tuning the equipment off and on, the user is encouraged to try and correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna

-Increase the distance between the equipment and the receiver.

-Connect the equipment to outlet on a circuit different from that to which the receiver is connected.

-Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Caution: Exposure to Radio Frequency Radiation.

To comply with FCC RF exposure compliance requirements, a separation distance of at least 20 cm must be maintained between the antenna of this device and all persons. This device must not be co-located or operating in conjunction with any other antenna or transmitter.

Canada – Industry Canada (IC)

This device complies with RSS 210 of Industry Canada.

Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of this device.

L ' utilisation de ce dispositif est autorisée seulement aux conditions suivantes : (1) il ne doit pas produire de brouillage et (2) l' utilisateur du dispositif doit étre prêt à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

The term "IC" before the equipment certification number only signifies that the Industry Canada technical specifications were met.

To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (EIRP) is not more than that required for successful communication.

To prevent radio interference to the licensed service, this device is intended to be operated indoors and away from windows to provide maximum shielding. Equipment (or its transmit antenna) that is installed outdoors is subject to licensing.

Pour empecher que cet appareil cause du brouillage au service faisant l'objet d'une licence, il doit etre utilize a l'interieur et devrait etre place loin des fenetres afin de Fournier un ecram de blindage maximal. Si le matriel (ou son antenne d'emission) est installe a l'exterieur, il doit faire l'objet d'une licence.

Caution: Exposure to Radio Frequency Radiation.

The installer of this radio equipment must ensure that the antenna is located or pointed such that it does not emit RF field in excess of Health Canada limits for the general population; consult Safety Code 6, obtainable from Health Canada's website www.hc-sc.gc.ca/rpb.