D-Link DI-808HV

Broadband VPN
Router

Manual

D-Link

Building Networks for People
09/10/2003

Contents

Package Contents

Contents of Package:

- **D-Link DI-808HV** Broadband VPN Router
- 5V DC Power Adapter
- Ethernet (CAT5-UTP/Straight-Through) Cable
- Manual on CD
- Quick Installation Guide

Note: Using a power supply with a different voltage rating than the one included with the DI-808HV will cause damage and void the warranty for this product.

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

System Requirements For Configuration:

- Ethernet-based Cable or DSL Modem

- Computer with Windows-, Macintosh-, or Linux-based operating system with an installed Ethernet adapter

- Internet Explorer version 6.x or Netscape Navigator version 6.x and above, with JavaScript enabled
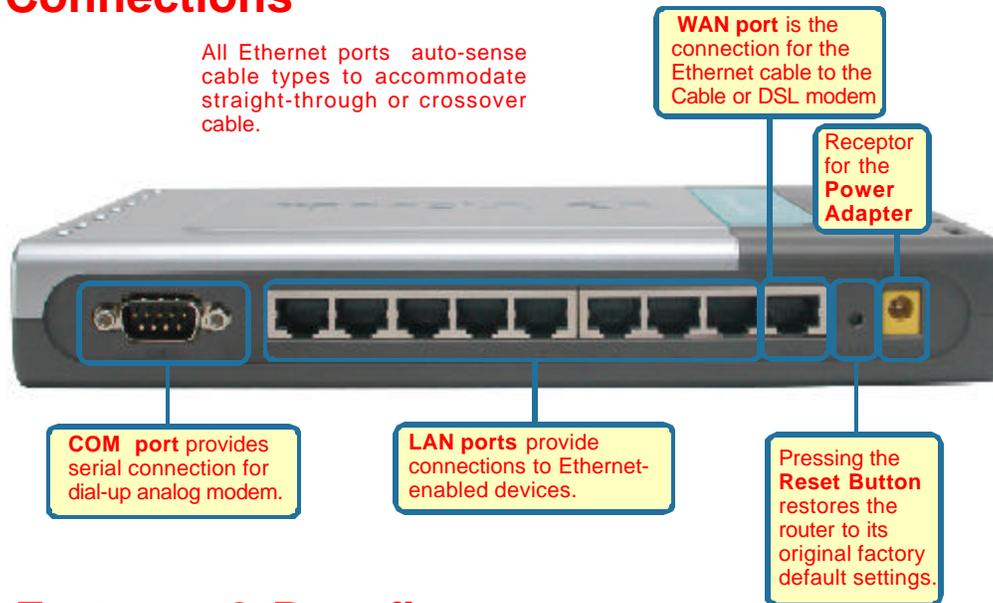
Introduction

The D-Link DI-808HV is a 8-port Broadband Router with Virtual Private Network (VPN) functionality. It provides a complete solution for Internet and office resource sharing, and secure access to remote corporate networks. It is an ideal way to extend the number and reach of computers connected to your network.

After completing the steps outlined in the *Quick Installation Guide* (included in your package) you will have the ability to share information and resources.

The DI-808HV is compatible with most popular operating systems, including Macintosh, Linux, and Windows and can be integrated into a large network.

Connections

All Ethernet ports auto-sense cable types to accommodate straight-through or crossover cable.

WAN port is the connection for the Ethernet cable to the Cable or DSL modem

Receptor for the **Power Adapter**

COM port provides serial connection for dial-up analog modem.

LAN ports provide connections to Ethernet-enabled devices.

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

Features & Benefits

- **Broadband modem and IP sharing**
  Connects multiple computers to a broadband (cable or DSL) modem to surf the Internet

- **Auto-sensing Ethernet Switch**
  Equipped with a 8-port auto-sensing Ethernet switch

- **Hardware VPN Termination Device**
  Supports up to 40 VPN Tunnels

- **VPN Pass-Through supported**
  Supports pass-through VPN sessions and allows you to setup VPN server and VPN clients

- **Firewall**
  Unwanted packets from outside intruders can be blocked to protect your network

- **DHCP server supported**
  All of the networked computers can retrieve TCP/IP settings automatically from the DI-808HV

- **Web-based configuration**
  Configurable through any networked computer's web browser using Netscape or Internet Explorer

5

Features & Benefits continued

- ### Access Control supported
  Allows you to assign different access rights for different users.

- ### Packet Filter supported
  Packet Filter allows you to control access to a network by analyzing the incoming and outgoing packets and letting them pass or halting them based on the IP address of the source and destination.

- ### Virtual Server supported
  Enables you to expose WWW, FTP, and other services on your LAN to be accessible to Internet users.

- ### User-Definable Application-Sensing Tunnel
  You can define the attributes, for instance opening special ports to allow packets to come through, to support special applications requiring multiple connections, such as Internet gaming, video conferencing, and Internet telephony. The DI-808HV can sense the application type and open a multi-port tunnel for it.

- ### DMZ Host supported
  Allows a networked computer to be fully exposed to the Internet; this function is used when the special "Application-Sensing Tunnel feature" is insufficient to allow an application to function correctly.

Introduction to Broadband Router Technology

A router is a device that forwards data packets from a source to a destination. Routers forward data packets using IP addresses and not a MAC address. A router will forward data from the Internet to a particular computer on your LAN.

The information that resides on the Internet gets moved around using routers. When you click on a link on a web page, you send a request to a server to show you the next page. The information that is sent and received from your computer is moved from your computer to the server using routers. A router also determines the best route that your information should follow to ensure that the information is delivered properly.

A router controls the amount of data that is sent through your network by eliminating information that should not be there. This provides security for the computers connected to your router, because computers from the outside cannot access or send information directly to any computer on your network. The router determines which computer the information should be forwarded to and sends it. If the information is not intended for any computer on your network, the data is discarded. This keeps any unwanted or harmful information from accessing or damaging your network.

Introduction to Firewalls

A firewall is a device that sits between your computer and the Internet that prevents unauthorized access to or from your network. A firewall can be a computer using firewall software or a special piece of hardware built specifically to act as a firewall. In most circumstances, a firewall is used to prevent unauthorized Internet users from accessing private networks or corporate LANs and Intranets.

A firewall watches all of the information moving to and from your network and analyzes each piece of data. Each piece of data is checked against a set of criteria that the administrator configures. If any data does not meet the criteria, that data is blocked and discarded. If the data meets the criteria, the data is passed through. This method is called packet filtering.

A firewall can also run specific security functions based on the type of application or type of port that is being used. For example, a firewall can be configured to work with an FTP or Telnet server. Or a firewall can be configured to work with specific UDP or TCP ports to allow certain applications or games to work properly over the Internet.

Introduction to Local Area Networking

Local Area Network (LAN) is the term used when several computers are connected together over a small area such as a building or a group of buildings. LANs can be connected over large areas. A collection of LANs connected over a large area is called a Wide Area Network (WAN).

A LAN consists of multiple computers connected to each other. There are many types of media that can connect computers together. The most common media is CAT5 cable (UTP or STP twisted pair wire). Each computer must have a Network Interface Card (NIC), which communicates the data between computers. A NIC is usually a 10Mbps network card, or 10/100Mbps network card, or a wireless network card. Wireless Local Area Networks (WLANs) do not use wires; instead they communicate over radio waves.

Most networks use hardware devices such as hubs or switches that each cable can be connected to in order to continue the connection between computers. A hub simply takes any data arriving through each port and forwards the data to all other ports. A switch is more sophisticated, in that a switch can determine the destination port for a specific piece of data. A switch minimizes network traffic overhead and speeds up the communication over a network.

Networks take some time in order to plan and implement correctly. There are many ways to configure your network. You may want to take some time to determine the best network set-up for your needs.

Introduction to Virtual Private Networking

Virtual Private Networking (VPN) uses a publicly wired network (the Internet) to securely connect two different networks through a secure "data tunnel." For example, an employee can access a corporate network from home using VPN, allowing the employee to access files, databases, and other networked resources. Here are several different implementations of VPN that can be used.

Point-to-Point Tunneling Protocol (PPTP)

PPTP uses proprietary means of connecting two private networks over the Internet. PPTP is a way of securing the information that is communicated between networks. PPTP secures information by encrypting the data inside of a packet.

IP Security (IPSec)

IPSec provides a more secure network-to-network connection across the Internet or a Wide Area Network (WAN). IPSec encrypts all communication between the client and server whereas PPTP only encrypts the data packets.

Both of these VPN implementations are used because there is not a standard for VPN server software. Because of this, each ISP or business can implement its own VPN network making interoperability a challenge.

LEDS

LED stands for **L**ight-**E**mitting **D**iode. The **DI-808HV** has the following LEDs as described below:

LED	LED Activity
Power	A steady light indicates a connection to a power source
Status	Flash indicates device work properly
WAN	A solid light indicates connection on the WAN port. This LED blinks during data transmission
COM	A solid light indicates a connection to an external dial-up analog modem
LOCAL NETWORK (Ports 1-8)	A solid light indicates a connection to an Ethernet-enabled computer on ports 1-8. This LED blinks during data transmission

Getting Started
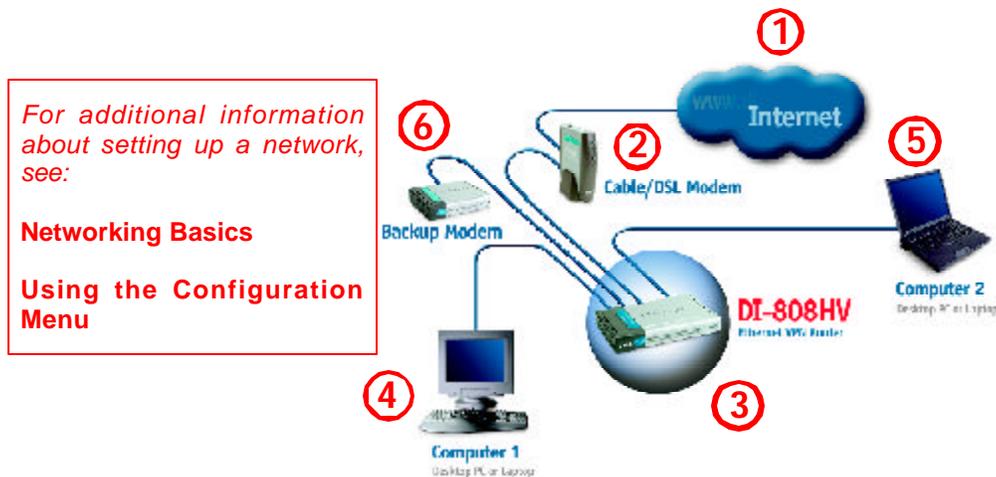
For a typical network setup in a home or small office (as shown above)**, please do the following:**

1 You will need broadband Internet access (a Cable or DSL subscription 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-808HV wireless broadband router (*see the Quick Installation Guide included with the DI-808HV.*)

4 If you are connecting a desktop computer to your network and you need an Ethernet connection, you can install the D-Link *DFE-530TX+* Ethernet adapter into an available PCI slot. (See the Quick Installation Guide included with the DFE-530TX+.)

5 If you are connecting a laptop computer to your network, install the drivers for the Ethernet Cardbus adapter (e.g., D-Link DFE-690TXD) into a laptop computer.(See the Quick Installation Guide included with the DFE-690TXD.)

6 You may connect an analog modem (optional) to function as a backup to the DI-808HV. To use a backup modem, you must have dial-up service.

Using the Configuration Menu

Whenever you want to configure your network or the DI-808HV, you can access the Configuration Menu by opening the Web browser (i.e., Internet Explorer or Netscape Navigator) and typing in the IP Address of the DI-808HV. The DI-808HV default IP Address is shown below:

- Open the Web browser
- Type in the **IP Address** of the DI-808HV (http://192.168.0.1)

http://192.168.0.1

Note: If you have changed the default IP Address assigned to the DI-808HV, make sure to enter the correct IP Address.

The factory default **User name** is **admin** and the default **Password** is blank (empty). It is recommended that you change the admin password for security purposes. Please refer to **Tools>Admin** to change the admin password.

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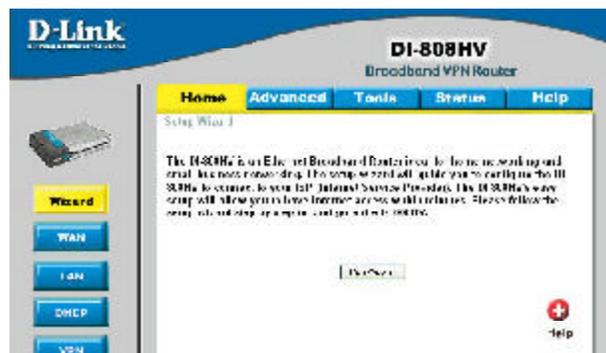
The **Home>Wizard** screen will appear. Please refer to the *Quick Installation Guide* for more information regarding the Setup Wizard.

 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

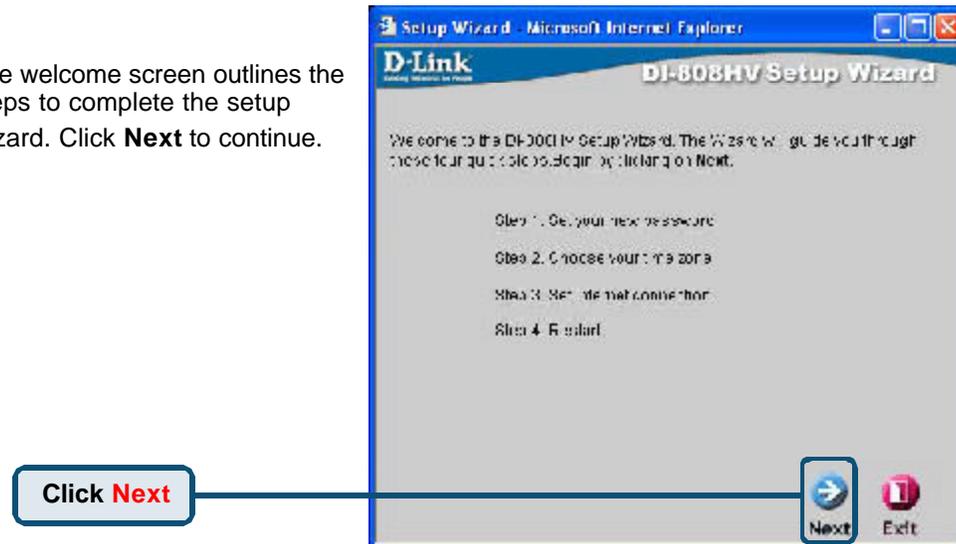 **Restart**   Clicking **Restart** will restart the router. (Necessary for some changes.)

11

Using the Configuration Menu

Setup Wizard

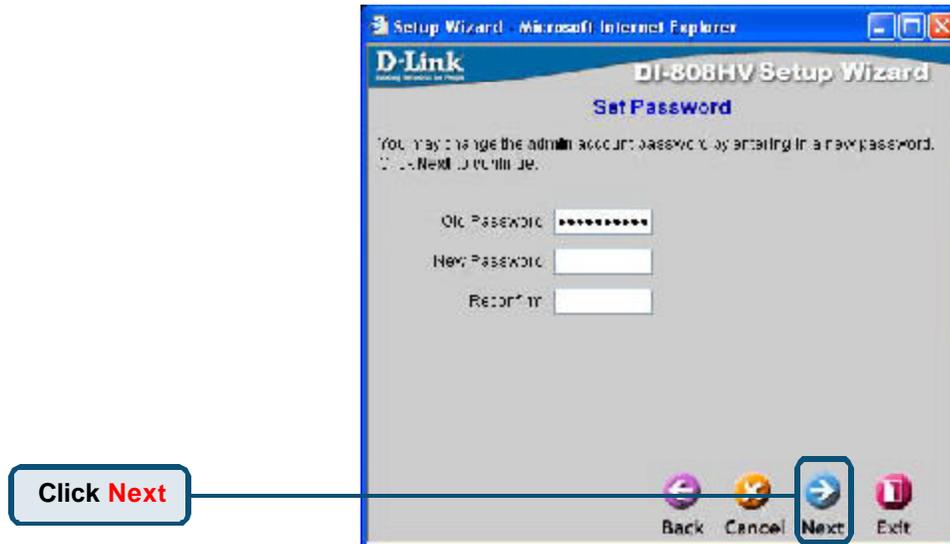Once you have logged in, the **Home** screen will appear.

Click **Run Wizard**
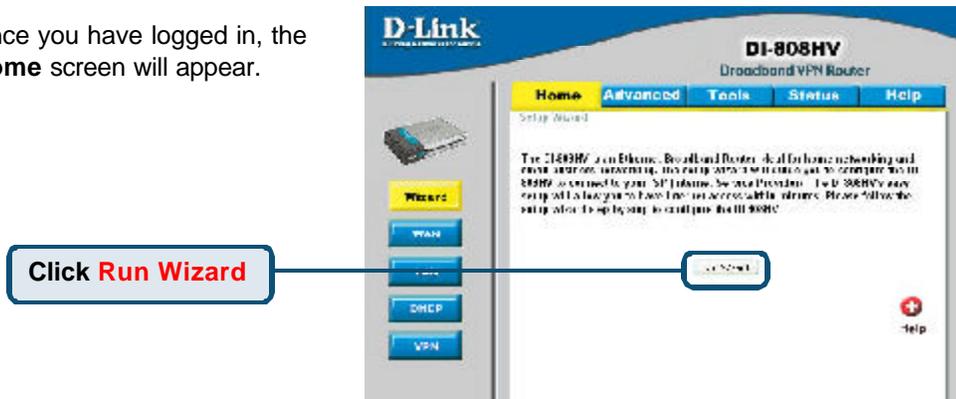
The welcome screen outlines the steps to complete the setup wizard. Click **Next** to continue.

Click **Next**
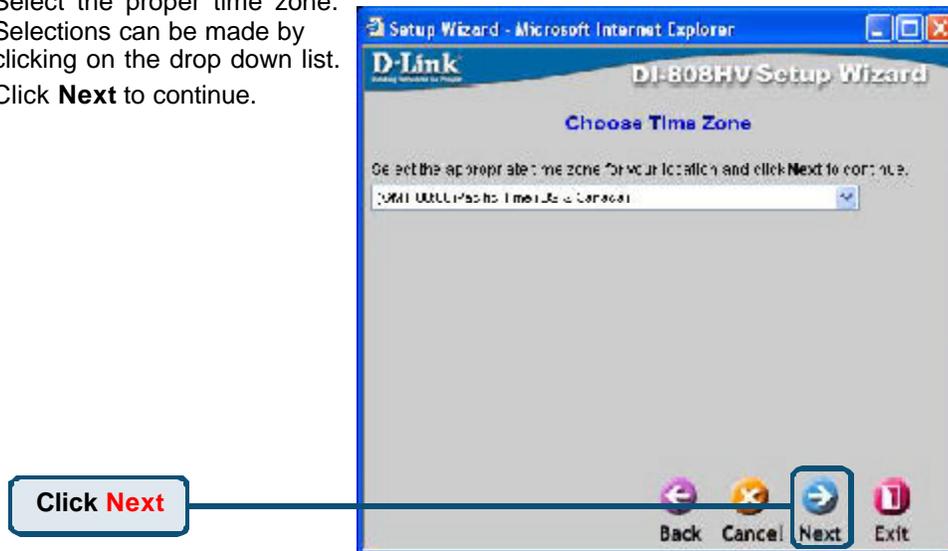
Using the Configuration Menu

Setup Wizard > Set Password

Click Next

Old Password-	This information is masked.
New Password-	Type in the new password for the **admin** account.
Reconfirm-	Type in the new password again to confirm. Click **Next** to continue with the Setup Wizard.

Using the Configuration Menu

Setup Wizard > Time Zone

Select the appropriate time zone for your location-

Select the proper time zone. Selections can be made by clicking on the drop down list. Click **Next** to continue.

Click **Next**

Setup Wizard > Auto Detecting WAN

Please wait a moment while the DI-808HV auto detects your WAN.
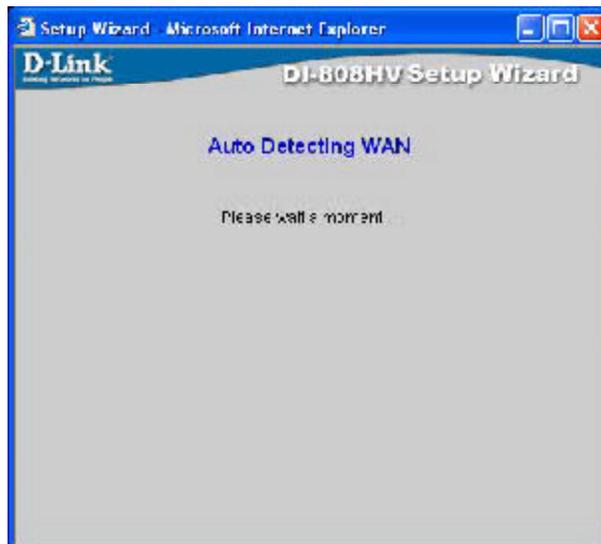
Using the Configuration Menu

Setup Wizard > Connection Type (WAN)

Select Your Internet Connection-

You will be prompted to select
the type of internet connection
for your router. Choose the
appropriate selection and click
Next to continue.

Click Next
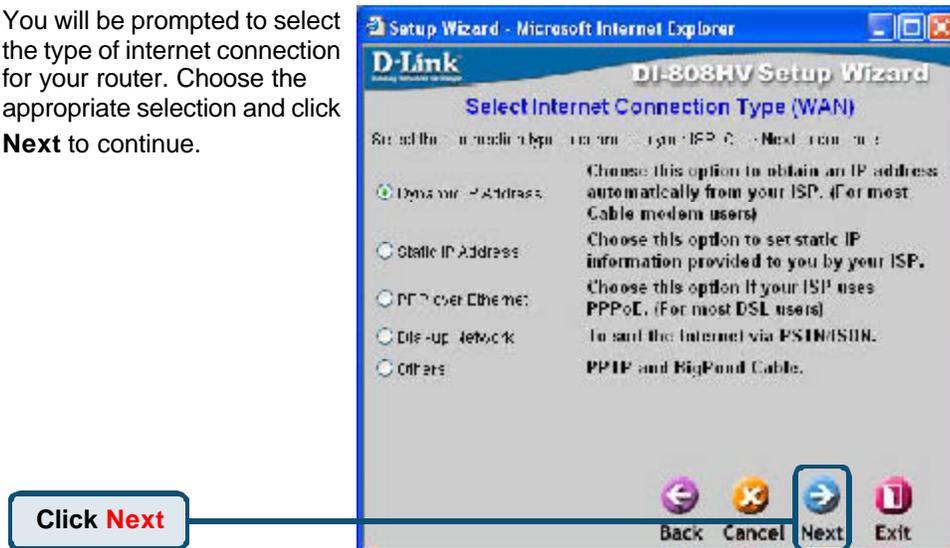
> ⚠️ **If you are unsure of which setting to select, please contact your Internet Service Provider.**

> ⚠️ Select **Others** only if you use PPTP in Europe or Big Pond Cable in Australia.

Using the Configuration Menu

Setup Wizard > Set Dynamic IP Address

Click Next
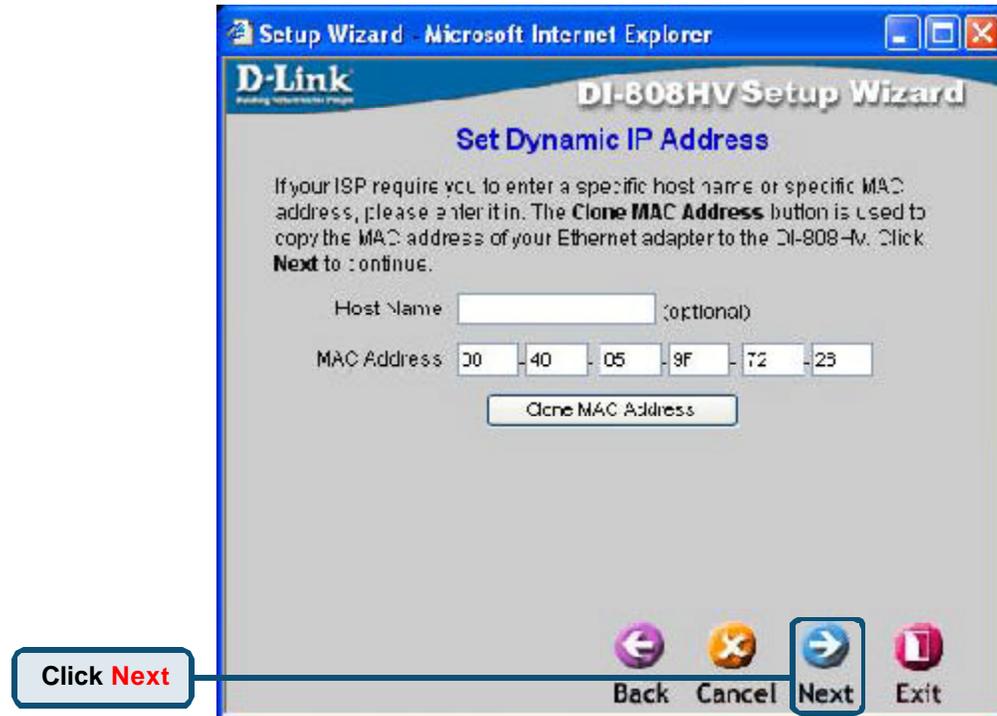
If your ISP uses **Dynamic IP Address**, this screen will appear: **(Used mainly for Cable Internet service.)**

Host Name
Host name is the section where you input the name of your ISP. This section is optional and is not required to be filled in.

MAC Address
Each network adapter has a discrete Media Access Control (MAC) address. Note that some computer and peripherals may already include built-in network adapter.

Clone MAC Address
By clicking on Clone MAC Address, the DI-808HV will automatically copy the MAC address of the network adapter in your computer. You can also manually type in the MAC address. Click **Next** to continue.

Using the Configuration Menu

Setup Wizard > Set Static IP Address

Click Next

If your ISP uses a **Static IP Address**, and this option is selected, then this screen will appear.

WAN IP Address If your ISP requires a Static IP Address, and this option is selected, then this screen will appear. Enter the IP address information originally provided to you by your ISP. You will need to complete all the required fields.

WAN Subnet Mask The subnet for the DI-808HV is preconfigured to 255.255.255.0. Configurations can be made, but are not recommended. This feature is for advanced users.

WAN Gateway This information is provided by your ISP.

Primary DNS The Primary DNS can be found by contacting the ISP.

Secondary DNS The Secondary DNS can be found by contacting the ISP.

17

Using the Configuration Menu

Setup Wizard > PPPoE

Click Next

If your ISP uses **PPPoE** (Point-to-Point Protocol over Ethernet), and this option is selected, then this screen will appear: (Used mainly for DSL Internet service.)

PPPoE Account   Enter in the username provided to you by your ISP.

PPPoE Password   Enter in the password provided to you by your ISP.

PPPoE Service Name   Enter in the name of your service provider. This is an optional field and is not necessary to be filled in.

18

Using the Configuration Menu

Setup Wizard > Dial-up Network

Click Next

Configure this section only if you have an analog dial-up account. Otherwise click **Next** to skip.

Dial-up Telephone	Enter the telephone number to connect to your ISP.
Dial-up Account	This information is provided by your ISP. The Dial-up Account is also known as username.
Dial-up Password	Enter in the password to log into your Dial-up account.
Primary DNS	The Primary DNS can be found by contacting the ISP.
Secondary DNS	The Secondary DNS can be found by contacting the ISP.

19

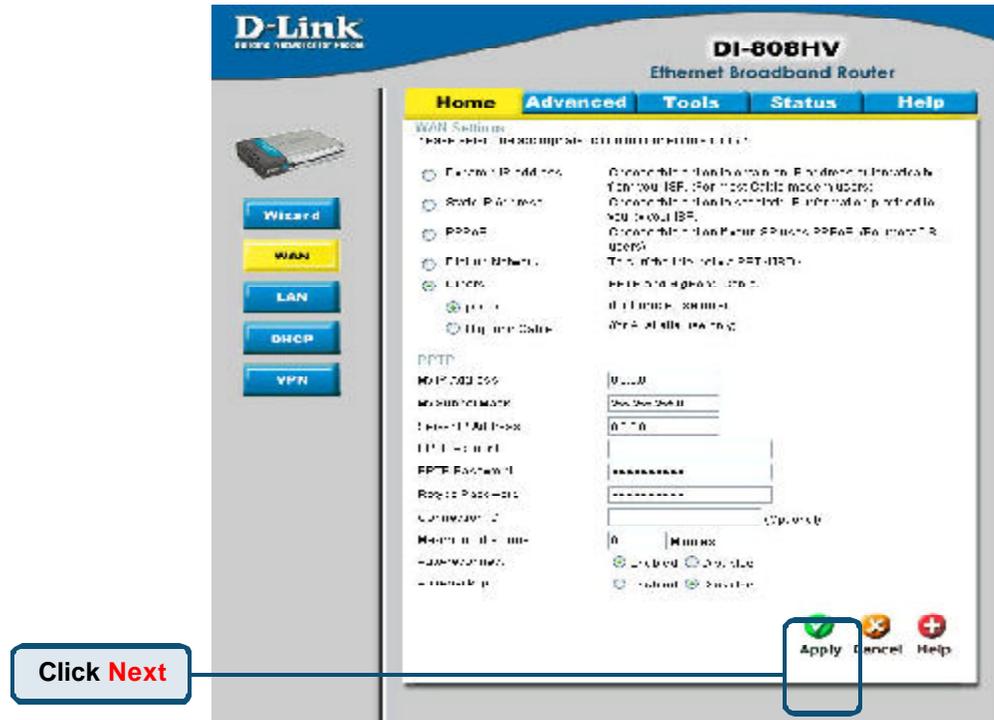# Using the Configuration Menu

Click **Next**

Select the connection type to connect to your ISP. Choose the appropriate selection and click **Next** to continue.

PPTP   This is a WAN connection used in Europe.

BigPond Cable   This is a WAN connection used in Australia.

20

Using the Configuration Menu

Setup Wizard > Others > PPTP

Click Next

If your ISP uses **PPTP** (Point-to-Point Tunneling Protocol), and this option is selected, then this screen will appear: (Used for Internet service in Europe.)

My IP Address   Enter the IP address information originally provided to you by your ISP. You will need to complete all the required fields.

My Subnet Mask   The subnet for the DI-808HV is preconfigured to 255.255.255.0. Configurations can be made, but are not recommended. This feature is for advanced users.

Server IP Address   Enter the server IP address information originally provided to you by your ISP.

PPTP Account   Enter in the username provided to you by your ISP.

PPTP Password   Enter in the password provided to you by your ISP.

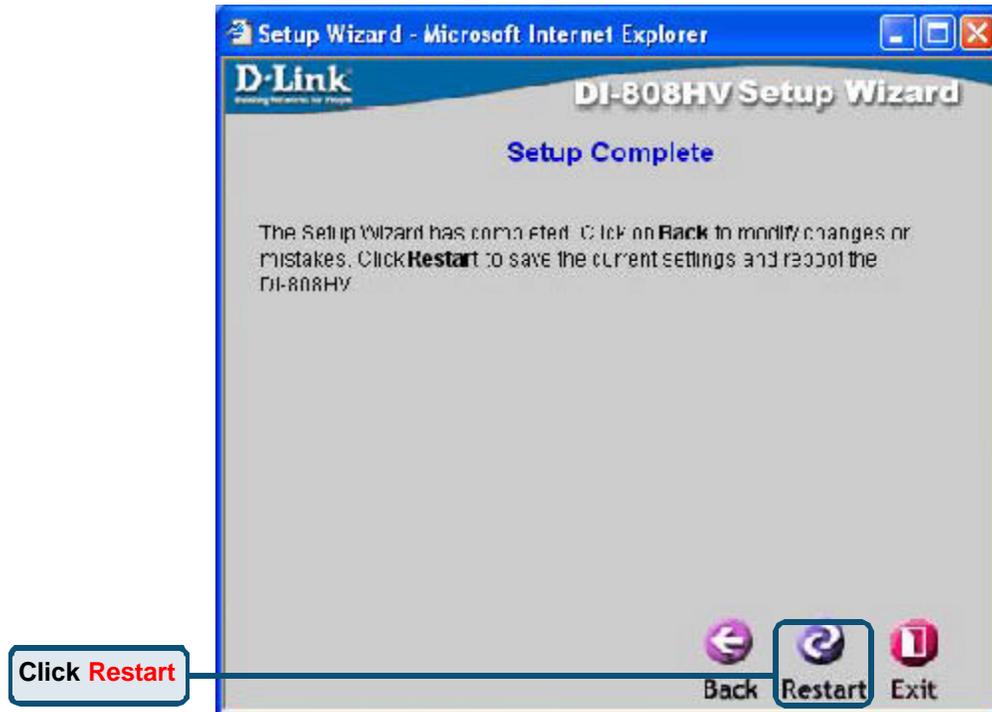# Using the Configuration Menu

Click Next

If your ISP uses **BigPond Cable** (Point-to-Point Protocol over Ethernet), and this option is selected, then this screen will appear: (Used for Internet service in Australia.)

Account   Enter in the username provided to you by your ISP.

Password   Enter in the password provided to you by your ISP.

Login Server   Enter in the name of your login server. This is an optional field and is not necessary to be filled in.

22

Using the Configuration Menu

Setup Wizard

Click Restart

Back   Click on the Back button to go back to previous page.

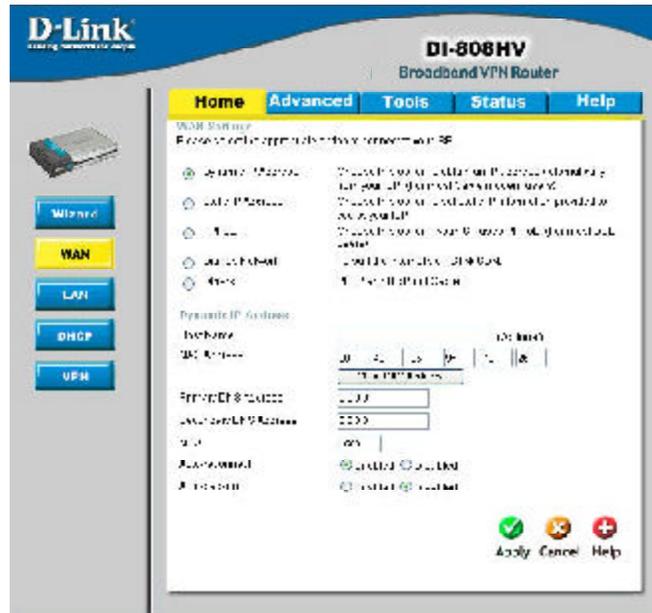**Restart**   Click on the **Restart** button to finalize the settings made.

Exit   Click on the Exit button to end the Setup Wizard without saving
                any changes.

Using the Configuration Menu

Choose WAN Type

WAN stands for **Wide Area Network**. In this case, WAN represents the mode in which you connect to the Internet. If you are uncertain, please ask your ISP which of the following represents your connection mode to the Internet:

|	
Dynamic IP Address	Obtain an IP address from your ISP automatically (mainly for Cable users)
Static IP Address	Your ISP assigns you a Static IP Address
PPPoE	Some ISPs require the use of PPPoE to connect to their services (mainly for DSL users)
Dial-up Network	Dial-up users can select this option to connect to their ISP through an analog dial-up modem if broadband connectivity is unavailable.
Others	
PPTP	For use in Europe only
BigPond Cable	For use in Australia only

24

Using the Configuration Menu
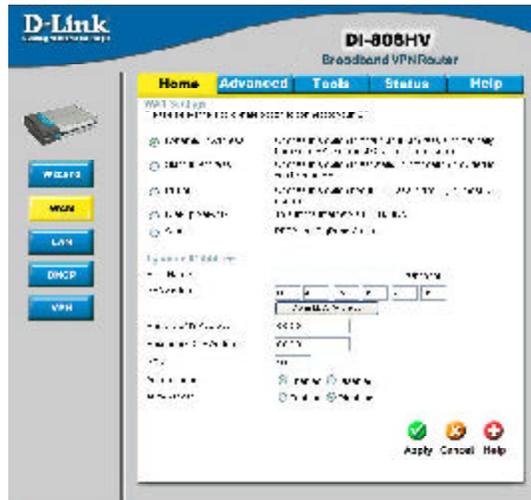
Most cable modem users will select this option to obtain an IP Address automatically from their ISP (Internet Service Provider).

Host Name	This is optional, but may be required by some ISPs. The host name is the device name of the Router.
MAC Address	The default MAC Address is set to the WAN's physical interface MAC address on the Router.
Clone MAC Address	This feature will copy the MAC address of the Ethernet card, and replace the WAN MAC address of the Router with this Ethernet card MAC address. It is not recommended that you change the default MAC address unless required by your ISP.
Primary DNS Address	Input the primary DNS address provided by your ISP
Secondary DNS Address	(Optional) Input the Secondary DNS address provided by your ISP.
MTU	*Maximum Transmission Unit*; default is 1500; you may need to change the MTU to conform to your ISP.
Auto-reconnect	If enabled, the Broadband Router will automatically connect to your ISP after your system is restarted or if the connection is dropped.
Auto-backup	Enabling this feature will connect your router to the Internet using a dial-up service if your broadband connection becomes unavailable. A subscription to a dial-up service is required for the auto-backup to work.

25

Using the Configuration Menu

If you use a Static IP Address, you will input information here that your ISP has provided to you.

IP Address   Input the IP Address provided by your ISP

Subnet Mask   Input the Subnet Mask provided by your ISP

ISP Gateway
Address   Input the Gateway address provided by your ISP

Primary DNS
Address   Input the primary DNS address provided by your ISP

Secondary DNS
Address   (Optional) Input the Secondary DNS address provided by your ISP.

MTU   *Maximum Transmission Unit*; default is 1500; you may need to change the MTU to conform to your ISP.

Auto-backup   Enabling this feature will connect your router to the Internet using a dial-up service if your broadband connection becomes unavailable. A subscription to a dial-up service is required for the auto-backup to work.

26

Using the Configuration Menu

Home > WAN > PPPoE

Most DSL users will select this option to obtain an IP address automatically from their ISP through the use of PPPoE.

User Name	Your PPPoE username provided by your ISP
Password	Your PPPoE password is provided by your ISP
Service Name	(Optional) Check with your ISP for more information if they require the use of service name.
IP Address	(Optional) Enter in the IP Address if you are assigned a static PPPoE address.
Primary DNS Address	You will get the DNS IP automatically from your ISP but you may enter a specific DNS address that you want to use instead.
	(Optional) Input the secondary DNS address
Maximum Idle Time	Enter a maximum idle time during which Internet connection is maintained during inactivity. To disable this feature, enable *Auto-reconnect*.
MTU	*Maximum Transmission Unit*; default is 1492; you may need to change the MTU to conform to your ISP.

27

Using the Configuration Menu

Home > WAN > Dial-up Network

Most dial-up users will select this option to connect to their ISP through an analog dial-up modem. This feature can be used as a back-up when your broadband connectivity is unavailable.

Dial-up Telephone	Telephone number to connect to your ISP
Dial-up Account	Username provided by your ISP
Dial-up Password	Password provided by your ISP
Primary DNS- Secondary DNS	If the settings are configured as "0.0.0.0," they will be automatically assigned upon connection.
Assigned IP Address	(Optional) Enter in the IP Address if you are assigned a static PPPoE address.
Extra Settings	This setting is used to optimize the communication quality between the ISP and your analog dial-up modem. (Initialization string) - optional.
Maximum Idle Time	Enter a maximum idle time during which Internet connection is maintained during inactivity. To disable this feature, enable *Auto-reconnect*.
Baud Rate	The communication speed between the DI-808HV and your modem.

28

Using the Configuration Menu

Home > WAN > PPTP

Point-to-Point Tunneling Protocol (PPTP) is a WAN connection used in Europe.

My IP Address	Enter the IP Address
My Subnet Mask	Enter the Subnet Mask
Server IP Address	Enter the Server IP Address
PPTP Account	Enter the PPTP account name
PPTP Password	Enter the PPTP password
Connection ID	(Optional) Enter the connection ID if required by your ISP
Maximum Idle Time	Enter a maximum idle time during which Internet connection is maintained during inactivity. To disable this feature, enable *Auto-reconnect*.

Using the Configuration Menu

Home > WAN > BigPond Cable

Dynamic IP Address for BigPond is a WAN connection used in Australia.

User Name	Enter in the username for the BigPond account
Password	Enter the password for the BigPond account
Login Server IP	(Optional) enter the Login Server name if required
Renew IP forever	If enabled, the device will automatically connect to your ISP after your unit is restarted or when the connection is dropped.

Using the Configuration Menu

Home > LAN
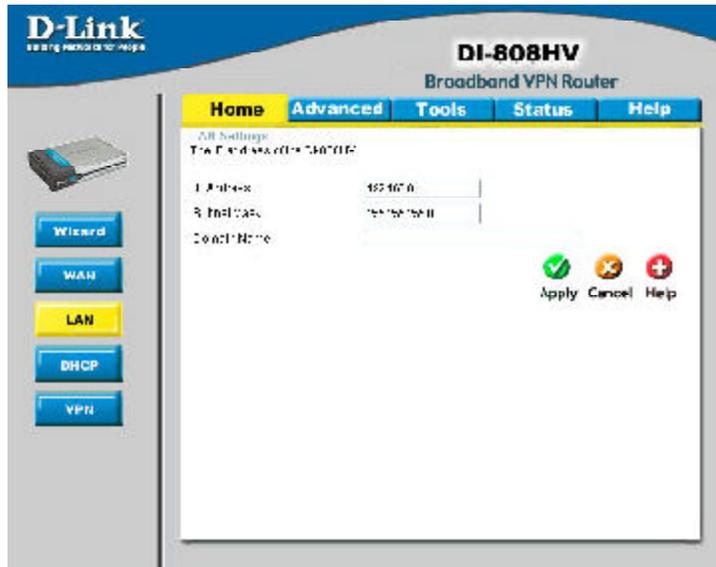
LAN (Local Area Network). This is considered your internal network. These are the IP settings of the LAN interface for the DI-808HV. These settings may be referred to as Private settings. You may change the LAN IP address if needed. The LAN IP address is private to your internal network and cannot be seen on the Internet.

LAN 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.

Domain Name (Optional) The name of your local domain

Using the Configuration Menu
Home >DHCP
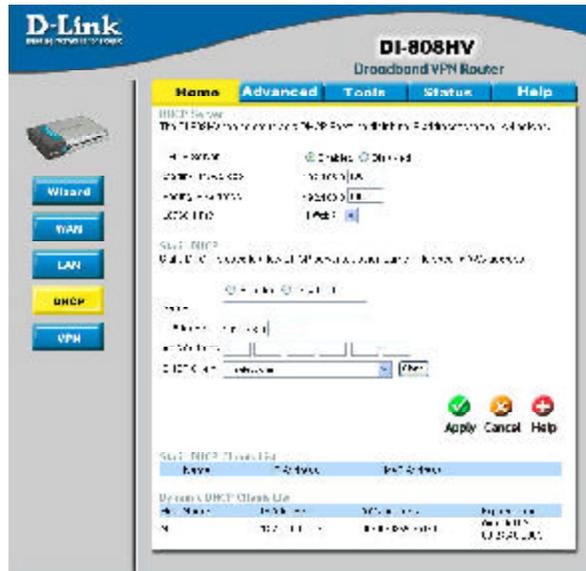
DHCP stands for **Dynamic Host Control Protocol**. The DI-808HV has a built-in DHCP server. The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set your computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When you turn your computers on, they will automatically load the proper TCP/IP settings provided by the DI-808HV. 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   Enable or disable the DHCP service.

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 DHCP lease.

DHCP Clients List   Lists the DHCP clients connected to the DI-808HV. Click **Refresh** to update the list. The table will show the Host Name, IP Address, and MAC Address of the DHCP client computer.

32

Using the Configuration Menu

Home >VPN Settings

VPN Settings are settings that are used to create virtual private tunnels to remote VPN gateways. The tunnel technology supports data confidentiality, data origin, authentication, and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

VPN	Check here to enable VPN tunnels. When you are not using the VPN feature, it is best to keep VPN disabled.
NetBIOS broadcast	Enable this to allow NetBIOS braodcast over the VPN tunnels.
Max. number of tunnels	Select the maximum number of allowable tunnels.
Tunnel Name	Create a name for the tunnel.
Method	IPSec VPN supports two kinds of key-obtained methods: manual key and automatic key exchange. Manual key approach indicates that the two endpoint VPN gateways require setting up authentication and encryption key by the Administrator manually. However, IKE approach will perform automatic Internet key exchange. Admins of both endpoint gateways will only need to set the same pre-shared key.
More	For more in depth configuration to adjust manual key or IKE method settings, click **More.**

33

Using the Configuration Menu

Home >VPN Settings > Tunnel > Method>IKE

Tunnel Name	Current tunnel name.
Aggressive Mode	Enabling this mode will accelerate establishing tunnel, but the device will have less security.
Local Subnet	The subnet of the VPN gateway's local network. It can be a host, a partial subnet or a whole subnet.
Local Netmask	Local netmask combined with local subnet to form a subnet domain.
Remote Subnet	The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Remote Netmask	The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Remote Gateway	The WAN IP address of remote VPN gateway.
Preshared Key	The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be the same for both endpoint gateways.
IKE Proposal index	Click the button to setup a set of frequent-used IKE proposals and select from the set of IKE proposals for the tunnel.
IPSec Proposal index	Click the button to setup a set of frequent-used IPSec proposals and select from the set of IKE proposals for the tunnel.

34

Using the Configuration Menu

Home >VPN Settings > Tunnel > Method > IKE > Select IKE Proposal

IKE Proposal index	A list of selected proposal indexes from the IKE proposal pool listed below.
Proposal Name	This is the name used to classify the IKE proposal.
DH Group	There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).
Encrypt algorithm	There are two algorithms that can be selected: 3DES and DES.
Auth algorithm	There are two algorithms that can be selected: SHA1 and MD5.

Using the Configuration Menu

Home >VPN Settings > Tunnel > Method > IKE > Select IKE Proposal
Continued...

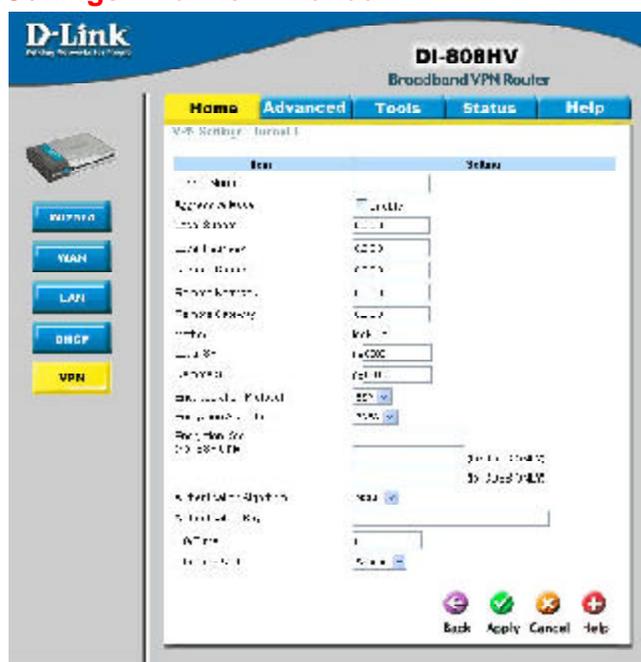| **Life Time**	Enter in the life time value.
Life Time Unit	There are two units that can be selected: second and KB.
Proposal ID	The identifier of IKE proposal can be chosen for adding corresponding proposal to the dedicated tunnel.
Add to	Click it to add the chosen proposal indicated by proposal ID to IKE Proposal index list.

Using the Configuration Menu

Home >VPN Settings > Tunnel > Method > IKE > Select IPSEC Proposal

IPSec Proposal index	A list of selected proposal indexes from the IPSec proposal pool listed below.
Proposal Name	This is the name used to classify the IPSec Proposal
DH Group	There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).
Encap protocol	There are two protocols that can be selected: ESP and AH.
Encrypt algorithm	There are two algorithms that can be selected: 3DES and DES.
Auth algorithm	There are two algorithms that can be selected: SHA1 and MD5.

Using the Configuration Menu

Home >VPN Settings > Tunnel > Method > IKE > Select IPSEC Proposal
Continued...
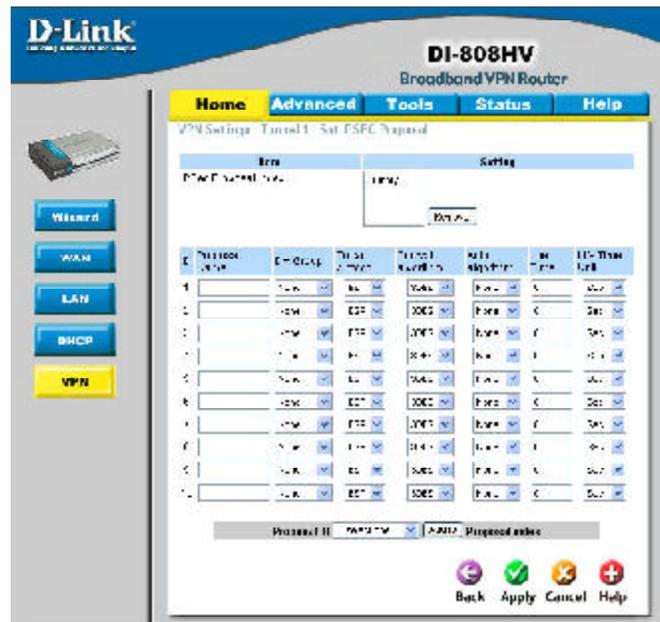
Life Time	Enter in a life time value.			
Life Time Unit	There are two units that can be selected: second and KB.			
Proposal ID	The identifier of IPSec proposal can be chosen for adding the proposal to the dedicated tunnel.			
Add to	Click it to add the chosen proposal indicated by proposal ID to IPSec Proposal index list.			

38

Using the Configuration Menu

Home >VPN Settings > Tunnel > Manual

|	
Tunnel Name	Current tunnel name.
Aggressive Mode	Enabling this mode will accelerate establishing tunnel, but the device will have less security.
Local Subnet	The subnet of the VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Local Netmask	Local netmask combined with local subnet to form a subnet domain.
Remote Subnet	The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Remote Netmask	The subnet of the remote VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Remote Gateway	The WAN IP address of remote VPN gateway.
Method	The set of rules applied when connecting to the VPN gateway.
Local SPI	The value of the local SPI should be set in hex format.
Remote SPI	The value of the remote SPI should be set in hex format.

39

Using the Configuration Menu

Home >VPN Settings > Tunnel > Manual *Continued...*

Encapsulation Protocol   There are two protocols that can be selected: ESP and AH.

Encryption Algorithm   There are two algorithms that can be selected: 3DES and DES.

Encryption Key   For DES, the encryption key is 8 bytes (16 Char.). For 3DES, the encryption key is 24 bytes (48 Char.).

Authentication Algorithm   There are two algorithms that can be selected: SHA1 and MD5.

Authentication Key   For MD5, the authentication algorithm is16 bytes (32 Char.). For SHA1, the authentication algorithm is 20 bytes.(40 Char.).

Life Time   Enter in the life time value.

Life Time Unit   There are two units that can be selected: Second and KB.

40

Using the Configuration Menu

Home >VPN Settings > Dynamic VPN Tunnel

VPN Settings - IKE	There are three parts that are necessary to setup the configuration of IKE for the dedicated tunnel: basic setup, IKE proposal setup, and IPSec proposal setup. Basic setup includes the setting of following items: local subnet, local netmask, remote subnet, remote netmask, remote gateway, and pre-shared key. The tunnel name is derived from the previous page of VPN setting. IKE proposal setup includes the setting of a set of frequent-used IKE proposals and selecting from the set of IKE proposals.
Tunnel Name	Current tunnel name.
Dynamic VPN	This feature works with a VPN software client so the DI-808HV does not need to know the IP address of the remote clients.
Aggressive Mode	Enabling this mode will accelerate establishing the tunnel, but the device will have less security.
Local Subnet	The subnet of the VPN gateway's local network. It can be a host, a partial subnet, or a whole subnet.
Local Netmask	The netmask of the VPN gateway's local network.

41

Using the Configuration Menu
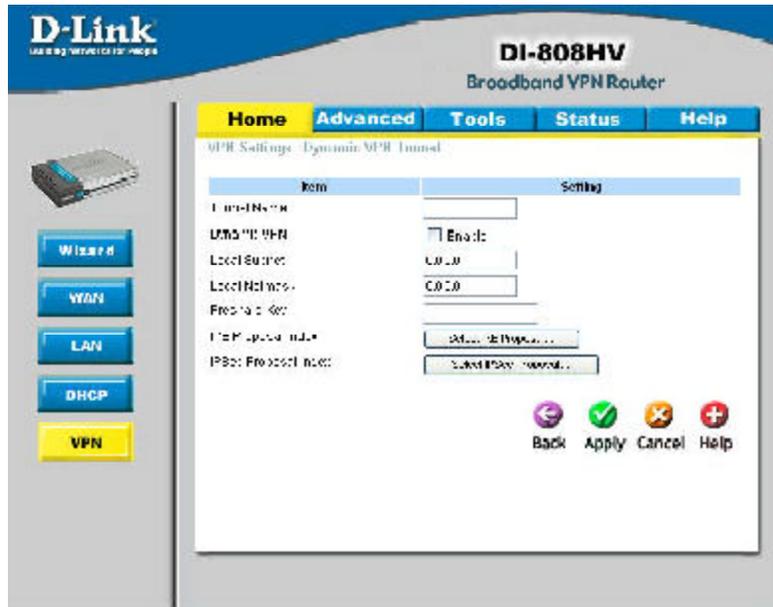
Preshared Key	The first key that supports IKE mechanism of both VPN gateways for negotiating further security keys. The pre-shared key must be the same for both endpoint gateways.
IKE Proposal index	Click the button to setup a set of frequent-used IKE proposals and select from the set of IKE proposals for the dedicated tunnel.
IPSec Proposal index	Click the button to setup a set of frequent-used IPSec proposals and select from the set of IKE proposals for the dedicated tunnel.

42

Using the Configuration Menu
Home >VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal
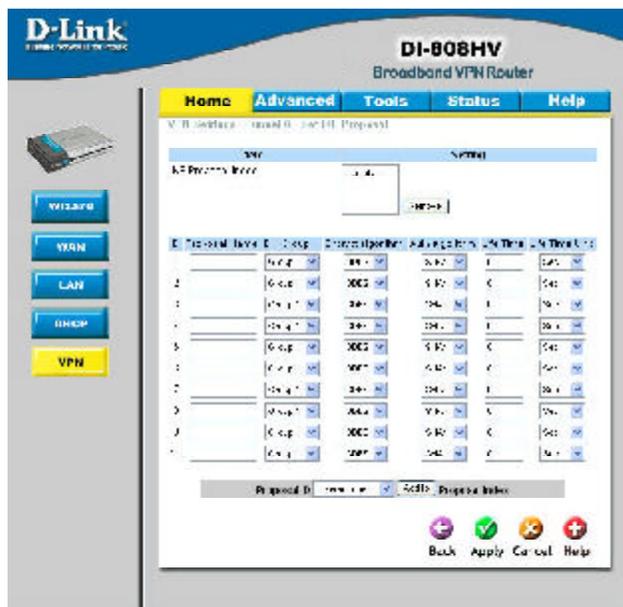
IKE Proposal index A list of selected proposal indexes from the IKE proposal pool listed below.

Proposal Name It indicates which IKE proposal to be focused.

DH Group There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).

Encrypt algorithm There are two algorithms that can be selected: 3DES and DES.

Auth algorithm There are two algorithms that can be selected: SHA1 and MD5.

Using the Configuration Menu

Home >VPN Settings > Dynamic VPN Tunnel > Set IKE Proposal
Continued...

Life Time	Enter in the life time value.
Life Time Unit	There are two units that can be selected: second and KB.
Proposal ID	The identifier of IKE proposal can be chosen for adding corresponding proposal to the dedicated tunnel.
Add to	Click it to add the chosen proposal indicated by proposal ID to IKE Proposal index list.

Using the Configuration Menu

Home >VPN Settings > Dynamic VPN Tunnel > Set IPSEC Proposal

IPSec Proposal index	A list of selected proposal indexes from the IPSec proposal pool listed below.
Proposal Name	This is the name used to classify the IPSec proposal.
DH Group	There are three groups that can be selected: group 1 (MODP768), group 2 (MODP1024), and group 5 (MODP1536).
Encap protocol	There are two protocols that can be selected: ESP and AH.
Encrypt algorithm	There are two algorithms that can be selected: 3DES and DES.
Auth algorithm	There are two algorithms that can be selected: SHA1 and MD5.

Using the Configuration Menu

Life Time	Enter in a life time value.
Life Time Unit	There are two units that can be selected: second and KB.
Proposal ID	The identifier of IPSec proposal can be chosen for adding the proposal to the dedicated tunnel.
Add to	Click it to add the chosen proposal indicated by proposal ID to IPSec Proposal index list.

46

Using the Configuration Menu

Enable L2TP Server Click to enable the L2TP Server function.

Virtual IP of L2TP Server Enter your Virtual IP address to access the L2PT server.

Authentication Protocol Select one of the following authentication protocols: PAP, CHAP, or MSCHAP.

Tunnel Name Current tunnel name.

User Name Enter in the username for the L2TP account.

Password Enter in the password for the L2TP account.

Using the Configuration Menu

Home >VPN Settings >PPTP Server Setting
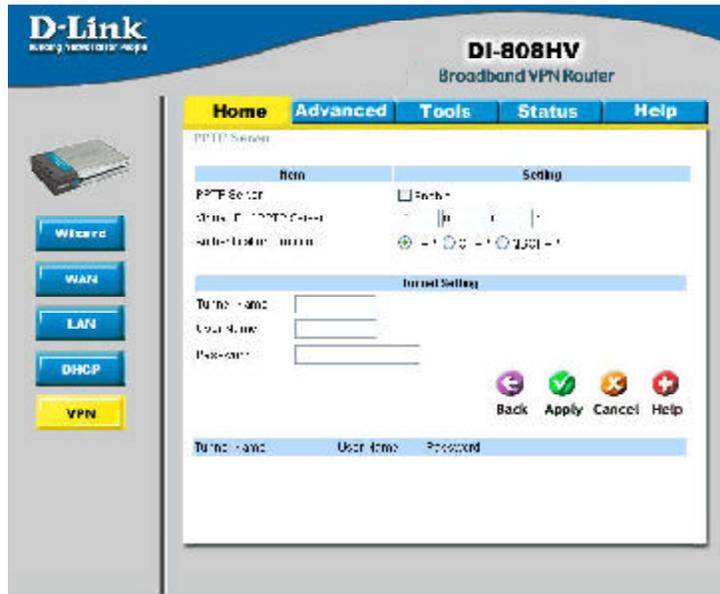
Enable PPTP Server	Click to enable the PPTP Server function.
Virtual IP of PPTP Server	Enter your Virtual IP address to access thePPPT server.
Authentication Protocol	Select one of the following authentication protocols: PAP, CHAP, or MSCHAP.
Tunnel Name	Current tunnel name.
User Name	Enter in the username for the PPTP account.
Password	Enter in the password for the PPTP account.

Using the Configuration Menu
Advanced > Virtual Server
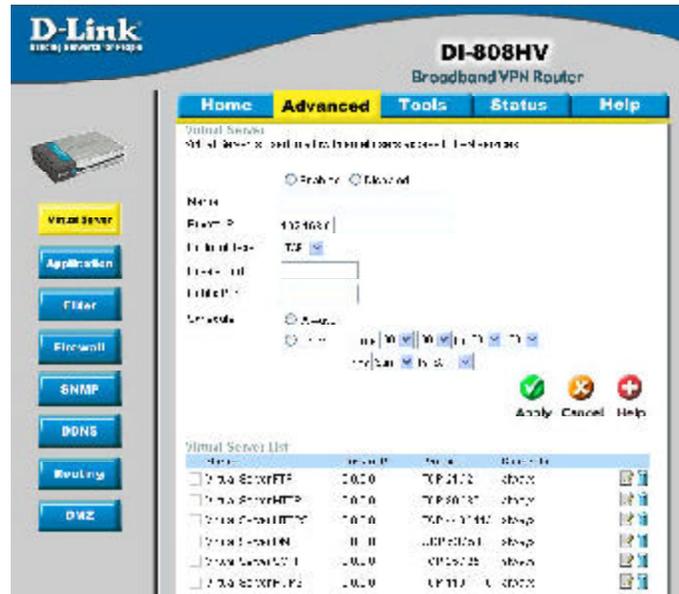
The DI-808HV can be configured as a virtual server so that remote users accessing Web or FTP services via the public IP address can be automatically redirected to local servers in the LAN (Local Area Network).

The DI-808HV firewall feature filters out unrecognized packets to protect your LAN network so all computers networked with the DI-808HV 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-808HV redirects the external service request to the appropriate server within the LAN network.

Name   The name referencing the virtual service.

Private IP   The server computer in the LAN 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 side that will be used to access the virtual service.

Schedule   Select **Always**, or choose **From** and enter the time period during which the virtual service will be available

49

Using the Configuration Menu
Advanced > Application

Some applications require multiple connections, such as Internet gaming, videoconferencing, Internet telephony and others. These applications have difficulty working through NAT (Network Address Translation). *Special Applications* makes some of these applications work with the DI-808HV. If you need to run applications that require multiple connections, specify the port normally associated with an application in the **Trigger Port** field, then enter the public ports associated with the trigger port into the **Public Ports** field.

At the bottom of the screen, there are defined special applications. To use them, select one from the drop down list and select an ID number you want to use. Then click the "Copy to" button and the router will fill in the appropriate information to the list. You will then need to enable the service. If the mechanism of Special Applications fails to make an application work, try using DMZ host instead.

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

Enabled   Select to activate the policy

Trigger Port   This is the port used to trigger the application. It can be either a single port or a range of ports.

Public Ports   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.

50

Using the Configuration Menu
Advanced > Filter > IP Filter

Use IP (Internet Protocol) filters to allow or deny computers access to the Internet based on their IP address.
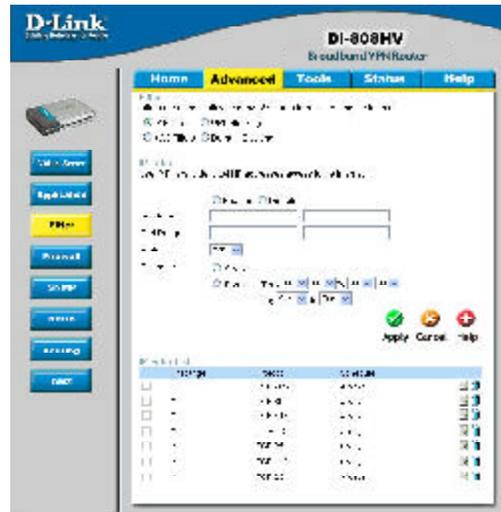
IP Filter
Use IP Filters to deny LAN IP addresses access to the internet

Enabled or Disabled
Click **Enabled** to apply the filter policy or click **Disabled** to enter an inactive filter policy (You can reactivate the policy later.)

IP Address
Enter in the IP address range of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

Port Range
Enter in the port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

Protocol
Select the protocol type to allow or deny certain types of IP addresses.

Schedule
Select **Always**, or choose **From** and enter the time period during which the IP filter policy will be in effect.

Using the Configuration Menu

Advanced > Filter > MAC Filters
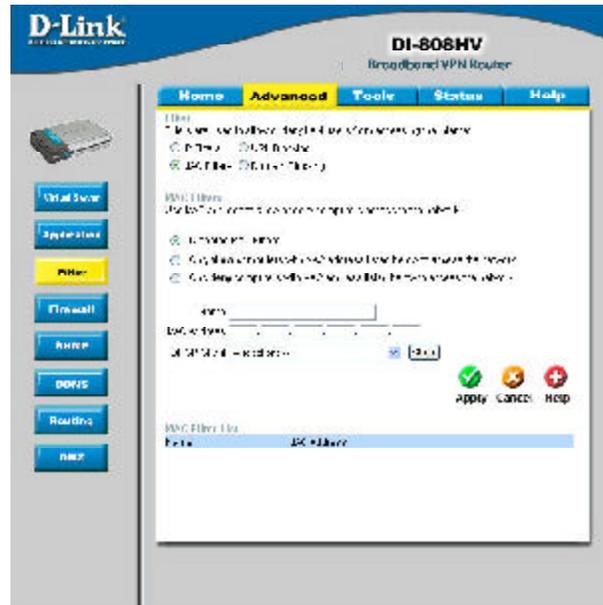
MAC (Media Access Control) Filters are used to allow or deny LAN (Local Area Network) computers from accessing the Internet and network by their MAC address.

At the bottom of the screen, there is a list of MAC addresses from the DHCP client computers connected to the DI-808HV. To use them, select one from the drop down list. Then click the "Apply" button and the DI-808HV will fill in the appropriate information to the list.

Disabled MAC Filter   Select this option if you do not want to use MAC filters.

Only allow computers with MAC address listed below to access the network
Select this option to only allow computers that are in the list to access the network and Internet. All other computers will be denied access to the network and Internet.

Only deny computers with MAC address listed below to access the network
Select this option to only deny computers that are in the list to access the network and Internet. All other computers will be allowed access to the network and Internet.

MAC Address   Enter the **MAC Address** of the client that will be filtered

Using the Configuration Menu
Advanced > Filter > URL Blocking

Use URL Blocking to deny LAN computers from accessing specific web sites by its 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.

Disabled URL Blocking
Select this option if you do not want to use URL Blocking.

Using the Configuration Menu

Advanced > Filter > Domain Blocking

Use Domain Blocking to allow or deny computers access to specific Internet domains whether it is through www, ftp, snmp, etc.

Disabled Domain Blocking
Select this option if you do not want to use Domain Blocking.

Allow users to access all domains except "Blocked Domains"
Select this option to allow users to access the specified Internet domains listed below. Users will be denied access to all other Internet domains.

Deny users to access all domains except "Permitted Domains"
Select this option to deny users to access the specified Internet domains listed below. Users will be allowed access to all other Internet domains.

54

Using the Configuration Menu
Advanced > Firewall

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

Enabled or Disabled
Click **Enabled** to apply the filter policy or click **Disabled** to enter an inactive filter policy (You can reactivate the policy later).

Name
Enter the name of the Firewall Rule.

Action
Select Allow or Deny to allow or deny traffic to pass through the DI-808HV.

Source
Choose between a LAN or WAN source. An asterisk signifies the selection of both sources.

IP Start
The starting IP address for the filter policy. Leaving the field blank selects all IPs.

IP End
The ending IP address for the filter policy. Leaving the field blank sleects all IPs.

Destination
Choose between a LAN or WAN destination. An asterisk signifies the selection of both destinations.

55

Using the Configuration Menu
Advanced > Firewall *Continued*
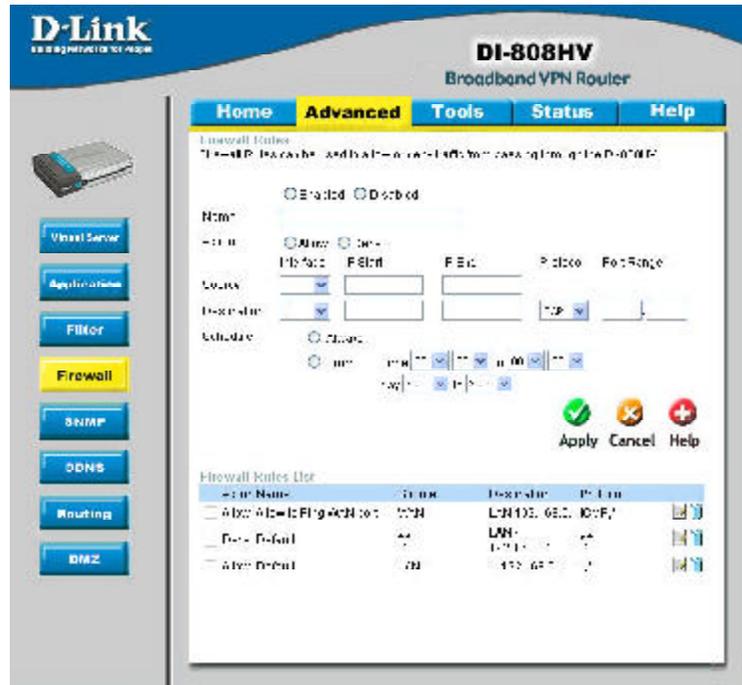
IP Address
Enter in the IP address range of the computers that you want the policy to apply to. If it is only a single computer that you want the policy applied to, then enter the IP address of that computer in the Start Source IP and leave the End Source IP blank.

Protocol
Select one of the following protocols: TCP, UDP, or ICMP.

Port Range
Enter in the port range of the TCP/UDP ports that you want the policy to apply to. If it is only a single port that you want the policy applied to, then enter the port number in the Start Port field and leave the End Port field blank. If you want to use all the ports, you can leave the port range empty.

Schedule
Select **Always**, or choose **From** and enter the time period during which the virtual service will be available.

Using the Configuration Menu
Advanced > SNMP
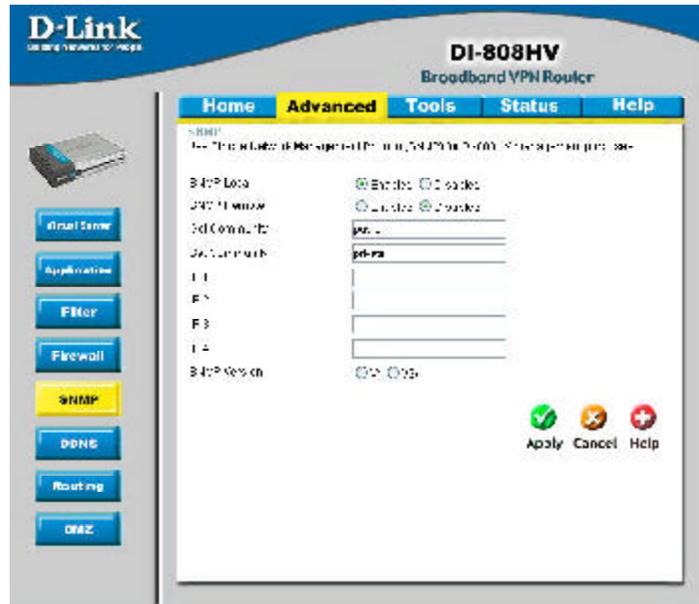
SNMP (Simple Network Management Protocol) is a widely used network monitoring and control protocol that reports activity on each network device to the administrator of the network. SNMP can be used to monitor traffic and statistics of the DI-808HV. The DI-808HV supports SNMP v1 or v2c

Enable SNMP   (Simple Network Management Protocol)

Local   LAN (Local Area Network)

Remote   WAN (Wide Area Network)

Get Community   Enter the password **public** in this field to allow "Read only" access to network administration using SNMP. You can view the network, but no configuration is possible wth this setting.

Set Community   Enter the password **private** in this field to gain "Read and Write" access to the network using SNMP software. The administrator can configure the network with this setting.

SNMP v1   Simple Network Management Protocol (SNMP) is an application layer protocl that facilitates the exchange of management information between nework devices.

SNMP v2   Enhanced version of SNMP v1 with additional protocol operations such as UDP, IP, CLNS, DDP, and IPX.

57

Using the Configuration Menu
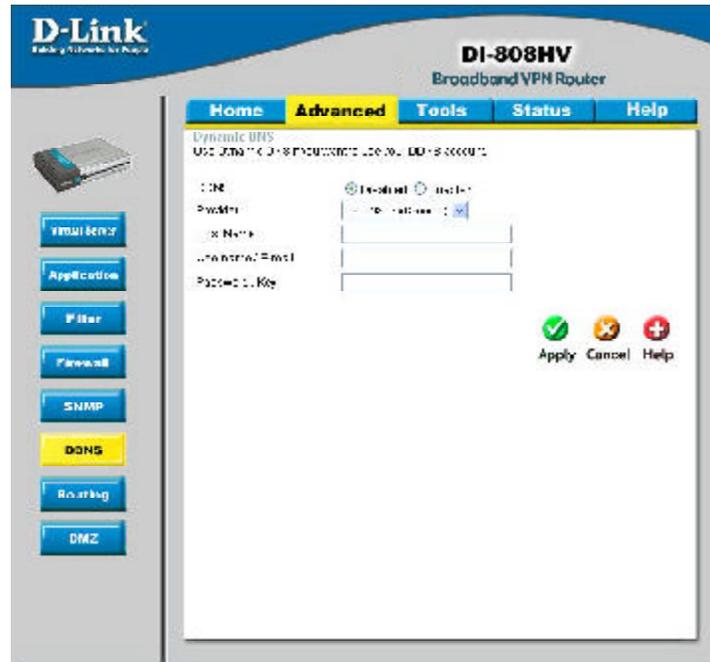
DDNS (Dynamic Domain Name System) keeps dynamic IP addresses (*e.g.*, IP addresses assigned by a DHCP capable router or server) linked to a domain name. Users who have a Dynamic DNS account may use this feature on the DI-808HV.

DDNS   When an IP address is automatically assigned by a DHCP server, DDNS automatically updates the DNS server. Select **Disabled** or **Enabled**

Provider   Select from the pull-down menu

Host Name   Enter the Host name

Username/Email Enter the username or email address

Password/Key   Enter the password or key

58

Using the Configuration Menu

Advanced > Routing

Dynamic Routing Dynamic Routing Settings allow the VPN Router to route IP packets to another network automatically. The RIP protocol is applied, and broadcasts the routing information to other routers on the network regularly.
By default, it is set to disable. Check to enable (RIPv1 / RIPv2) protocol.

RIP v1 Protocol in which the IP address is routed through the internet.

RIP v2 Enhanced version of RIP v1with added features such as Authentication, Routing Domain, Next Hop Fowarding, and Subnet-mask Exchange.

Using the Configuration Menu

Advanced > DMZ

If you have a computer that cannot run Internet applications properly from behind the DI-808HV, then you can allow that computer to have unrestricted Internet access. Enter the IP address of that computer as a DMZ (Demilitarized Zone) host with unrestricted Internet access. Adding a client to the DMZ may expose that computer to a variety of security risks; so only use this option as a last resort.

Using the Configuration Menu

Tools> Admin
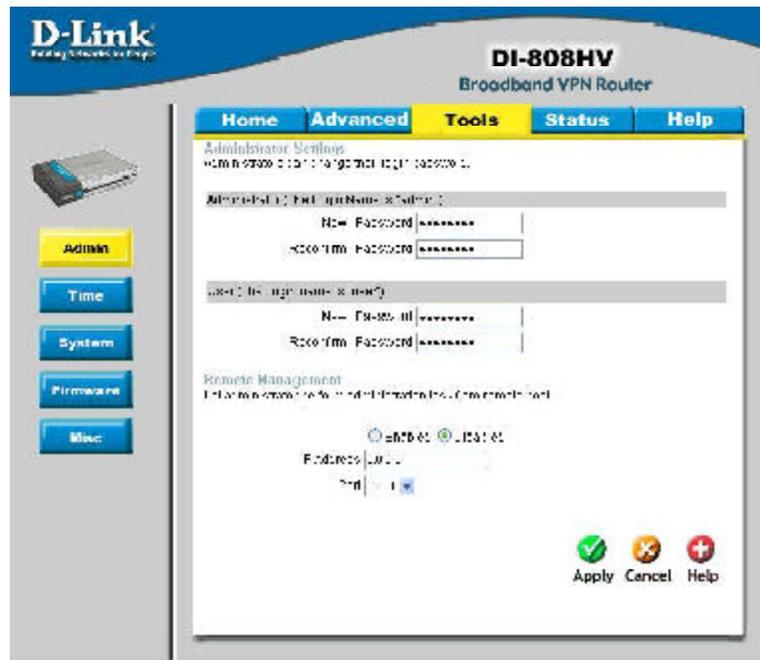
You can change the admin and user passwords here. It is recommended that you change the admin password from the default setting. The default passwords are blank (no password).

Password	To change the passwords, enter the new password twice to confirm.
Remote Management	Remote Management allows the device to be configured through the WAN (Wide Area Network) port from the Internet using a web browser. A username and password is still required to access the browser-based management inter-face.
IP Address	Internet IP Address of the computer that has access to the DI-808HV. If the IP Address is set to 0.0.0.0, this allows all Internet IP addresses to access the DI-808HV.
Port	The port number used to access the DI-808HV. E.g., http://x.x.x.x:8080, where x.x.x.x is the WAN IP address of the DI-808HV and 8080 is the port used for the Web Management interface.

Using the Configuration Menu

Tools> Time
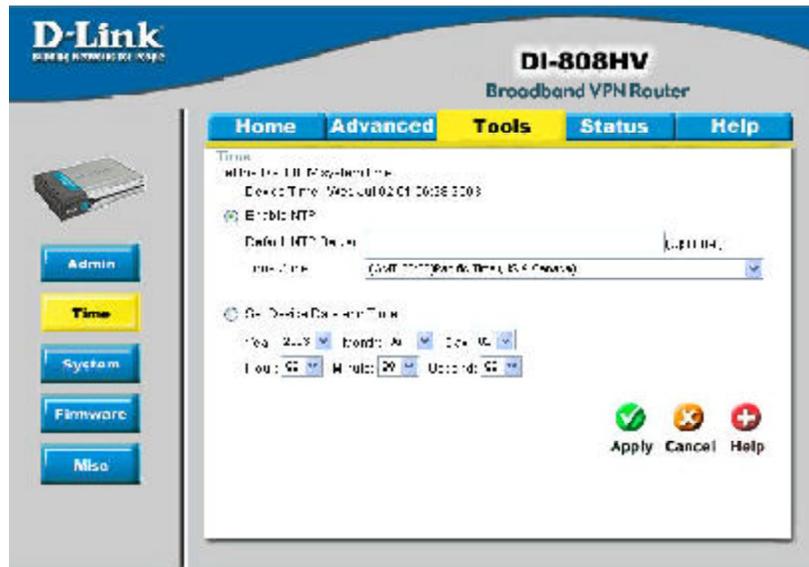
Set the time here by entering it manually or use NTP (Network Time Protocol). NTP is the standard protocol on the Internet that synchronizes the time settings accurately for the DI-808HV.

Enable NTP	Select to enable NTP and synchronize the time settings on your network using an NTP server
Default NTP server	If you are enabling NTP, please enter the link to the default server
Time Zone	Select your time zone from the pull-down menu
Set Device Date and Time	If you are entering the time manually, select the correct Year, Month, Day, Hour, Minute, and Second

Using the Configuration Menu

Tools > System
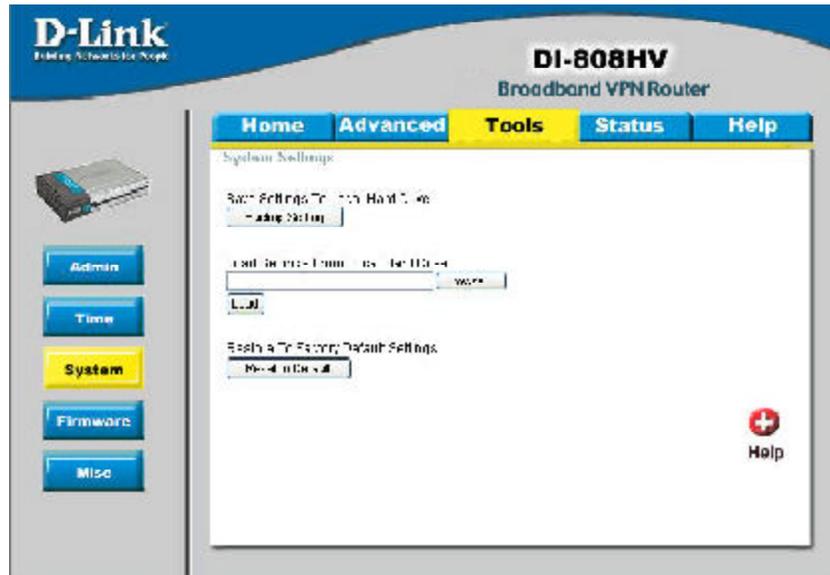
The current system settings can be saved as a file onto the local hard drive. The saved file or any other saved setting file created by the DI-808HV can be uploaded into the unit. To reload a system settings file, click on **Browse** to search the local hard drive for the file to be used. The device can also be reset back to factory default settings by clicking on the **Reset to Default** button. Use the restore feature only if necessary. This will erase previously saved settings for the unit. Make sure to save your system settings to the hard drive before doing a factory reset.

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

Load Settings from Local Hard Drive   Click **Browse** to find the settings file, then click **Load**

Restore to Factory Default Settings   Click **Reset to Default** to restore the factory default settings

Using the Configuration Menu

Tools > Firmware
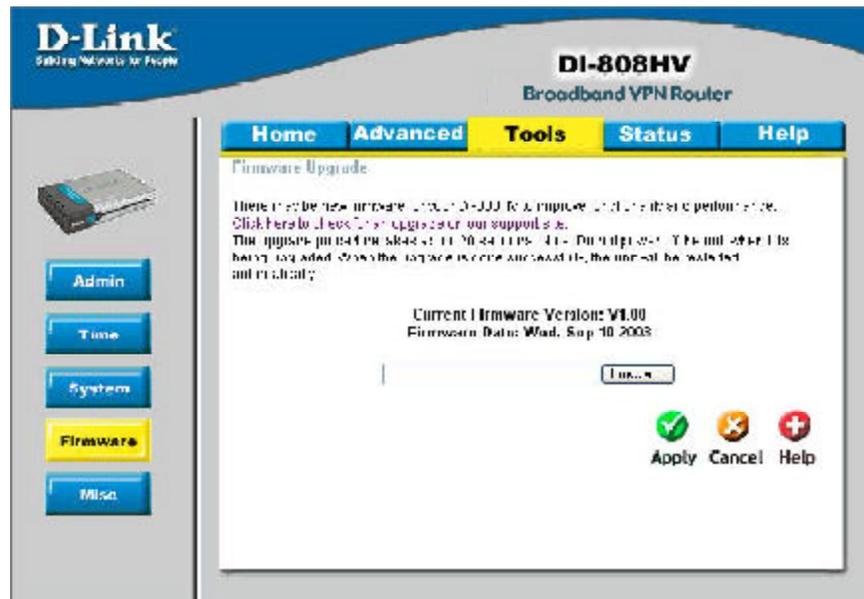
You can upgrade the firmware by using this tool. First, check the D-Link support site for firmware updates at http://support.dlink.com. Make sure that the firmware you want to use is saved on the local hard drive of your computer. Click on **Browse** to search the local hard drive for the firmware that you downloaded from the D-Link website to be used for the update. Upgrading the firmware will not change any of your system settings but it is recommended that you save your system settings before doing a firmware upgrade.

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.

> Note! Do not power off the unit when it is being upgraded. When the upgrade is complete, the unit will restart automatically.

Using the Configuration Menu

Tools > Misc
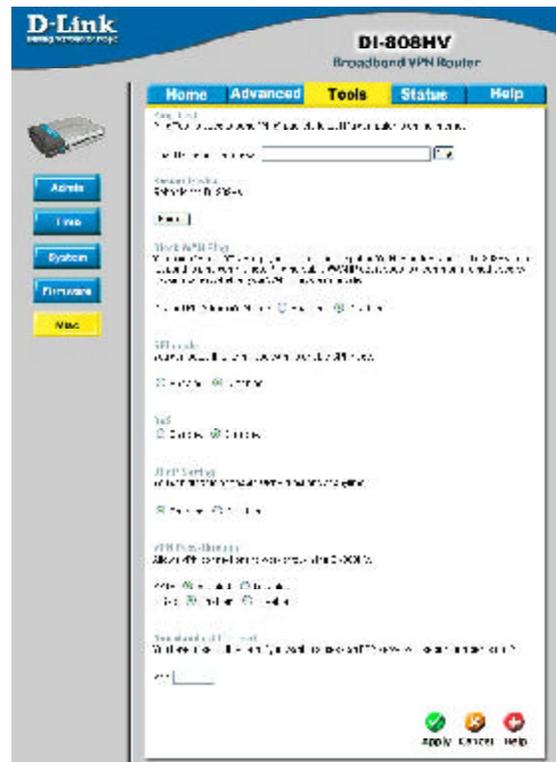
Ping Test In the open box, enter in a URL (i.e., www.dlink.com) or an IP address and click on Ping to test your internet connection.

Restart Device Click Reboot to restart the unit.

Block WAN Ping Click **Enable** to block the WAN ping. Computers on the Internet will not get a reply back from the DI-808HV when it is being "ping"ed. This may help to increase security.

SPI Mode When this feature is enabled, the router will record the packet information passed through the router such as IP address, port address, ACK, SEQ number, and so on. The router will also check every incoming packet to detect if it is valid.

DoS When DoS is enabled, the router will prevent Denial of Service attacks on all computers connected to the DI-808HV.

Using the Configuration Menu
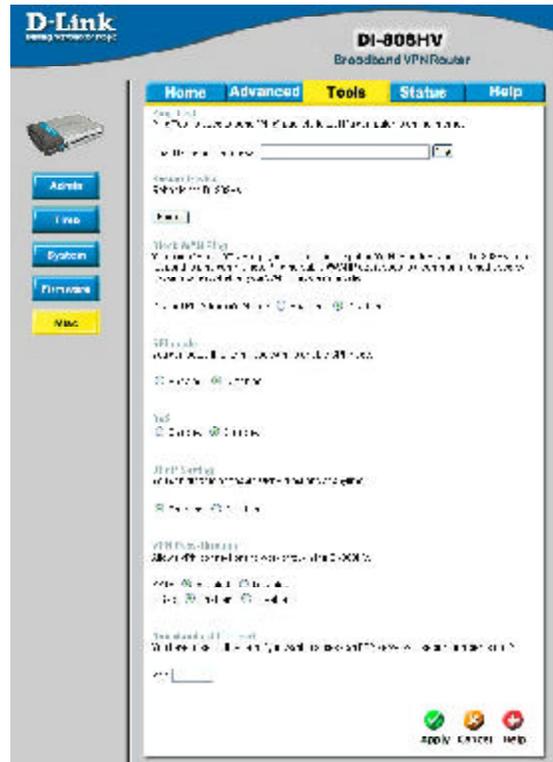
UPnP UPnP is short for **Universal Plug and Play** which is a networking architecture that provides compatibility among networking equipment, software, and peripherals. The DI-808HV is a UPnP enabled router and will only work with other UPnP devices/softwares. If you do not want to use the UPnP Functionality, it can be disabled by selecting "Disabled".

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

Non-standard FTP port If an FTP server you want to access is not using the standard port 21, then enter in the port number that the FTP server is using instead.

66

Using the Configuration Menu

Status > Device Info

This screen displays information about the DI-808HV

DHCP Renew   Click to refresh IP addresses sent from the DHCP server.

DHCP Release   Click to release IP addreses sent from the DHCP server.

Using the Configuration Menu
Status > Log

This screen displays activities occurring on the DI-808HV.

First Page   Click **First Page** to go to the first page of the log.

Last Page   Click **Last Page** to go to the last page of the log.

Previous   Click **Previous** to go to the previous page of the log.

Next   Click **Next** to go to the next page of the log.

Clear   Click **Clear** to clear the current page of the log.

Log Settings   Click for advanced features (see next page).

Using the Configuration Menu
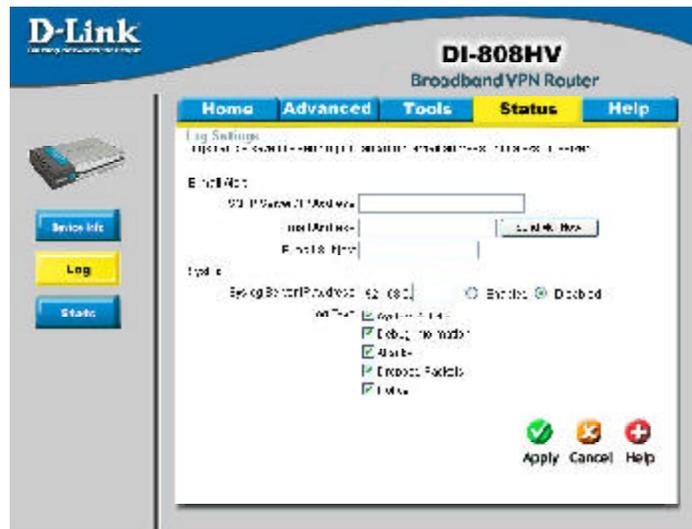
E-Mail Alert	The DI-808HV can be set up to send the log files to a specific email address.
SMTP Server IP	Enter in the IP address of the mail server.
Email Address	Enter in the email address of the recipient who will receive the email log.
Send Mail Now	Click to send mail immediately.
IP Address of the Syslog Server	Enter in the IP address of a syslog server within the network. Click **Enable** to activate the policy. The DI-808HV will send all of it's logs to the specified syslog server.
Log Type	Select the types of activity to log. By default, all values are selected.

Using the Configuration Menu

Status > Stats

In Stats section, traffic statistics are displayed.

Refresh   This will update the page.

Reset   This will reset the packet counter to zero.

WAN-   Displays Received / Transmitted packets from the WAN port.

LAN   Displays Received / Transmitted packets from the LAN port.

Using the Configuration Menu

Help

This screen displays the complete **Help** menu. For help at anytime, click the **Help** tab in the Configuration menu.

Networking Basics

Using the Network Setup Wizard in Windows XP

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

Note: Please refer to websites such as http://www.homenethelp.com and http://www.microsoft.com/windows2000 for information about networking computers using Windows 2000, ME or 98.

Go to **Start>Control Panel>Network Connections**
Select **Set up a home or small office network**
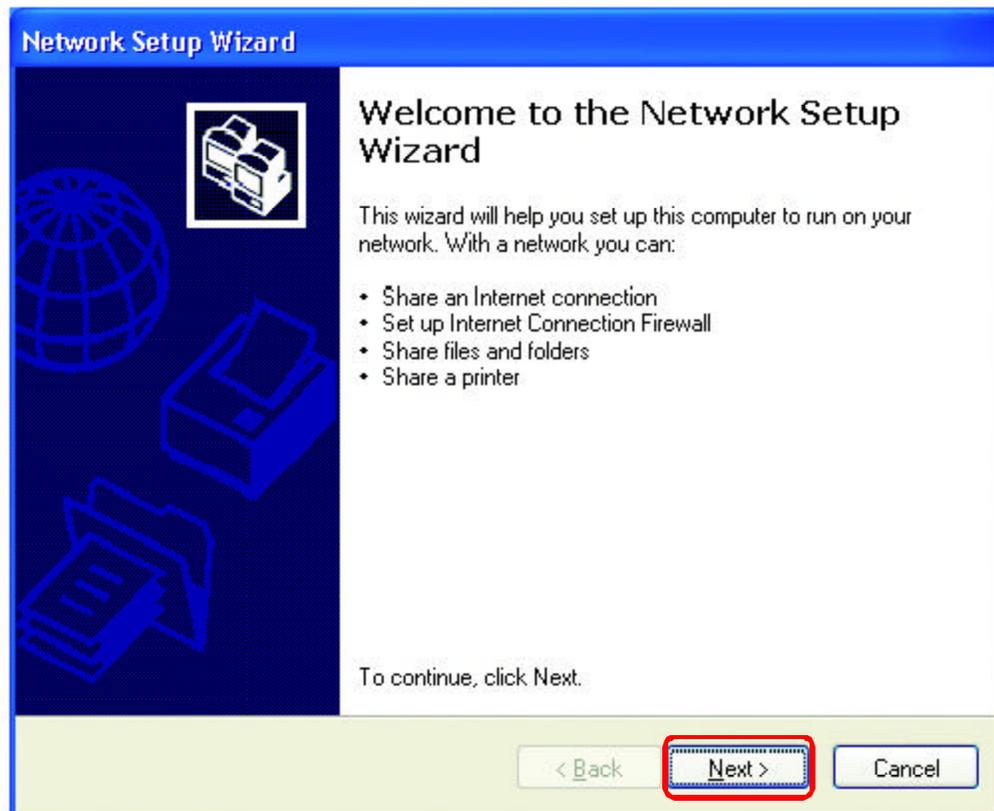
To Continue, **Click Next.**

Networking Basics

Please follow all the instructions in this window:
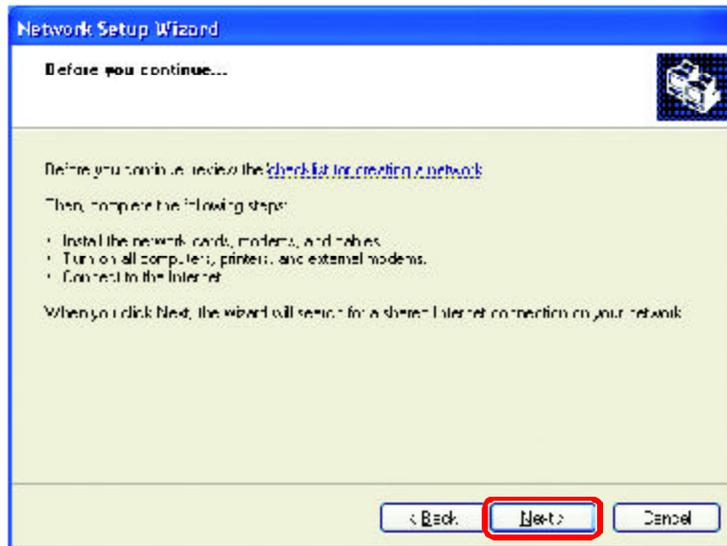
Click **Next**

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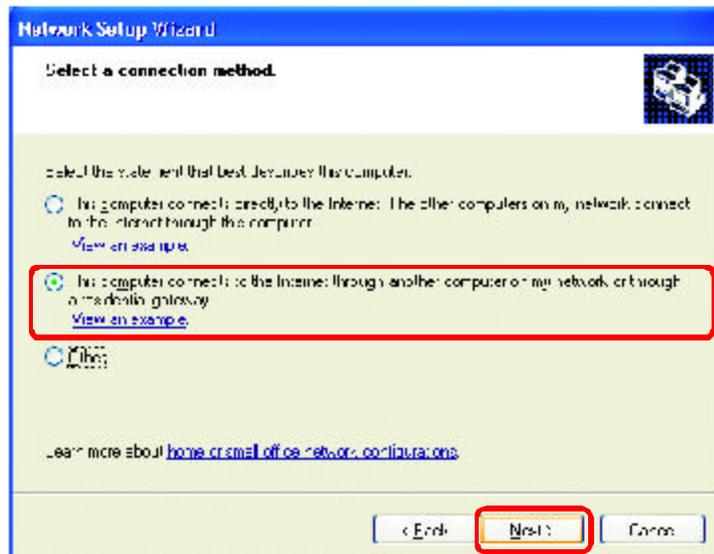
Click **Next**

Networking Basics

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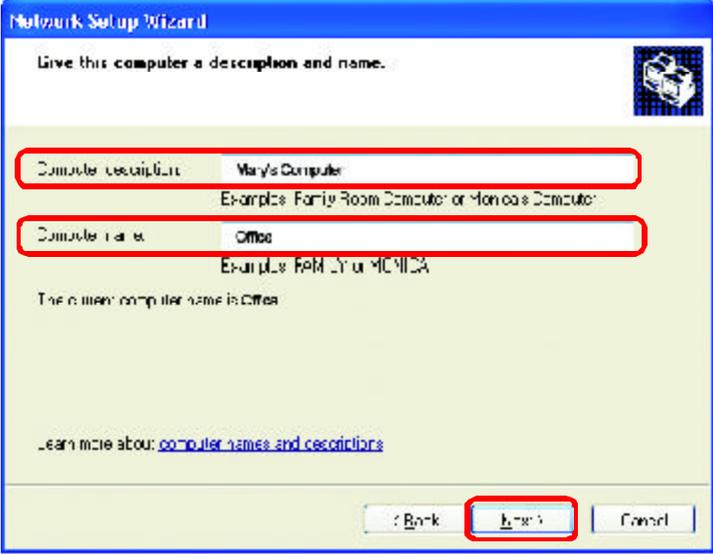
Click **Next**

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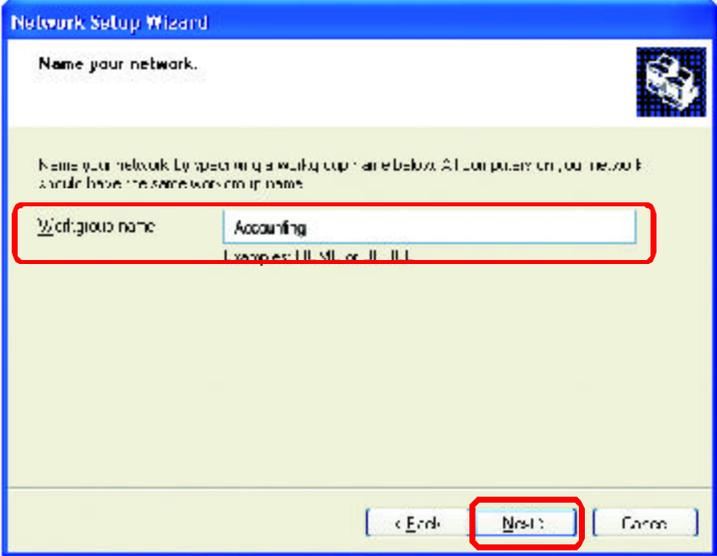
Click **Next**

Networking Basics

Please wait while the **Network Setup Wizard** applies the changes.
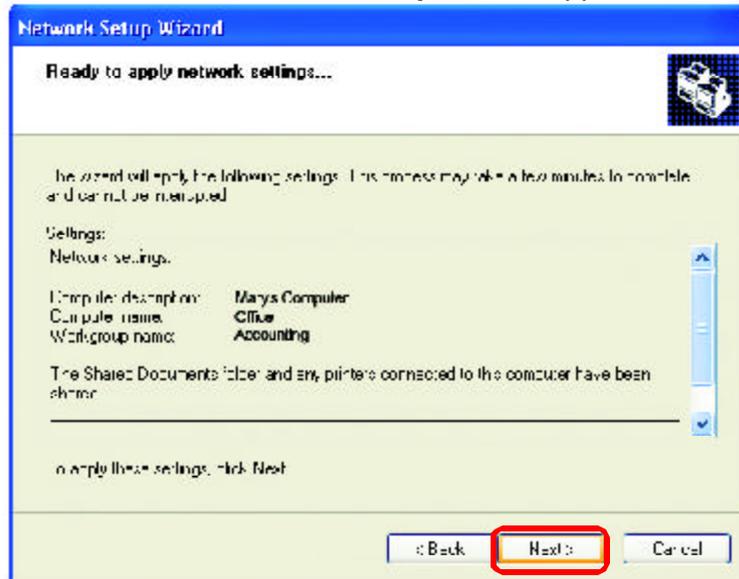
When the changes are complete, click **Next**.

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

Networking Basics

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

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

Networking Basics

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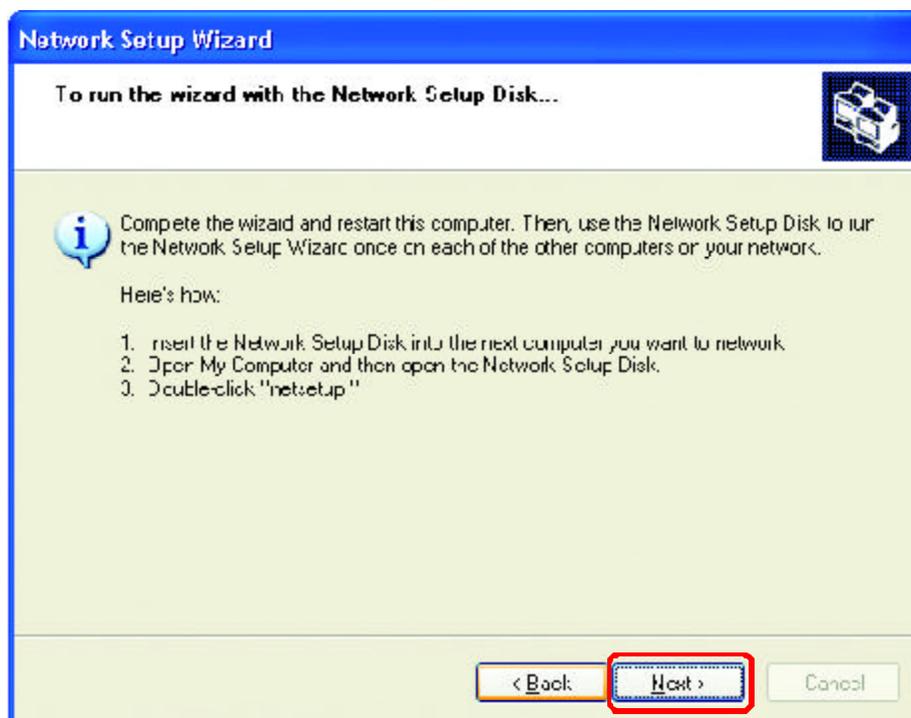
Networking Basics

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

The new settings will take effect when you restart the computer. Click **Yes** to restart the computer.
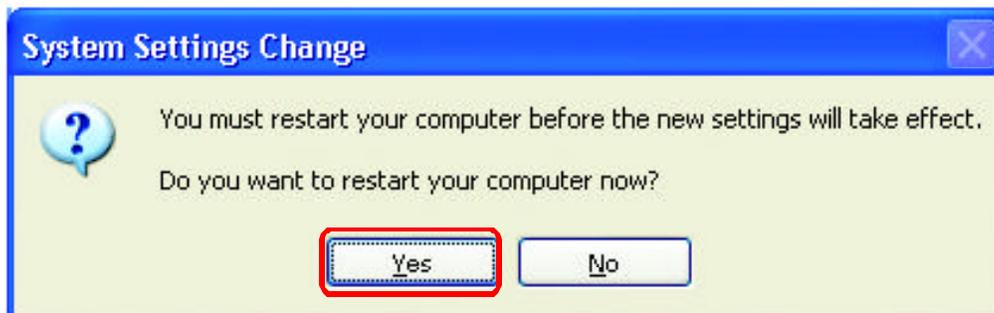
You have completed configuring this computer. Next, you will need to run the **Network Setup Disk** on all the other computers on your network. After running the **Network Setup Disk** on all your computers, your new network will be ready to use.

78

Networking Basics
Naming your Computer

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

- **Click Start** (in the lower left corner of the screen)

- **Right-click** on **My Computer**

- Select **Properties** and click

- Select the **Computer Name Tab** in the System Properties window.
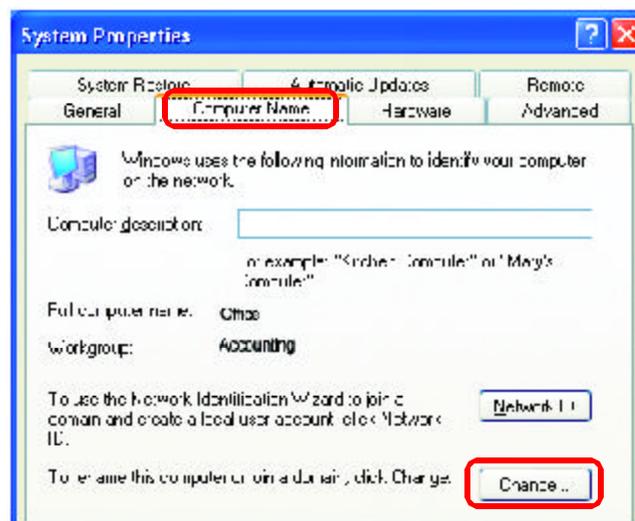
- You may enter a **Computer Description** if you wish; this field is optional.

- To rename the computer or join a domain, Click **Change**.

Networking Basics
Naming your Computer

■ In this window, enter the **Computer name**

■ Select **Workgroup** and enter the name of the **Workgroup**

■ All computers on your network must have the same **Workgroup** name.

■ Click **OK**
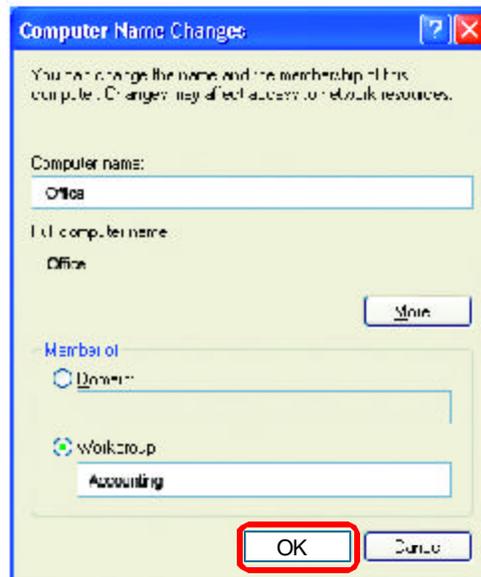
Checking the IP Address in Windows XP

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

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

■ Click on **Status**

Networking Basics
Checking the IP Address in <u>Windows XP</u>

This window will appear.

■ Click the
   Support tab

■ Click **Close**
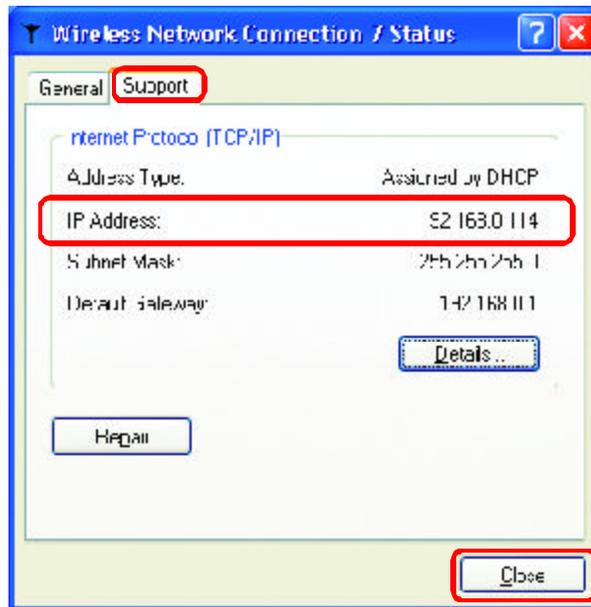
Assigning a Static IP Address in <u>Windows XP/2000</u>

***Note: Residential gateways/broadband routers will automatically assign IP addresses
to the computers on the network, using DHCP (Dynamic Host Configuration Proto-
col) technology. If you are using a DHCP-capable gateway/router you will not need
to assign static IP addresses.***

If you are not using a DHCP capable gateway/router, or you need to assign a static IP
address, please follow these instructions:

■ Go to **Start**

■ Double-click on
   Control Panel

Networking Basics
Assigning a Static IP Address in <u>*Windows XP/2000*</u>

■ Double-click on
   **Network
   Connections**
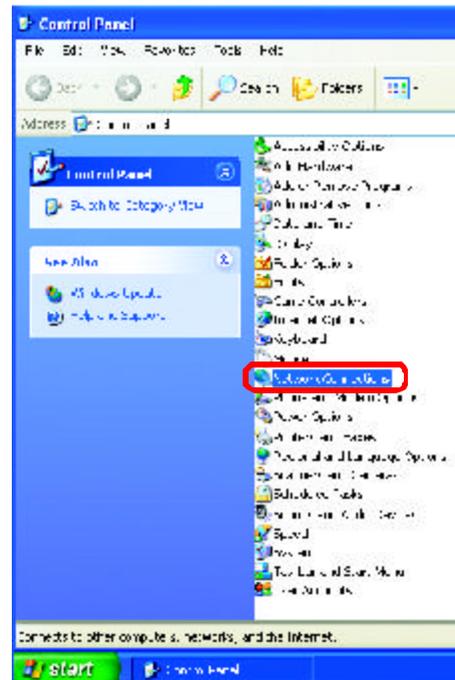
■ Right-click on **Local Area
   Connections**

■ Click on **Properties**
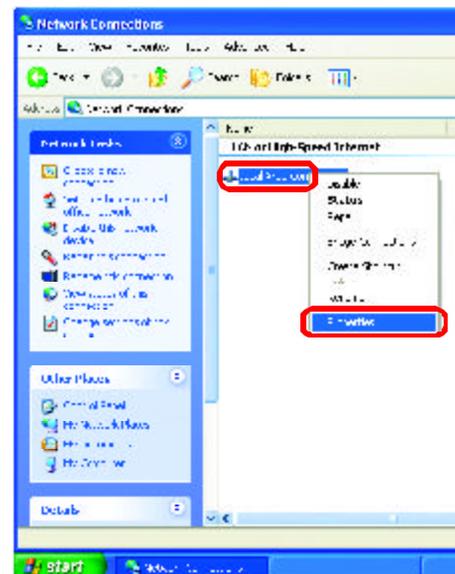
Networking Basics
Assigning a Static IP Address in <u>Windows XP/2000</u>

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

■ Click **Properties**

■ In the window below, input your **IP address, subnet mask, default gateway and DNS server address.** (The IP Addresses on your network must be within the same range. For example, if one computer has an IP address of 192.168.0.2, the other computers should have IP addresses that are sequential, like 192.168.0.3 and 192.168.0.4. The subnet mask must be the same for all the computers on the network.)

> **IP Address:**
> e.g., 192.168.0.2
>
> **Subnet Mask:**
> 255.255.255.0
>
> Enter the LAN IP address of the wireless router. (D-Link wireless routers have a LAN IP address of 192.168.0.1)

■ Select **Use the following DNS server addresses.**

Enter the LAN IP address of the wireless router. (D-Link wireless routers have a LAN IP address of 192.168.0.1)

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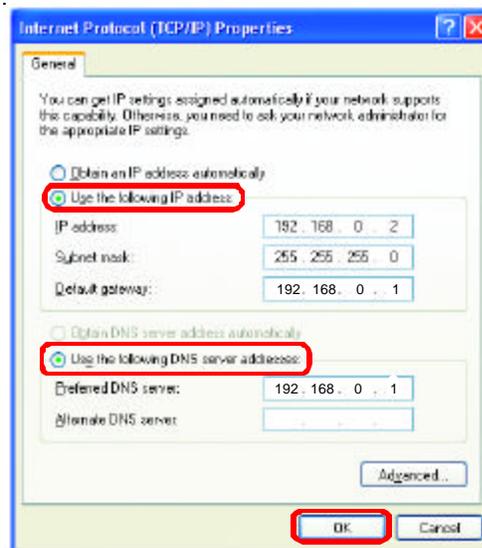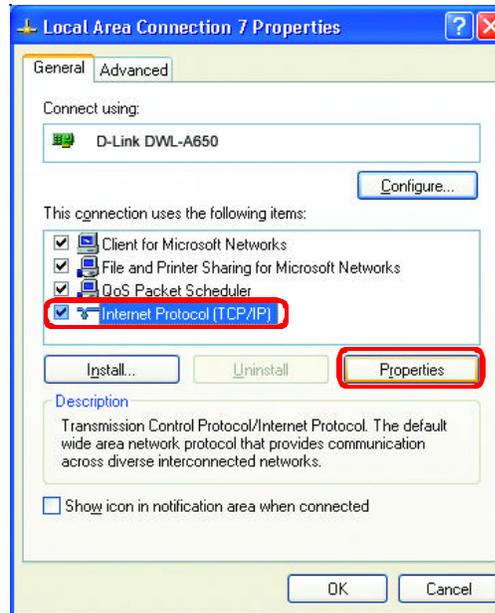
The DNS server information will be supplied by your ISP (Internet Service Provider).

Networking Basics
Assigning a Static IP Address with <u>Macintosh OSX</u>
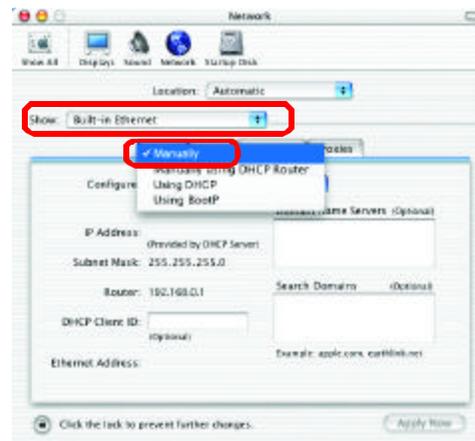
■ Go to the **Apple Menu** and se-
lect **System Preferences**
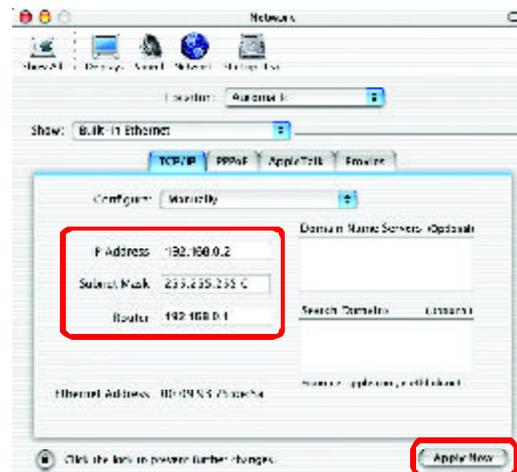
■ Click on **Network**

■ Select **Built-in Ethernet** in the
Show pull-down menu

■ Select **Manually** in the **Con-
figure** pull-down menu

■ Input the **Static IP Address**,
the **Subnet Mask,** and the
Router IP Address in the ap-
propriate fields

■ Click **Apply Now**

84

Networking Basics
Selecting a Dynamic IP Address with <u>*Macintosh OSX*</u>

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

- Click on **Network**

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

- Select **Using DHCP** in the **Configure** pull-down menu
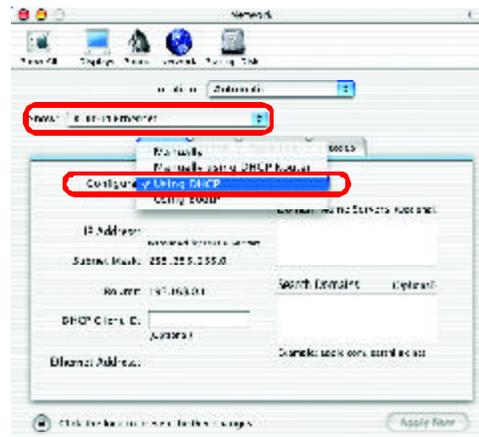
- Click **Apply Now**

- The **IP Address, Subnet mask**, and the **Router's IP Address** will appear in a few seconds
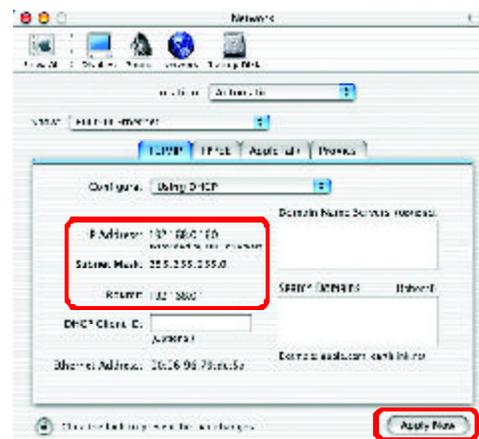
Networking Basics
Adding and Sharing Printers in <u>Windows XP</u>

After you have run the **Network Setup Wizard** on all the computers in your network (please see the **Network Setup Wizard** section at the beginning of **Networking Basics**), you can use the **Add Printer Wizard** to add or share a printer on your network.

Whether you want to add a **local printer** (a printer connected directly to one computer), share an **LPR printer** (a printer connected to a print server), or share a **network printer** (a printer connected to your network through a gateway/router), use the **Add Printer Wizard**. Please follow the directions below:

First, make sure that you have run the <u>Network Setup Wizard</u> on all of the computers on your network.

On the following pages, we will show you these 3 ways to use the **Add Printer Wizard:**

1. Adding a local printer

2. Sharing an network printer

3. Sharing an LPR printer

(Other Networking Tasks)

For help with other tasks, that we have not covered here, in home or small office networking, see **Using the Shared Documents** folder and **Sharing files and folders** in the **Help and Support Center** in Microsoft **Windows XP**.
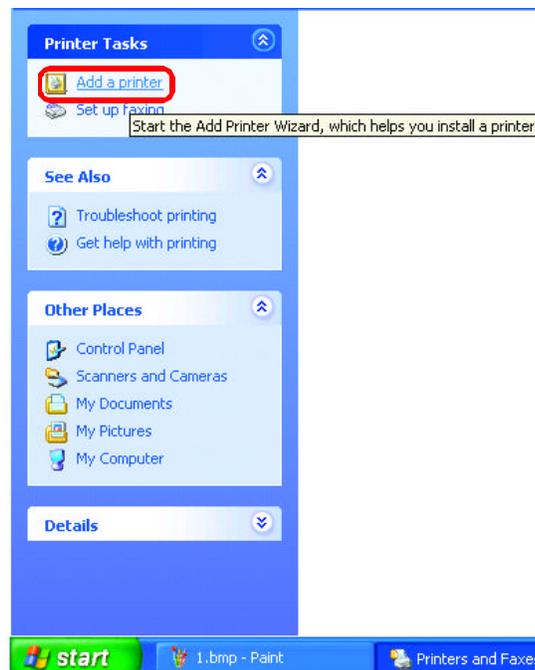
Networking Basics
Adding a local printer (a printer connected directly to a computer)

A printer that is not shared on the network and is connected directly to one computer is called a **local printer**. If you do not need to share your printer on a network, follow these directions to add the printer to one computer.

■ Go to
  Start>
  Printers
 **and Faxes**
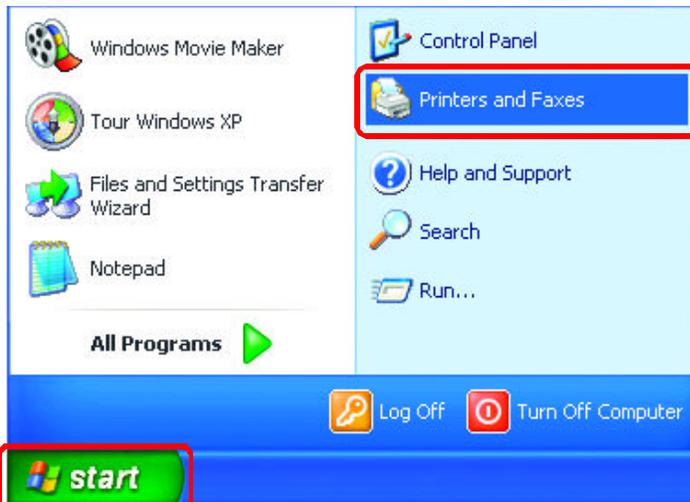
■ Click on **Add a printer**

Networking Basics
Adding a local printer

■ Click **Next**

■ Select **Local printer attached to this computer**

■ (Deselect **Automatically detect and install my Plug and Play printer** if it has been selected.)

■ Click **Next**

■ Select **Use the following port:**

■ From the pull-down menu **select the correct port** for your printer

(Most computers use the **LPT1:** port, as shown in the illustration.)

■ Click **Next**
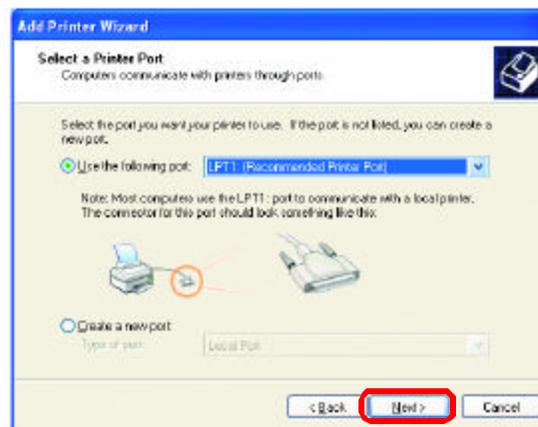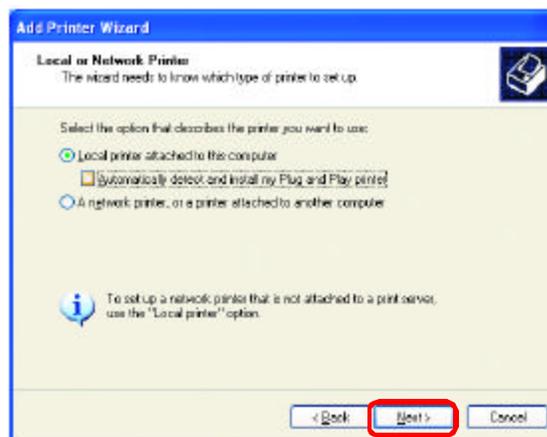
Networking Basics
Adding a local printer

- Select and highlight the **correct driver** for your printer.
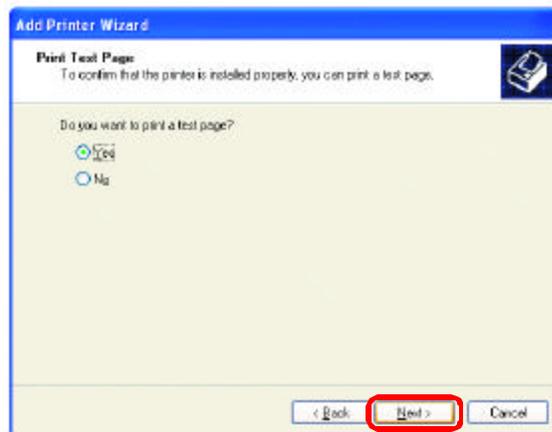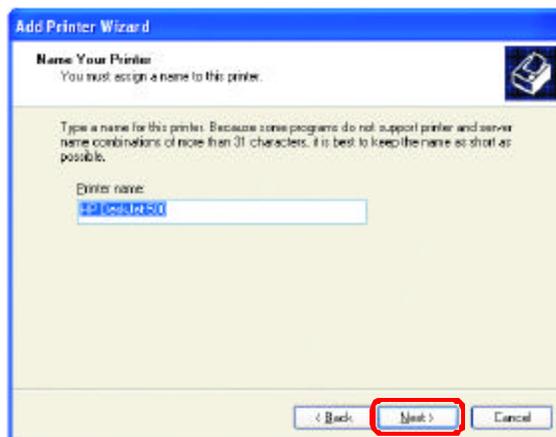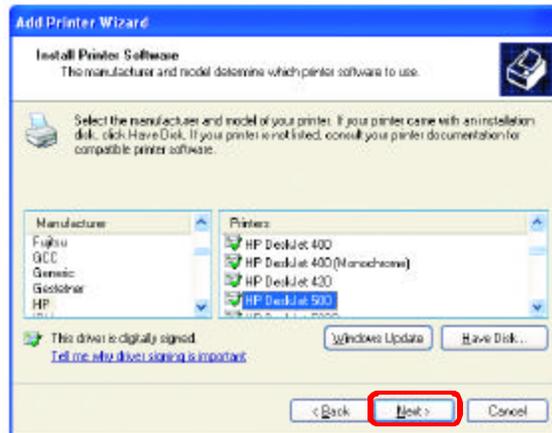
- Click **Next**

  *(If the correct driver is not displayed, insert the CD or floppy disk that came with your printer and click **Have Disk**.)*

- At this screen, you can change the name of the printer (optional).

- Click **Next**

- Select **Yes**, to print a test page. A successful printing will confirm that you have chosen the correct driver.
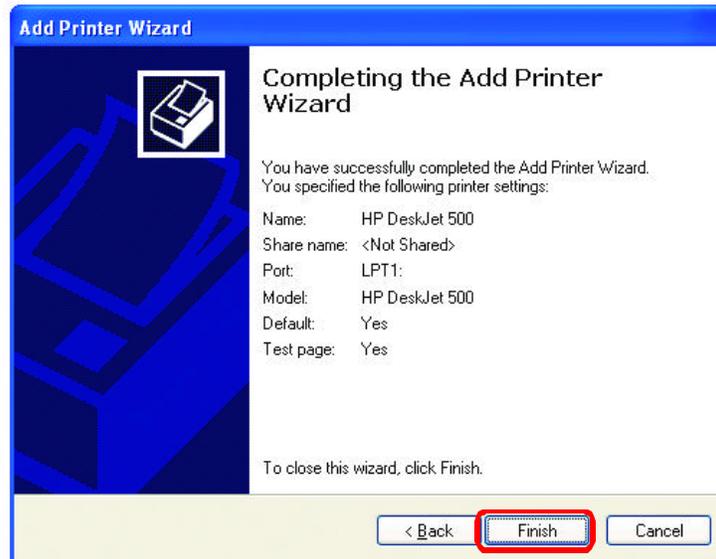
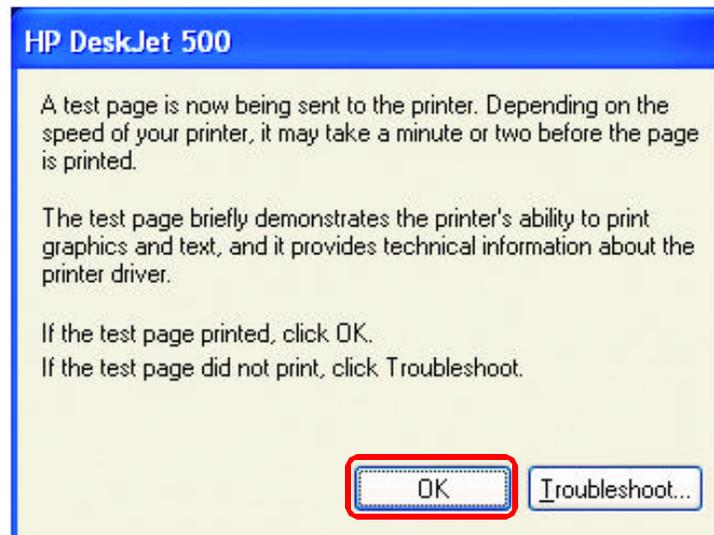- Click **Next**

Networking Basics
Adding a local printer

This screen gives you information about your printer.

Click **Finish**

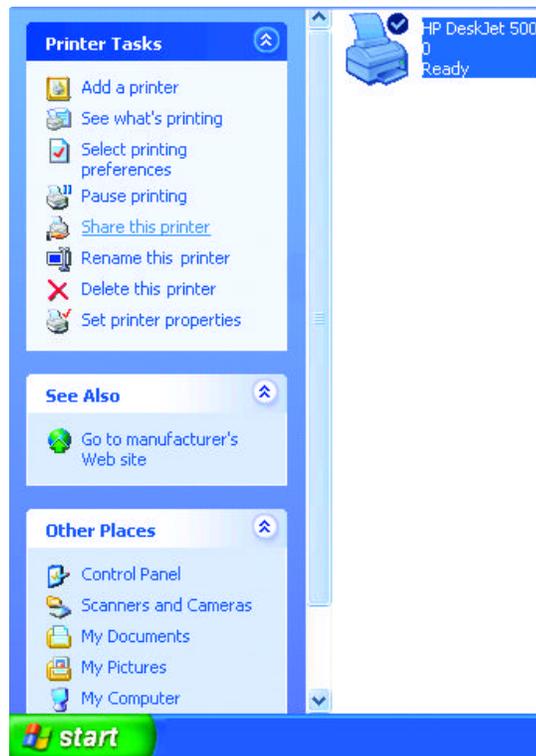When the test page has printed,

Click **OK**

Networking Basics
Adding a local printer

■ Go to **Start**> **Printers and Faxes**

A successful installation will display the printer icon as shown at right.
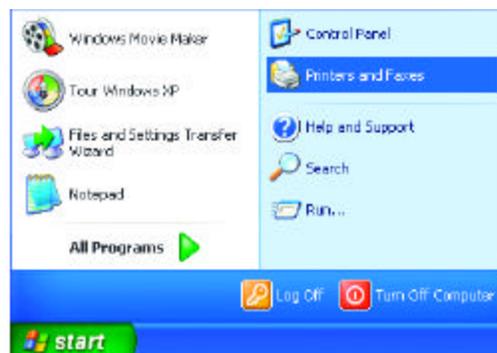
You have successfully added a local printer.

Sharing a network printer

After you have run the **Network Setup Wizard** on all the computers on your network, you can run the **Add Printer Wizard** on all the computers on your network. Please follow these directions to use the **Add Printer Wizard** to share a printer on your network:

■ Go to **Start**> **Printers and Faxes**
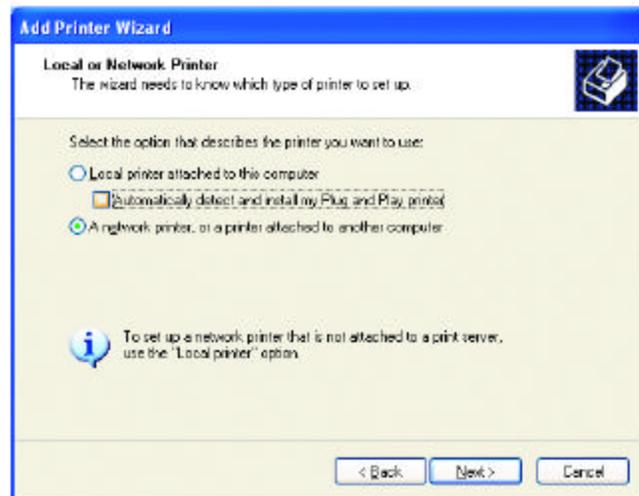
Networking Basics
Sharing a network printer

■ Click on
Add a printer

Printer Tasks ⌃

🖼 Add a printer

🖨 Set up faxing

Start the Add Printer Wizard, which helps you install a printer.

Add Printer Wizard

Welcome to the Add Printer Wizard

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

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

To continue, click Next.

< Back   Next >   Cancel

■ Click **Next**

Add Printer Wizard

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

■ Select
Network Printer

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

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

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

< Back   Next >   Cancel

■ Click **Next**

92

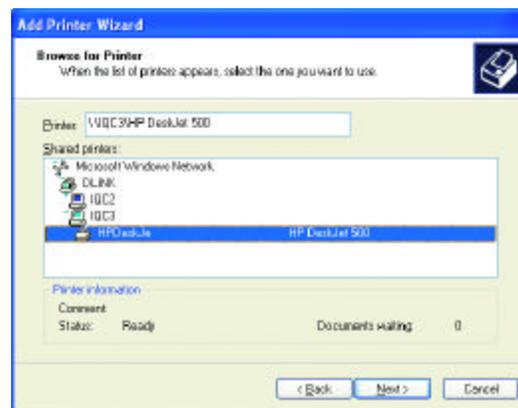## Networking Basics
Sharing a network printer

■ Select **Browse for a printer**

■ Click **Next**

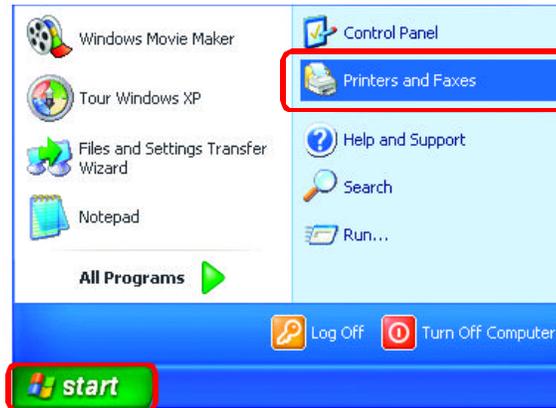Select the **printer** you would like to share

■ Click **Next**

■ Click **Finish**

Networking Basics
Sharing a network printer

■ To check for proper installation:

■ Go to **Start** > **Printers and Faxes**

The printer icon will appear at right, indicating proper installation.

You have completed adding the printer.

To share this printer on your network:

■ Remember the **printer name**

■ Run the **Add Printer Wizard** on all the computers on your network

■ Make sure you have already run the **Network Setup Wizard** on all the network computers

After you run the **Add Printer Wizard** on all the computers in the network, you can share the printer.

94
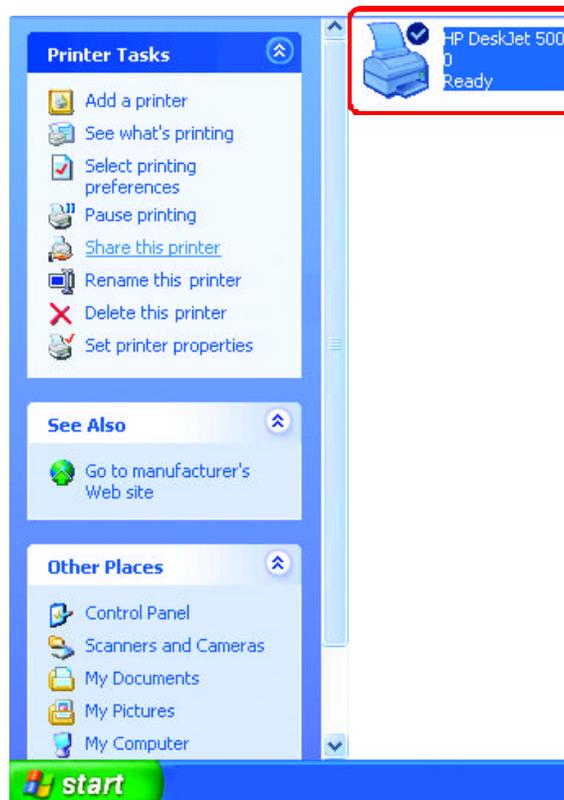
Networking Basics
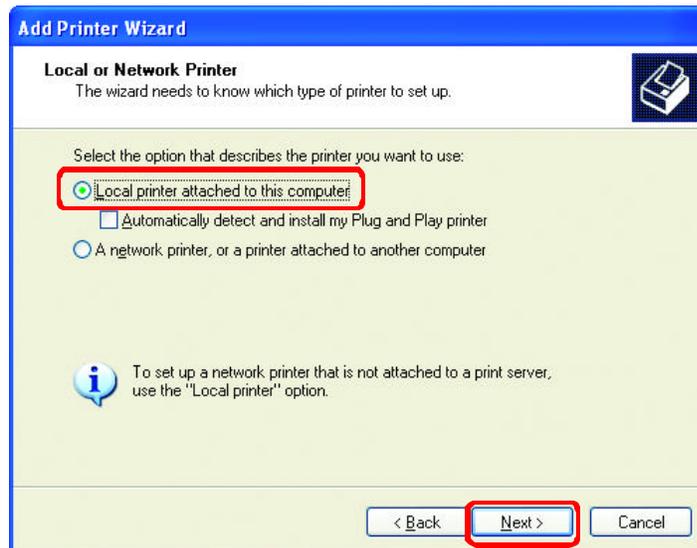### *Sharing an LPR printer*

To share an **LPR printer** (using a print server,) you will need a Print Server such as the **DP-101P+**. Please make sure that you have run the **Network Setup Wizard** on all the computers on your network. To share an **LPR printer**, please follow these directions:

- Go to **Start** > **Printers and Faxes**

- Click on **Add a Printer**
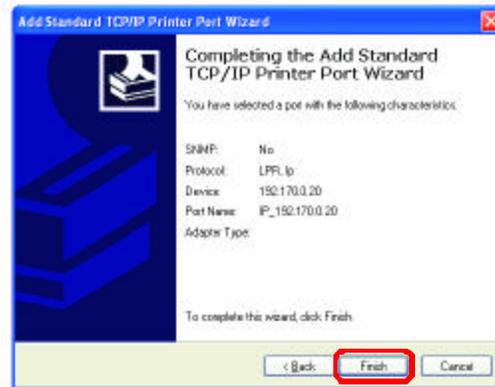
The screen to the right will appear

- Click **Next**

- Select **Local Printer...**

- Click **Next**

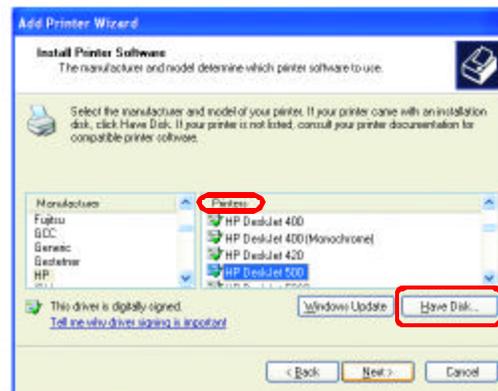95

Networking Basics
Sharing an LPR printer

■ This screen will show you information about your printer.

■ Click **Finish**

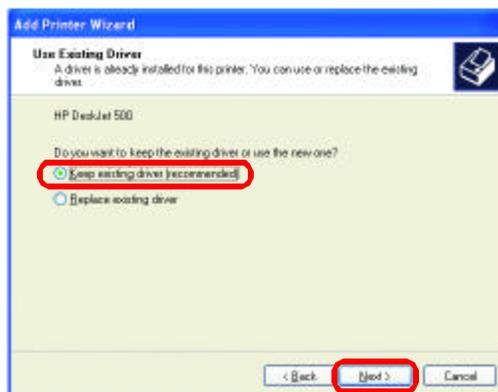■ Select the **printer** you are adding from the list of **Printers**.

■ Insert the printer driver disk that came with your printer.

■ Click **Have Disk**

If the printer driver is already installed, do the following:
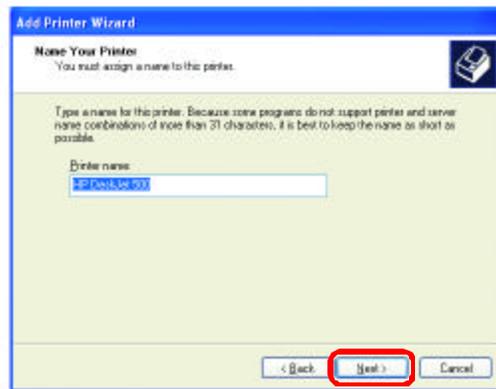
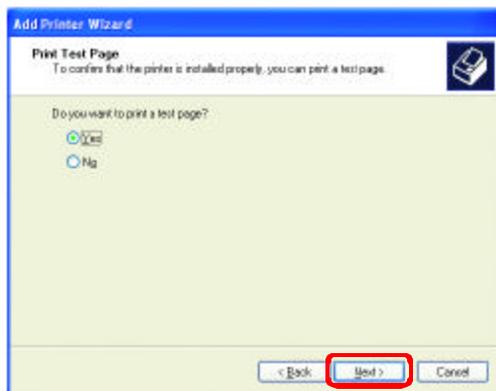■ Select **Keep existing driver**

■ Click **Next**

Networking Basics
Sharing an LPR printer

■ You can rename your printer if you choose. It is optional.

■ *Please remember the name of your printer. You will need this information when you use the **Add Printer Wizard** on the other computers on your network.*
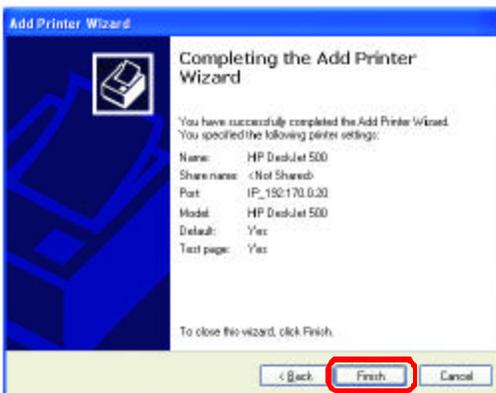
■ Click **Next**

■ Select **Yes**, to print a test page.

■ Click **Next**

This screen will display information about your printer.

■ Click **Finish** to complete the addition of the printer.

■ Please run the **Add Printer Wizard** on all the computers on your network in order to share the printer.

*Note: You must run the **Network Setup Wizard** on all the computers on your network before you run the **Add Printer Wizard**.*

97

Resetting the DI-808HV to the Factory Default Settings

After you have tried other methods for troubleshooting your network, you may choose to **Reset** the DI-808HV to the factory default settings.

To hard-reset the D-Link DI-808HV to the Factory Default Settings, please do the following:

- Locate the **Reset** button on the back of the DI-808HV.

- Use a paper clip to press the **Reset** button and power on.

- Hold for about 5 seconds (do not hold for too long) and then release. (Or, release when M1 and M2 flash at the same time.)

- After you have completed the above steps, the DI-808HV will be reset to the factory default settings.

Technical Specifications

Standards

- IEEE 802.3 10BASET-T Ethernet
- IEEE 802.3u 100BASE-TX Fast Ethernet
- IEEE 802.3x Flow Control
- ANSI/IEEE 802.3 NWay auto-negotiation

VPN Pass Through Function

- PPTP
- L2TP
- IPSec

Device Management

- Web-Based – Internet Explorer 6x or later; Netscape Navigator 6x or later; or other Java- enabled browsers.

LEDs

- WAN
- LAN
- M1
- M2
- COM

Operating Temperature

- 41°F to 131°F (5°C to 55°C)

Humidity

- 10-90%

Power

- 5V DC

Dimensions

- L = 9.25 inches (233mm)
- W = 6.5 inches (165mm)
- H = 1.375 inches (35mm)

Weight

- ~2.0oz. (907g)

Ports

- 4 x NWay 10Base-T/100Base-TX Fast Ethernet LAN (Media Auto Sensing)
- 1 x NWay 10Base-T/100Base-TX Fast Ethernet WAN (Media Auto Sensing)
- 1 COM Port (Dial-up Modem)

Frequently Asked Questions

> **Why can´t I access the Web-based configuration?**

When entering the IP Address of the DI-808HV (192.168.0.1), you are not connecting to the Internet or have to be connected to the Internet. The device has the utility built-in to a ROM chip in the device itself. Your computer must be on the same IP subnet to connect to the web-based utility.

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

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

What type of cable should I be using?

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

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

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

> **Why can´t I access the Web-based configuration? (continued)**

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

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

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

*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

101

Frequently Asked Questions (continued)

### Why can´t I access the Web-based configuration? (continued)

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

Step 3 Configure your Internet settings.

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

> Click to the **Connection** tab and set the dial-up option to **Never Dial a Connection**. Click the **LAN Settings** button
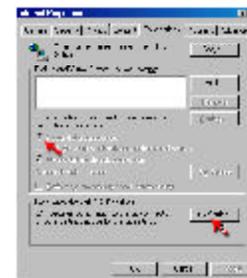
> Nothing should be checked. Click **OK**

> Go to the **Advanced** tab and click the **Restore Defaults** button to restore these settings to their facotry defaults

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

102

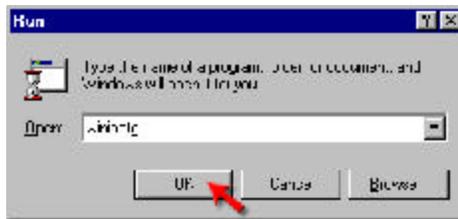## Frequently Asked Questions (continued)

> ### Why can´t I access the Web-based configuration? (continued)

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?

Step 1 Click on **Start**, then click on **Run**.

Step 2 The Run Dialogue Box will appear. Type **winipcfg** in the text field and click **OK**.

Step 3 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.

Step 4 After selecting your adapter, it will display your IP Address, subnet mask, and default gateway.

Step 5 Click **OK** to close the IP Configuration window

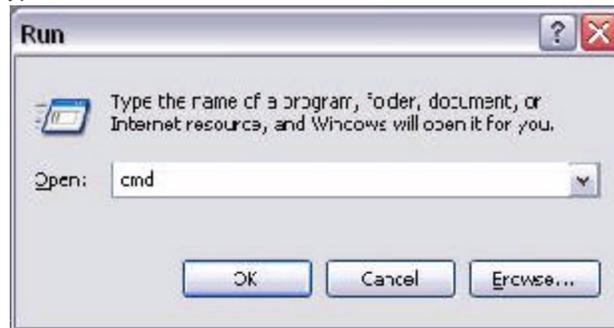103

Frequently Asked Questions (continued)

> **Why can´t I access the Web-based configuration? (continued)**

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

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

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

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

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

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

Frequently Asked Questions (continued)

> **Why can´t I access the Web-based configuration? (continued)**

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

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

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

Step 1
Click on **Start > Control Panel > Network and Internet Connections > Network connections**.
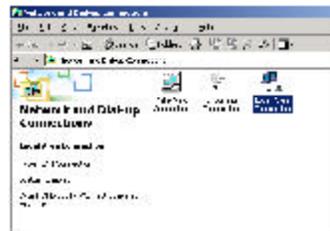
Step 2 See Step 2 for Windows 2000 and continue from there.

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

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

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

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

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

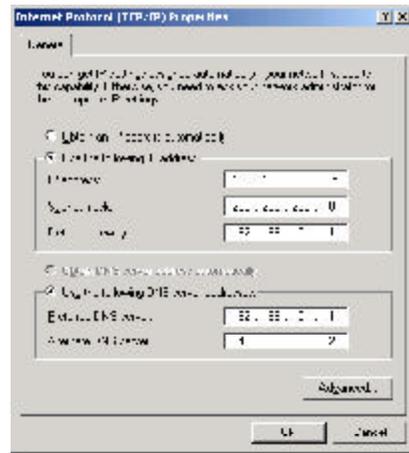## How can I assign a Static IP Address in Windows 2000? (continued)

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

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

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

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

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

How can I assign a Static IP Address in Windows 98/Me?

Step 1 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 one adapter, then there will be a TCP/IP "Binding" for each adapter. Highlight **TCP/IP > (your network adapter)** and then click **Properties**.

106

> **Why can´t I access the Web-based configuration? (continued)**

How can I assign a Static IP Address in Windows 98/Me? (continued)

Step 2 Click **Specify an IP Address**.

> Enter in an IP Address that is on the same subnet as the LAN IP Address on your router. <u>Example</u>: 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.

Step 3 Click on the **Gateway** tab.

> Enter the LAN IP Address of your router here (192.168.0.1).

> Click **Add** when finished.

Step 4 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**.

Step 5 Click **OK** twice.

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

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 log-in page for the web management. Follow instructions to log in and complete the configuration.
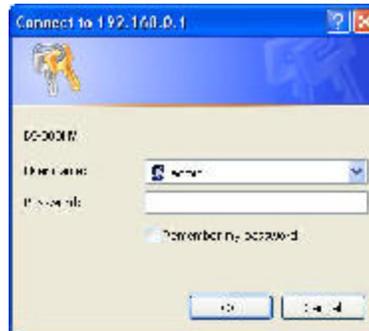
Frequently Asked Questions (continued)

How can I setup my DI-808HV to work with a cable modem connection?

Dynamic Cable connection
(i.e. Cox, Adelphia, Rogers, Roadrunner, Charter, and Comcast).

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

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

Step 2 Click the **Home** tab and click the **WAN** button. Dynamic IP address is the default value, however, if Dynamic IP address is not selected as the WAN type, select Dynamic IP address by clicking on the radio button. Click **Clone Mac address**. Click on **Apply** and then **Continue** to save the changes.
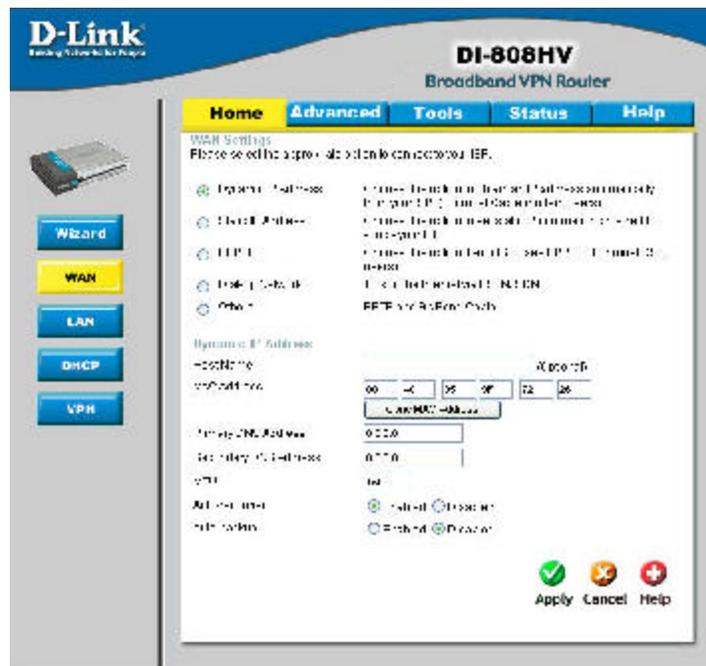
108

Frequently Asked Questions (continued)

How can I setup my DI-808HV to work with a cable modem connection? (continued)

Step 3 Power cycle the cable modem and router:

First turn the cable modem off. Then turn the router off Leave them off for 2 minutes.** Next turn the cable modem on. Wait until you get a solid cable light on the cable modem, and then 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 (empty).

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

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

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

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

109

Frequently Asked Questions (continued)

How can I setup my DI-808HV 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.

Frequently Asked Questions (continued)

> ### How can I setup my DI-808HV to work with Earthlink DSL or any PPPoE connection? (continued)

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

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

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

> ### Can I use my DI-808HV to share my Internet connection provided by AOL DSL Plus?

In most cases yes. AOL DSL Plus 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.
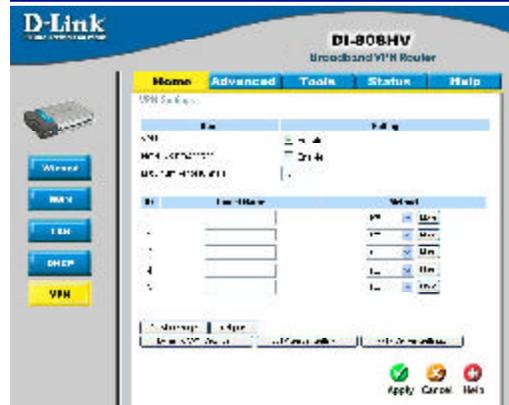
Frequently Asked Questions (continued)

I have two DI-808HV Routers, how can I set them up to work with each other?

Step 1 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.   By default the username is **admin** and there is no password.
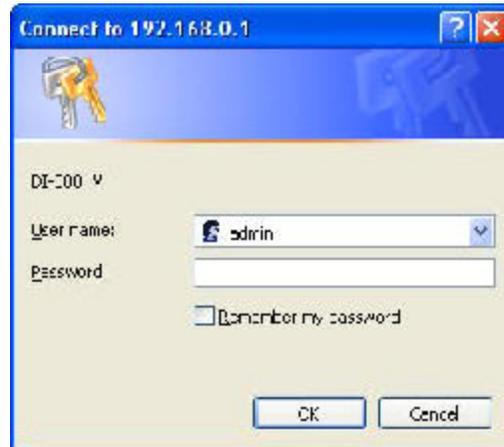
Step 2 Click the **VPN** button on the left column, select the checkbox to Enable the VPN, and then in the box next to Max. number of tunnels, enter the maximum numbers of VPN tunnels that you would like to have connected.
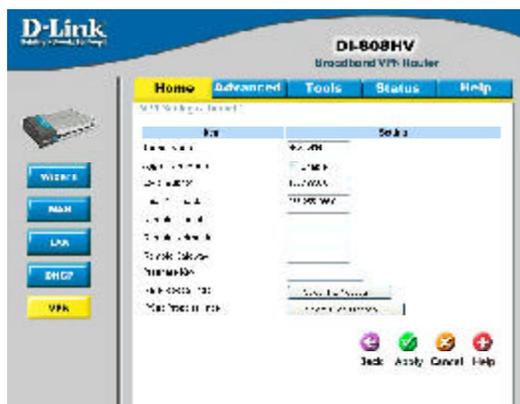
Step 3 In the space provided, enter the Tunnel Name for ID number 1, select IKE, and then click More.
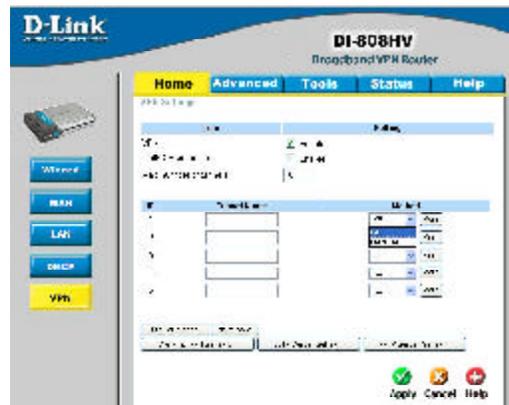
I have two DI-808HV Routers, how can I set them up to work with each other?(continued)

Step 4 In the **Local Subnet** and **Local Netmask** fields enter the network identifier for the local DI-808HV´s LAN and the corresponding subnet mask.

Step 5 In the **Remote Subnet** and **Remote Netmask** fields enter the network identifier for the remote DI-808HV´s LAN and the corresponding subnet mask.
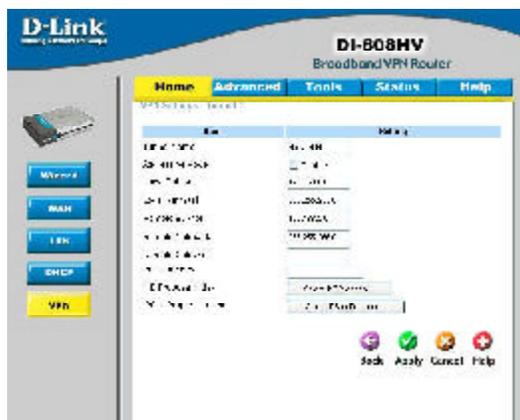
Step 6 In the **Remote Gateway** field enter the WAN IP address of the remote DI-808HV and in the **Preshare Key** field, enter a key which must be exactly the same as the Preshare Key that is configured on the remote DI-808HV.
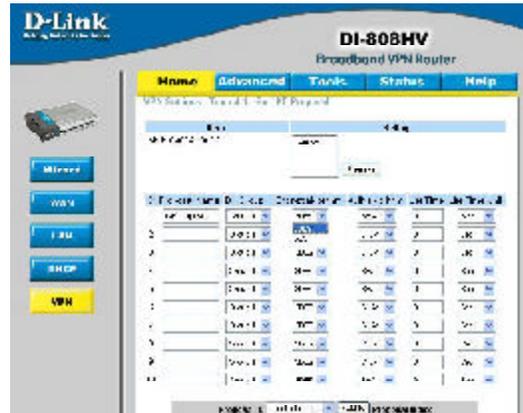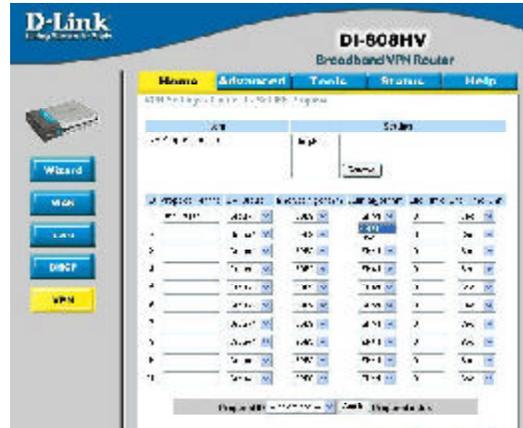
Step 7 Click Apply.

Frequently Asked Questions (continued)

I have two DI-808HV Routers, how can I set them up to work with each other?   (continued)
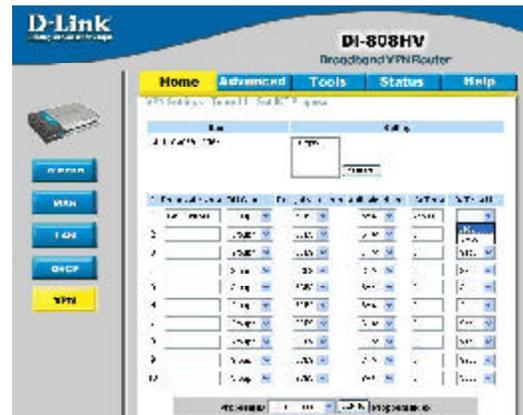
Step 8 The device will restart. Click on the Continue button.

Step 9 Click on Select IKE Proposal.

Step 10 Enter a name for proposal ID number 1 and select Group 1, 2, or 5 from the DH Group dropdown menu.

114

Frequently Asked Questions (continued)

I have two DI-808HV Routers, how can I set them up to work with each other?(continued)

Step 11 Select DES or 3DES as the Encryption Algorithm.

Step 12 Select SHA-1 or MD5 as the Authentication Algorithm.

Step 13 Enter a Lifetime value of 2800 and then either select Sec. or KByte as the unit for the lifetime value.

115

Frequently Asked Questions (continued)

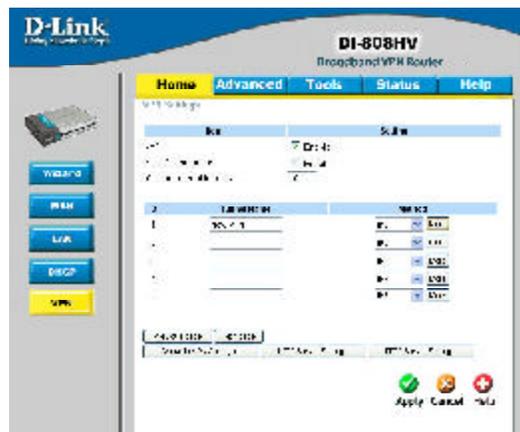**I have two DI-808HV Routers, how can I set them up to work with each other? (continued)**

Step 14 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IKE Proposal Index. Click Apply.

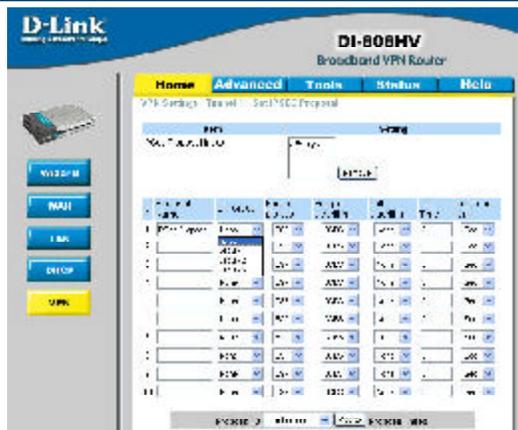**Step 15** The device will restart. Click on the Continue button. Then click Back.
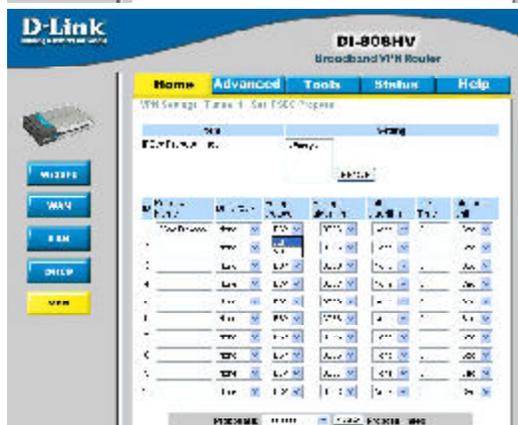

Step 16 Click on Select IPSec Proposal.

Frequently Asked Questions (continued)

I have two DI-808HV Routers, how can I set them up to work with each other?(continued)
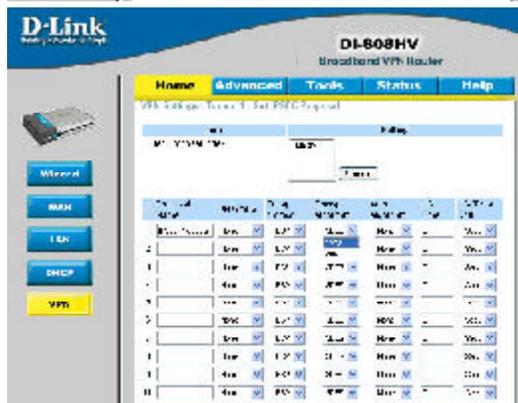
Step 17 Enter a name for proposal ID number 1 and select Group 1, 2, 5, or None from the DH Group dropdown menu.

Step 18 Select ESP or AH as the Encapsulation Protocol.

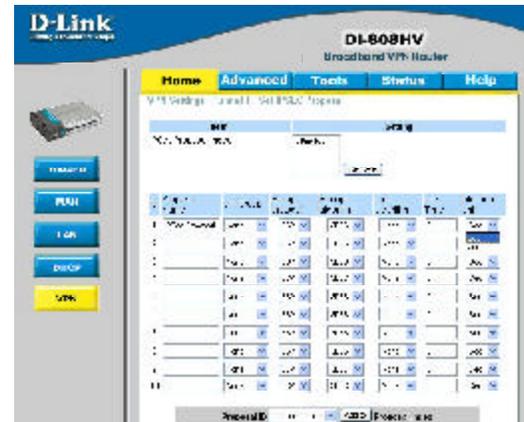**Step 19** Select DES or 3DES as the Encryption Algorithm.

Frequently Asked Questions (continued)

I have two DI-808HV Routers, how can I set them up to work with each other? (continued)

Step 20 Select SHA-1, MD5, or None as the Authentication Algorithm.

Step 21 Enter a Lifetime value and then either select Sec. or KB as the unit for the lifetime value.

Step 22 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IPSec Proposal Index. Click Apply and the device will restart.

Frequently Asked Questions (continued)

> **I have two DI-808HV Routers, how can I set them up to work with each other?(continued)**

Step 23 Follow these instructions to configure your other DI-808HV using the exact same settings for the IKE Proposal and the IPSec Proposal. Also make sure that Step 4 is configured to reflect the LAN settings for what is now the Local DI-808HV and that Steps 5 & 6 are configured to reflect the Subnet and WAN IP of what is now the remote DI-808HV

Step 24 To establish the connection, open a command prompt and ping an IP address of a computer on the remote LAN. Once you receive replies the tunnel has been established.

> **How can I set up my DI-808HV to work with a DI-804V or DI-804HV Router?**

You need to first configure your DI-808HV router.

Step 1 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. By default the username is "admin" and there is no password.

Step 2 Click the VPN button on the left column, select the checkbox to Enable the VPN, and then in the box next to Max. number of tunnels, enter the maximum numbers of VPN tunnels that you would like to have connected.

Frequently Asked Questions (continued)

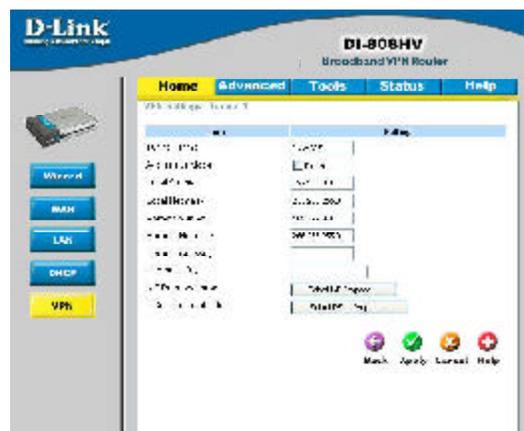**How can I set up my DI-808HV to work with a DI-804V or DI-804HV Router? (continued)**

Step 3 In the space provided, enter the Tunnel Name for ID number 1, select IKE, and then click More.

Step 4 In the **Local Subnet** and **Local Netmask** fields enter the network identifier for DI-808HV´s LAN and the corresponding subnet mask.

Step 5 In the **Remote Subnet** and **Remote Netmask** fields enter the network identifier for the DI-804V or DI-804HV's LAN and the corresponding subnet mask. Click Apply.
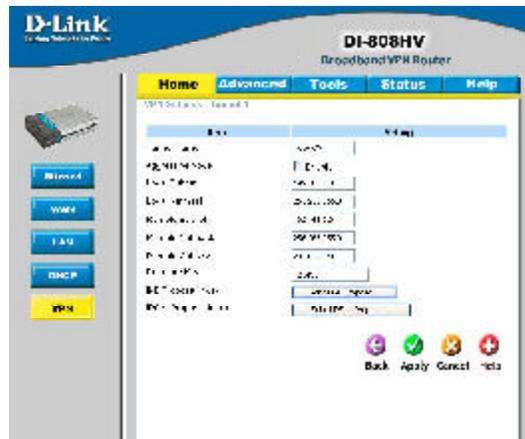
120

Frequently Asked Questions (continued)

How can I set up my DI-808HV to work with a DI-804V or DI-804HV Router? (continued)

Step 6 The device will restart. Click on the Continue button.

Step 7 In the **Remote Gateway** field enter the WAN IP address of the remote DI-804V or DI-804HV and in the **Preshare Key** field, enter a key which must be exactly the same as the Preshare Key that is configured on the DI-804V or DI-804HV.

Step 8 Click Apply and then click on Select IKE Proposal...

Step 9 Enter a name for proposal ID number 1 and select Group 2 from the DH Group drop down menu.

Step 10 Select 3DES as the Encryption Algorithm and SHA-1 as the Authentication Algorithm.

Step 11 Enter a Lifetime value of 28800 and then select Sec. as the unit for the lifetime value.

Frequently Asked Questions (continued)

How can I set up my DI-808HV to work with a DI-804V or DI-804HV Router? (continued)

Step 12 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IKE Proposal Index. Click Apply.

Step 13 The device will restart. Click on the Continue button.

Step 14 Click Back and click on Select IPSec Proposal.

Step 15 Enter a name for proposal ID number 1 and select None from the DH Group drop-down menu.
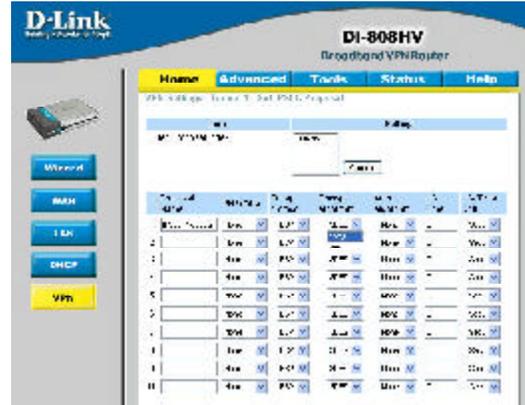
Step 16 Select ESP as the Encapsulation Protocol.

122

Frequently Asked Questions (continued)

Step 17 Select 3DES as the Encryption Algorithm and MD5 as the Authentication Algorithm. Click Apply.

Step 18 Enter a Lifetime value of 3600 and then select Sec. as the unit for the lifetime value.

Step 19 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IPSec Proposal Index. Click Apply. The device will restart. Click on the Continue button.
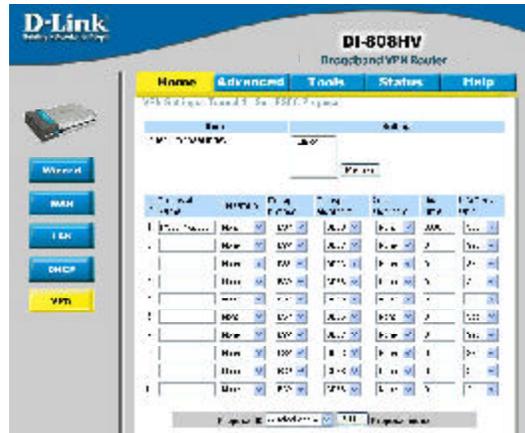
123

Frequently Asked Questions (continued)

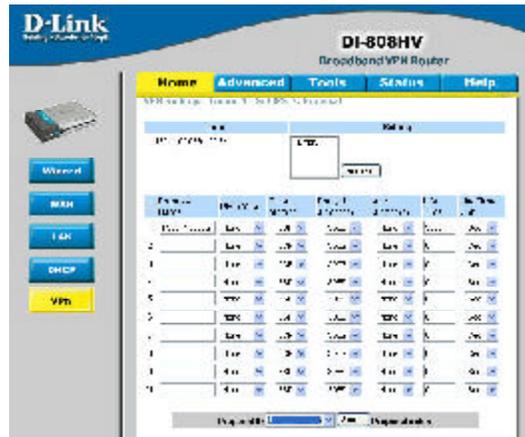**How can I set up my DI-808HV to work with a DI-804V or DI-804HV Router? (continued)**

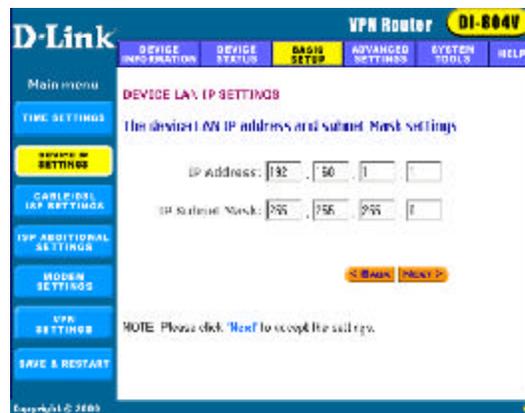Next you need to configure the DI-804V or DI-804HV Router.

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.

Step 2 Click on Basic Setup and then select Device IP Settings on the left.

Step 3 Change the LAN IP address so that it is on a different subnet than the LAN of the DI-808HV.

Step 4 Click Next until you reach the Save & Restart screen. Click Save & restart and then click Basic Setup once until the unit has rebooted.

Step 5 Click on VPN Settings.

Step 6 Name your VPN connection and click ADD.

Step 7 In Remote IP Network and Remote IP Netmask fields enter the network identifier and corresponding subnet mask of the DI-808HV´s LAN.

Step 8 In the Remote Gateway IP field enter the WAN IP address of the DI-808HV and make sure that the Network Interface is set to WAN Ethernet.

Step 9 Verify that Secure Association is set to IKE and that Perfect Forward Secure is Disabled.

Frequently Asked Questions (continued)

How can I set up my DI-808HV to work with a DI-804V or DI-804HV Router? (continued)

Step 10 Verify the Encryption Protocol is set to 3DES and enter in your Preshared Key.

Note: The Preshared Key needs to be identical to the one configured on the DI-808HV.

Step 11 Leave the Key Life and IKE Life Time values at their default levels and click SAVE.

Step 12 Click Next and then click on Save & Restart

After you have configured both routers, you need to establish a connection.

Step 1 Open a command prompt and from a computer on the internal LAN of the DI-808HV and ping the IP address of a computer that is on the internal LAN of the DI-804V or DI-804HV, or vice versa.

Step 2 Once you begin to receive replies, the VPN connection has been established.

Frequently Asked Questions (continued)

> **How can I set up my router to work with a DI-804V or DI-804HV router? (continued)**

Step 3 To view the Status of the VPN on the DI-804V or DI-804HV, click on Device Status.

Step 4 From the Device Status screen click on VPN Status.

Step 5 When the VPN has been established the Status will be Active.

> **How can I set up my DI-808HV to work with a DFL-300 Firewall?**

You need to first configure your DI-808HV router.

Step 1 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. By default the username is "admin" and there is no password.

Step 2 Click the VPN button on the left column, select the checkbox to Enable the VPN, and then in the box next to Max. number of tunnels, enter the maximum numbers of VPN tunnels that you would like to have connected.

Frequently Asked Questions (continued)

How can I set up my DI-808HV to work with a DFL-300 Firewall? (continued)

Step 3 In the space provided, enter the Tunnel Name for ID number 1, select IKE, and then click More.

Step 4 In the **Local Subnet** and **Local Netmask** fields enter the network identifier for DI-808HV´s LAN and the corresponding subnet mask.

Step 5 In the **Remote Subnet** and **Remote Netmask** fields enter the network identifier for the DFL-300´s Internal interface and the corresponding subnet mask.

Frequently Asked Questions (continued)

How can I set up my DI-808HV to work with a DFL-300 Firewall? (continued)

Step 6 In the Remote Gateway field enter the WAN IP address of the remote DFL-300 and in the Preshared Key field, enter a key which must be exactly the same as the Preshared Key that is configured on the DFL-300.

Step 7 Click Apply. The device will restart. Click on the Continue button and then click on Select IKE Proposal.

Step 8 Enter a name for proposal ID number 1 and select Group 2 from the DH Group dropdown menu.

Step 9 Select 3DES as the Encryption Algorithm and SHA-1 as the Authentication Algorithm.

Step 10 Enter a Lifetime value of 28800 and then select Sec. as the unit for the lifetime value.

Frequently Asked Questions (continued)

How can I set up my DI-808HV to work with a DFL-300 Firewall? (continued)

Step 11 Select 1 out of the Proposal ID dropdown menu and click Add To, which will add the proposal that was just configured to the IKE Proposal Index. Click Apply. The device will restart. Click on the Continue button and then click Back.

Step 12 Click on Select IPSec Proposal.

Step 13 Enter a name for proposal ID number 1 and select None from the DH Group dropdown menu.

Step 14 Select ESP as the Encapsulation Protocol.

Step 15 Select 3DES as the Encryption Algorithm and MD5 as the Authentication Algorithm.

Step 16 Enter a Lifetime value of 28800 and then select Sec. as the unit for the lifetime value.

Frequently Asked Questions (continued)

> ### How can I set up my DI-808HV to work with a DFL-300 Firewall? (continued)

Step 17 Select 1 out of the Proposal
ID dropdown menu and click Add To,
which will add the proposal that was just
configured to the IPSec Proposal Index.
Click Apply and then click Restart.
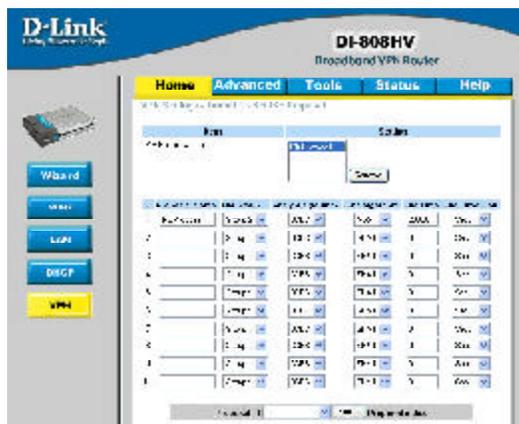
Step 18 The device will restart. Click
on the Continue button.

Next you need to configure the DFL-300 firewall.

Step 1 Access the configuration
screen of the DFL-300 by opening a
web browser such as Internet Explorer
and type the IP address of the DFL-
300 in the address bar (192.168.1.1).

Step 2 Enter the username (admin)
and the password (admin). Click OK.

Step 3 Click on Configuration and take
note of the IP address that your ISP has
assigned you.

Frequently Asked Questions (continued)

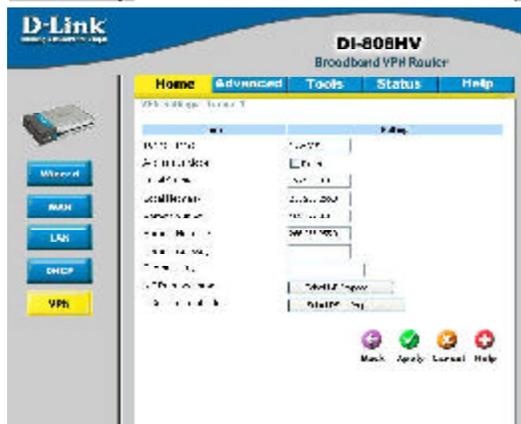**How can I set up my DI-808HV to work with a DFL-300 Firewall? (continued)**

Step 4 Click on Policy and verify that you have an Outgoing policy configured. If not, click on New Entry, accept the default values, and click OK.

Step 5 Click on VPN and then click New Entry.

Step 6 Give the VPN connection a name with no spaces.

Step 7 Enter the network identifier and subnet mask of the Internal interface.

Step 8 In the To Destination section, select either Remote Gateway—Fixed IP or Remote Gateway—Dynamic IP. Enter the WAN IP address of the DI-808HV if Remote Gateway—Fixed IP is selected.

Step 9 Enter the network identifier corresponding subnet mask of the DI-808HV´s LAN.

Step 10 Enter a Preshared Key. The Preshared Key needs to be identical to the one configured on the DI-808HV

Step 11 Select Data Encryption and Authentication as the Encapsulation and click OK.

131

How can I set up my DI-808HV to work with a DFL-300 Firewall? (continued)
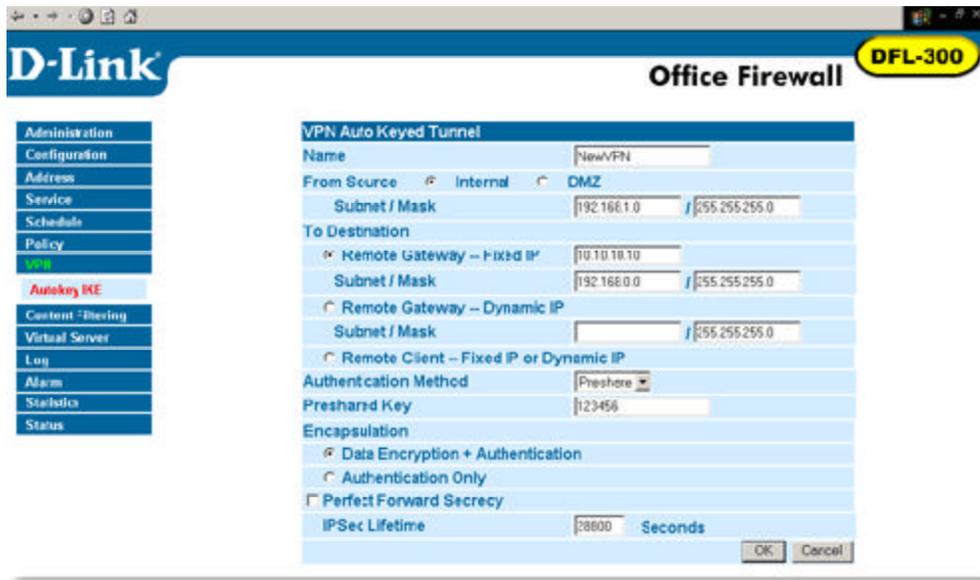
After you have configured both the router and firewall, you need to establish a connection.

Step 1 Open a command prompt and from a computer connected to the Internal interface of the DFL-300 and ping the IP address of a computer that is on the internal LAN of the DI-808HV, or vice versa.

Step 2 Once you begin to receive replies, the VPN connection has been established.

132

Frequently Asked Questions (continued)

How do I open ports on my DI-808HV?

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.

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.

133
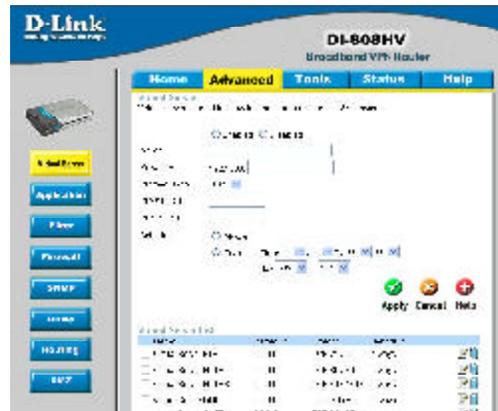
Frequently Asked Questions (continued)

What is DMZ?

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

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

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

How do I configure the DMZ Host?

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

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

To find out how to locate the IP Address of the computer in Windows XP/2000/ME/9x or Macintosh operating systems please refer to Step 4 of the first question in this section (Frequently Asked Questions).

Frequently Asked Questions (continued)

How do I configure the DMZ Host? (continued)

Step 2 Log into the web based configuration of the router by typing in the IP Address of the router (default:192.168.0.1) in your web browser. The username is **admin** (all lowercase) and the password is blank (empty).

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

135
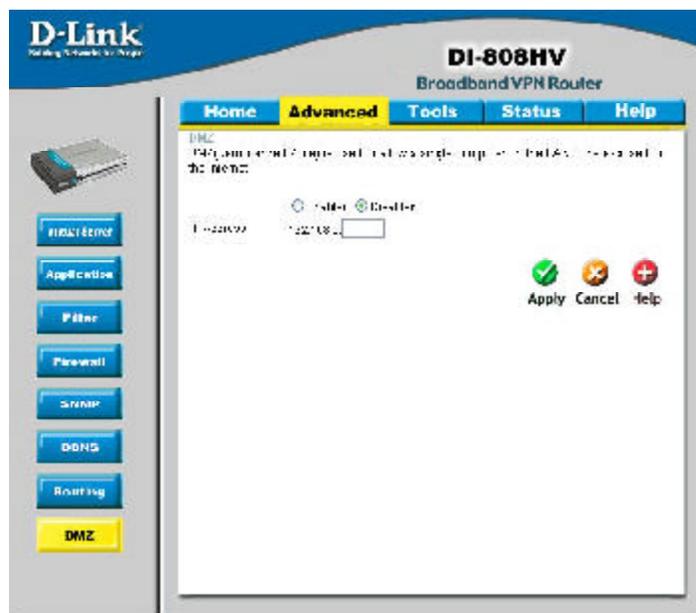
Frequently Asked Questions (continued)

> **How do I open a range of ports on my DI-808HV 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.
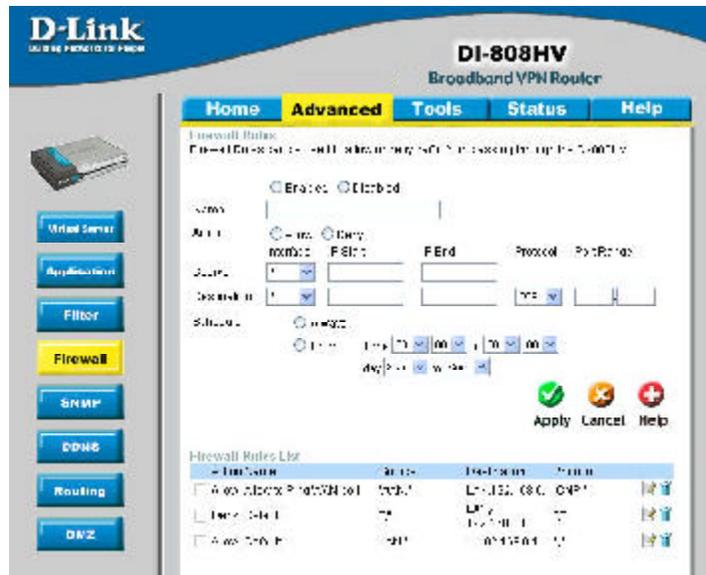
Step 5 Select **LAN** as the **Destination** and enter the IP Address of the computer on your local network that you want to allow the incoming service to. This will not work with a range of IP Addresses.

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.

Frequently Asked Questions (continued)

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 (port 1723) server at 192.168.0.7, then you need to specify the following virtual server mapping table:

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

How do I use *PC Anywhere* with my DI-808HV?

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

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

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

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

Step 4 The first entry will read as shown here:

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

137

Frequently Asked Questions (continued)

How do I use *PC Anywhere* with my DI-808HV? (continued)

Step 6 Create a second entry as shown here:

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

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

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

Step 10 Run *PCAnywhere* from the remote site and use the WAN IP Address of the router, not your computer´s IP Address.
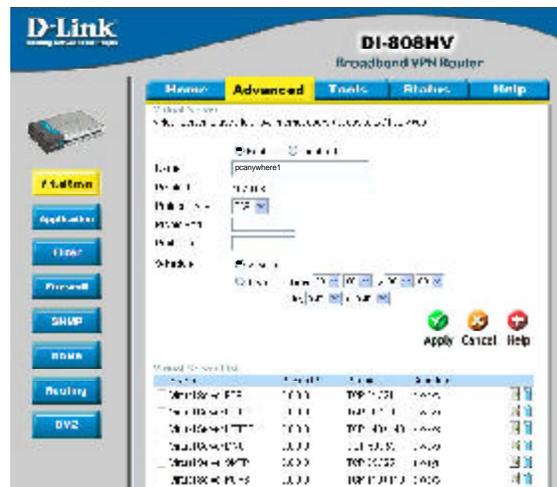
Frequently Asked Questions (continued)

> ### How can I use *eDonkey* behind my DI-808HV?

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**.

139

Frequently Asked Questions (continued)

How do I set up my DI-808HV 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**.

Frequently Asked Questions (continued)

> ### How can I use Gamespy behind my DI-808HV?

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

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

Step 3 You will create 2 entries.

Step 4 Click Enabled and enter Settings:

    NAME - Gamespy1

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

    PROTOCOL TYPE - Both

    PRIVATE PORT - 3783

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

Step 5 Enter 2nd entry:
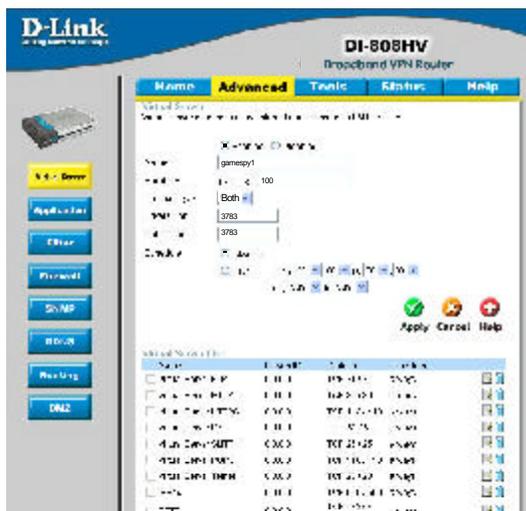   Click Enabled

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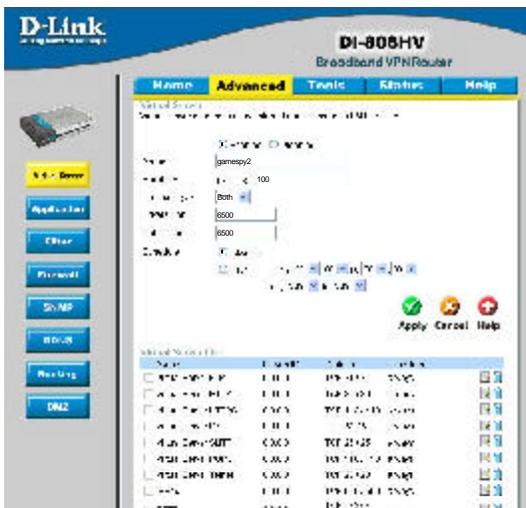
Click **Apply** and then **continue**.

Frequently Asked Questions (continued)

How do I configure my DI-808HV 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.

Frequently Asked Questions (continued)

How do I configure my DI-808HV to play Warcraft 3?

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

Warcraft 3 (Battlenet) uses port 6112.

For the DI808HV:

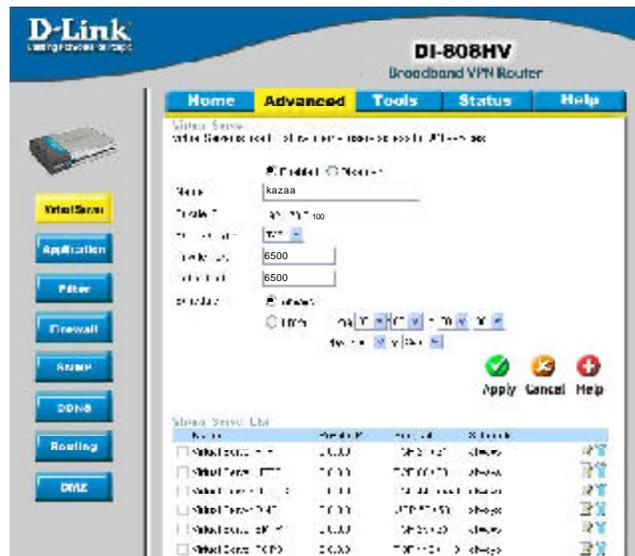Step 1 Open your web browser and enter the IP Address of your router (192.168.0.1). Enter username (admin) and your password (leave blank).

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.

143

Frequently Asked Questions (continued)

How do I use NetMeeting with my DI-808HV?

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

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

The solution is to put the router in DMZ.

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

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

How do I set up my DI-808HV 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), and 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**.

Frequently Asked Questions (continued)

How do I set up my DI-808HV to use iChat? -for Macintosh users-(continued)

Step 3 Create a new firewall rule:

    Click **Enabled**.
    Enter a name (ichat1).
    Click **Allow**.
    Next to Source, select **WAN** under interface.
    In the first box, enter an *.
    Leave the second box empty.
    Next to Destination, select **LAN** under interface.
    Enter the IP Address of the computer you are running iChat from.
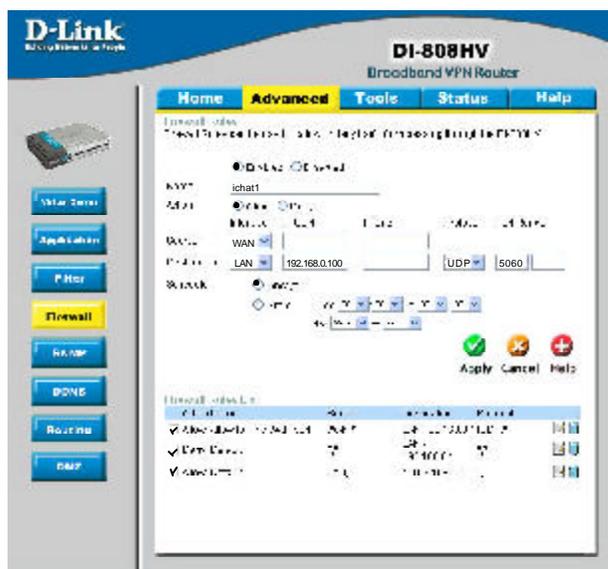
Leave the second box empty. Under Protocol, select **UDP**. In the port range boxes, enter **5060** in the first box and leave the second box empty. Click **Always** or set a schedule.

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

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

Frequently Asked Questions (continued)

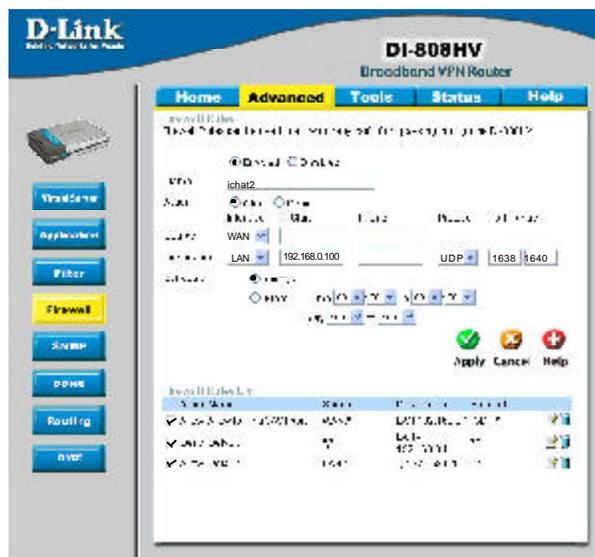### How do I set up my DI-808HV to use iChat? -for Macintosh users- (continued)

For File Sharing:
Step 1 Click on **Advanced** and then **Virtual Server**.

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

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

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

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

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

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

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

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

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

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

146

Frequently Asked Questions (continued)

> **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. "

147

Frequently Asked Questions (continued)

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. 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-808HV) support NAT. With proper configuration, multiple users can access the Internet using a single account via the NAT device.

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

Contacting Technical Support

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

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

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

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

When contacting technical support, you will need the information below. (Please look on the back side of the unit.)

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

Warranty and Registration

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 and shipped to **D-Link Systems, Inc., 53 Discovery Drive, Irvine, CA 92618**. 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.

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

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.

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