D-Link **DFL-100**

Firewall/VPN Router

Manual

Rev. 1.0

D-Link

Building Networks for People

Package Contents

Contents of Package:

- D-Link DFL-100 Firewall/VPN Router
- Manual
- Quick Installation Guide
- Power Adapter - 5V DC, 2.5A*

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

**Using a power supply with a different voltage rating will damage the product and void the warranty.*

System Requirements:

Internet Explorer 4.0 or higher or Netscape Navigator 4.0 or higher, with JavaScript enabled.

One computer with an installed 10Mbps, 100Mbps or 10/100 Mbps Ethernet adapter.

One RJ-45 DSL/Cable Modem for Internet connection.

Introduction

The D-Link DFL-100 Broadband VPN Router enables your network to connect to the Internet via a secure, private connection using a Cable/DSL modem, such as the D-Link DCM-200 Cable Modem. The Virtual Private Network that is created on the Internet between your home and your office (with a VPN server) is secure from interference when you use the DFL-100.

It is an ideal way to connect your computer to a Local Area Network (LAN). After completing the steps outlined in the Quick Install Guide (included in your package) you will have the ability to share information and resources, such as files and printers, and take full advantage of a "connected" environment for work or play!

Connect the WAN port on the DFL-100 to the Cable/DSL modem (e.g., the DCM-200) using an Ethernet cable. Your entire LAN can now access the Internet using just one Internet account. The DFL-100 has 3 LAN ports and one DMZ port. That means that 3 computers can share the benefits of the DFL-100- equipped network and 1 computer can be configured as a server for Internet applications that may conflict with the advanced protection from intrusion offered.

For the price of one Internet account, the DHCP-capable DFL-100 will automatically provide unique IP Addresses for all the computers on the network. *(DHCP stands for Dynamic Host Configuration Protocol. It is a protocol for assigning IP Addresses automatically. With a DHCP router like the DFL-100, there is no need to assign static IP Addresses, or purchase multiple addresses from the ISP - Internet Service Provider.)*

Everyone in your home can access the Internet on his or her own computer, at the same time, without any noticeable decrease in speed.

With the serial port, you can connect an analog modem (dial-up modem) as a back up in case of any difficulties that may arise with the Cable or DSL connection.

With Firewall Protection, Hacker attack logging, and Virtual Private Networking, the DFL-100 provides a level of security suitable for many businesses.

This manual provides a quick introduction to network technology. Please take a moment to read through this manual and get acquainted with your DFL-100.

Front View

LED Indicators

WAN Link/Act.	(Green)	Green LED will LIGHT when a good link is established. Green LED will BLINK when packet is transmitting or receiving (Act.).
WAN 10/100	(Green)	Green LED will LIGHT when a 100 Mbps Link is established. Green LED will NOT LIGHT when a 10 Mbps Link is established.
DMZ Link/Act.	(Green)	Green LED will LIGHT when a good link is established. Green LED will BLINK when packet is transmitting or receiving (Act.).
DMZ 10/100	(Green)	Green LED will LIGHT when a 100 Mbps Link is established. Green LED will NOT LIGHT when a 10 Mbps Link is established.
LAN (1-3) Link/Act.	(Green)	Green LED will LIGHT when link is established (Link). Green LED will BLINK when packet is transmitting or receiving (Act.).
LAN (1-3) 10/100	(Green)	Green LED will LIGHT when a 100 Mbps Link is established. Green LED will NOT LIGHT when a 10 Mbps Link is established.

Power	(Green)	Green LED will LIGHT when powered ON.

Rearview

Power (5V DC)	Connects the DC power adapter to the Power port
WAN	Connects DSL/Cable modem to the WAN Ethernet port
Ports 1-3	Connect networked devices such as computers and ftp servers to the three LAN ports. All LAN ports support auto crossover.
DMZ	Connects a networked device to the DMZ zone of the Firewall/VPN Router.
Reset	To reload the factory default settings, press the reset button. Pressing the Reset button will clear the current configuration as reset the DFL-100 to the factory default settings.

Product Features

VPN

Provides Virtual Private Networking when communicating with a VPN server-equipped office, or with another DFL-100-equipped network. Supports IPSEC, PPTP, L2TP, and VPN pass through.

DSL/Cable Modem support

The DFL-100 can connect any DSL/Cable Modem to the network.

DHCP

The DFL-100 is a DHCP-capable router. It automatically assigns unique IP Addresses to each network users that is connected to the DFL-100, for the price of one Internet account.

Firewall Protection

Supports general hacker attack pattern monitoring and logging

PPPoE Client

Supports PPPoE client function to connect to the remote PPPoE server.

Virtual Server

Allows the internal server to be accessible from the Internet

Upgradeable New Features

Allows new features to be added in the future

High Performance 64 bit RISC CPU Engine

With the most advanced 64 bit RISC CPU Engine, DFL-100 guarantees full compatibility with future DSL/Cable technologies

IPSec Security

(DES, 3DES, MD5, SHA-1)

Idle Timer

Set a specified idle-time before automatically disconnecting

Dial-on Demand

Eliminates the need for Dial-up. Automatically logs in to your ISP

Web-Based Configuration

No software installation required. Can be configured through a web browser making it OS independent.

IP Address Settings and Computer Settings

In order to install the DFL-100 you will need to check your computer's settings and the values from your ISP.

The information offered by your ISP:

- Dynamic IP settings
- Your fixed IP address for the gateway
- Your subnet mask for the gateway
- Your default gateway IP address
- Your DNS IP address

If you would like to use PPPoE, you will need the following values from your ISP in order to install your router:

- User Name
- Password

The static IP settings for the PC:

- Your PC's fixed IP address
- Your PC's subnet mask
- Your PC's default gateway
- Your PC's primary DNS IP address

Note: *The router's default IP address setting is 192.168.0.1.*

Dynamic IP Settings:

It is recommended that you leave your IP settings as automatically assigned (by a DHCP server). By default, the gateway is a DHCP server, and it will give your computer the necessary IP settings.

Introduction and Overview

The DFL-100 Firewall/VPN Router creates two separate networks on the LAN side of your network – by default, a 192.168.0.0 subnet and a 192.168.1.0 subnet (both with a subnet mask of 255.255.255.0). The DFL-100 routes packets between these two subnets and the Internet (or the network connected to the DFL-100's **WAN** port). The network address information of the WAN network is usually provided by an Internet Service Provider (ISP) or a network administrator.

The 192.168.0.0 network. The three Ethernet ports labeled – **Local Area Network** on the front panel, and **1, 2,** and **3** on the rear panel – are, by default, assigned the IP address range between 192.168.0.1 to 192.168.0.254. So computers and other devices connected to these three ports either allow the DFL-100's DHCP server to assign them IP addresses from this range, or you can manually assign devices connected to these ports an IP address from this range. Remember that the IP address, 192.168.0.0, is reserved. The DFL-100 is assigned 192.168.0.1 – on the LAN side – and is configured from a computer (again, on the LAN side of your network) using a web browser, at this IP address.

The 192.168.1.0 network. The port labeled – **DMZ** on both the front and rear panel – is, by default, assigned the IP address range between 192.168.1.1 to 192.168.1.254 – with a subnet mask of 255.255.255.0. So computers and other devices connected to this port must be assigned IP addresses from this range. The DHCP server on the DFL-100 only services the LAN ports, so you must manually assign a computer connected to the DMZ port an IP address from this range.

You can use this default IP addressing scheme, or configure your own. It is important to note that the three LAN ports and the DMZ port must be on different subnets (different ranges of IP addresses) and that the computers that are connected to these ports must have IP addresses in the appropriate range.

The **DMZ** port is used to allow computers and devices connected to this port more direct access to the Internet. This is useful for certain applications that may conflict with the firewall and Network Address Translation (NAT)

features of the DFL-100. Computers and devices connected to the **DMZ** port will not have the level of protection that the **Local Area Network** ports can provide, however. It is recommended that computers and devices connected to the DFL-100's DMZ port have some type of firewall software installed and running to provide these devices with at least some level of protection from unwanted intrusions from the Internet.

The **Wide Area Network (WAN)** side of the DFL-100 is anything connected to the **WAN** port. This is normally an Ethernet connection to a Cable or DSL modem that, in turn, provides a connection to the Internet. There are three different methods for your ISP to provide the necessary network address information to your DFL-100.

It can be useful when configuring your DFL-100 Firewall/VPN Router to think of the LAN side (all computers or devices connected to the three LAN ports or the DMZ port) and the WAN side (all computers or devices connected to the WAN port). The WAN side of the router is connected to some device that ultimately allows a connection to the Internet, while the LAN side is connected to your computers or other network devices (such as a switch or hub) that ultimately allows users access to the both the Internet and any other devices on your LAN (such as a printer or scanner).

The network information (including the IP address) required by the WAN side of the DFL-100 is either obtained automatically from your ISP (or other network device on the WAN side) or is entered manually. The DFL-100 allows three methods for this information to be obtained, as follows:

Dynamic – your ISP uses the Dynamic Host Configuration Protocol (DHCP) to provide the network information. Some ISP's may require you to enter an assigned **Host Name**, as well.

Static IP Address – your ISP assigns you an IP address that never changes. This is more common in businesses that lease dedicated connections. If your ISP uses this type of connection, you must manually enter the assigned IP address, subnet mask, default gateway address, and primary and secondary DNS addresses. This information will be provided by your ISP.

Point-to-Point Protocol over Ethernet (PPPoE) – this protocol requires the use of a **Username** and **Password** to gain access to the network. In addition, you can specify a **Connect on Demand** connection that will connect to the Internet only when a computer or device on your LAN makes a request.

If you do not know the appropriate method of obtaining the WAN side network address information, contact your ISP or network administrator.

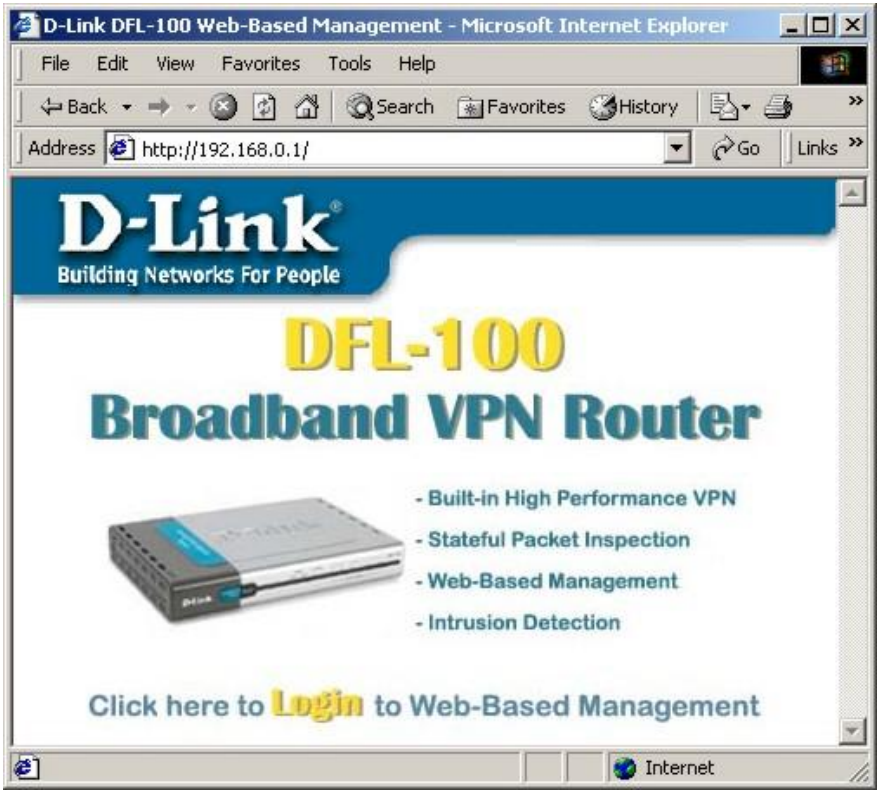
The **Device IP Settings** dialog box allows you to specify the IP address that computers on your LAN will use to access the DFL-100's web-based configuration utility. The default is 192.168.0.1 with a subnet mask of 255.255.255.0. If it becomes necessary to change this IP address, be sure to use an address that is in the same range (on the same subnet) as the three LAN ports, or you will not be able to access the DFL-100 from your LAN.

The many other features of the DFL-100 are describe in subsequent sections.

Using the Configuration Utility

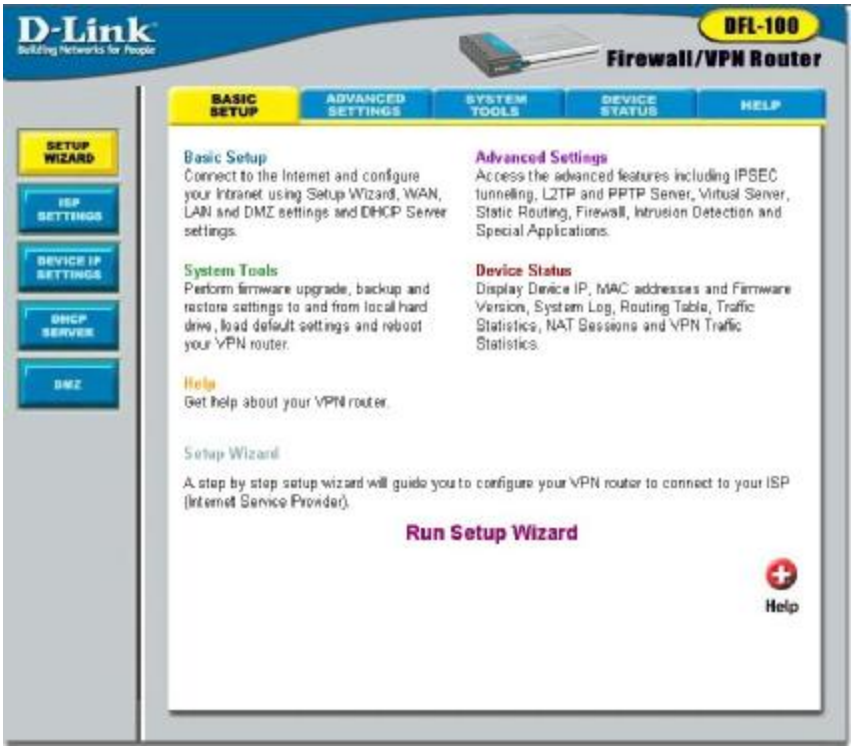
Launch your web browser and type the device IP address (http:// 192.168.0.1) in the browser's address box. This IP address is the default value of your gateway. Press Enter.

Note: Please make sure that the computer you will use to connect to and configure the DFL-100 is assigned an IP address that is in the same range as the DFL-100. The IP address of the DFL-100 is 192.168.0.1. All computers on your network must be within that range, for instance, the computer IP address could be 192.168.0.x, with a subnet mask of 255.255.255.0. All computers on the LAN side network must have the same subnet mask.



The logon menu appears. Click on the screen to open the **Enter Network Password** dialog box.

The default user name for the DFL-100 is **admin**. There is no default password. Click **OK** to open the **Basic Setup** menu.



The Setup Wizard will guide you the most basic setup tasks, such as setting an administrative password, selecting the type of WAN connection you have, entering your computer's host name (if required by your ISP), saving the configuration and restarting the router.

All other setup tasks can be accomplished using the configuration utility from your web browser.

To use the Setup Wizard, click on the **Run Setup Wizard** link. This will start the Setup Wizard.

Setup Wizard

The Setup Wizard will guide you through the most basic setup tasks for the DFL-100. All other configuration tasks can be accomplished through the web-based manager.

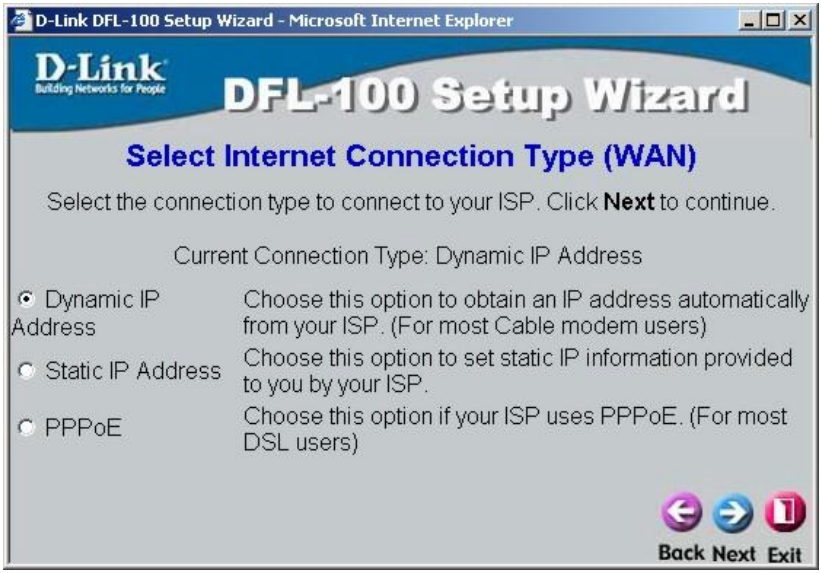
The **Basic Setup** menu contains a **Run Setup Wizard** link. Click on this link to run the Setup Wizard.

Click **Next** to continue.

Enter a password in the **Password** field, and again in the **Verify Password** field. This will become the logon password for the DFL-100. This password is case-sensitive, so remember to use capital letters when logging on to the DFL-100's web-based manager – if you enter a password with capital letters here. The user name, **admin**, will not be changed here. If you want to, you can change the user name later.

Note: *If you choose to input a password, please remember it. If you lose your password, you will have to reset the unit. Resetting the DFL-100 will return all configuration parameters to their factory default values, so all of your settings will be lost and will need to entered again. The default Username is* **admin** *with no password.*

Click **Next** to continue.

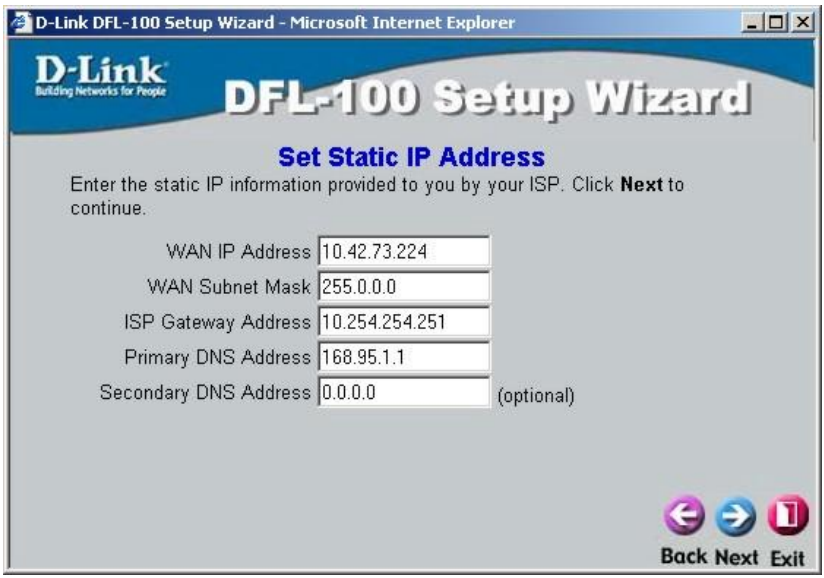


This menu allows you to select the type of connection your ISP provides. Most ISPs use the PPPoE (Point-to-Point Protocol over Ethernet) for DSL connections, while most Cable ISPs use DHCP (Dynamic Host Configuration Protocol). DHCP assigns an IP address for your Internet connection each time you log on (and is therefore, a dynamic IP address). The Setup Wizard will open a page with the appropriate fields for the entry of your ISP contact information, depending upon which of the three options you choose.

Click **Next** to continue.

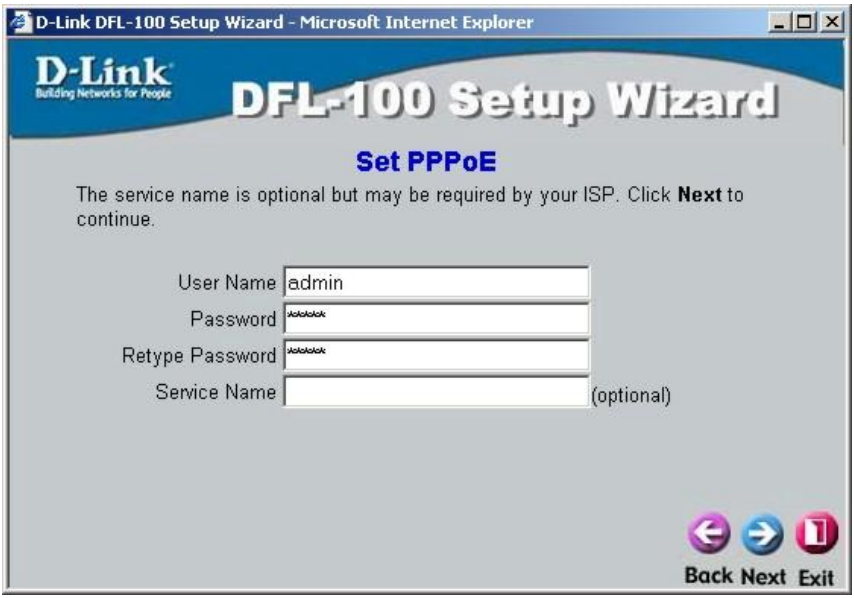
Some ISPs require you to use an assigned host name for your Internet connection. If your ISP requires this, you can enter the assigned host name in the **Host Name** field.

If you selected **Static IP Address** on the **Select Internet Connection Type (WAN)** wizard screen above, the following screen will open:



This screen will allow you to enter the static IP address information, if your ISP has assigned a static IP address to your Internet account. Your ISP must provide this information.

If you selected **PPPoE** (Point-to-Point Protocol over Ethernet) on the **Select Internet Connection Type (WAN)** screen above, the following window will open:



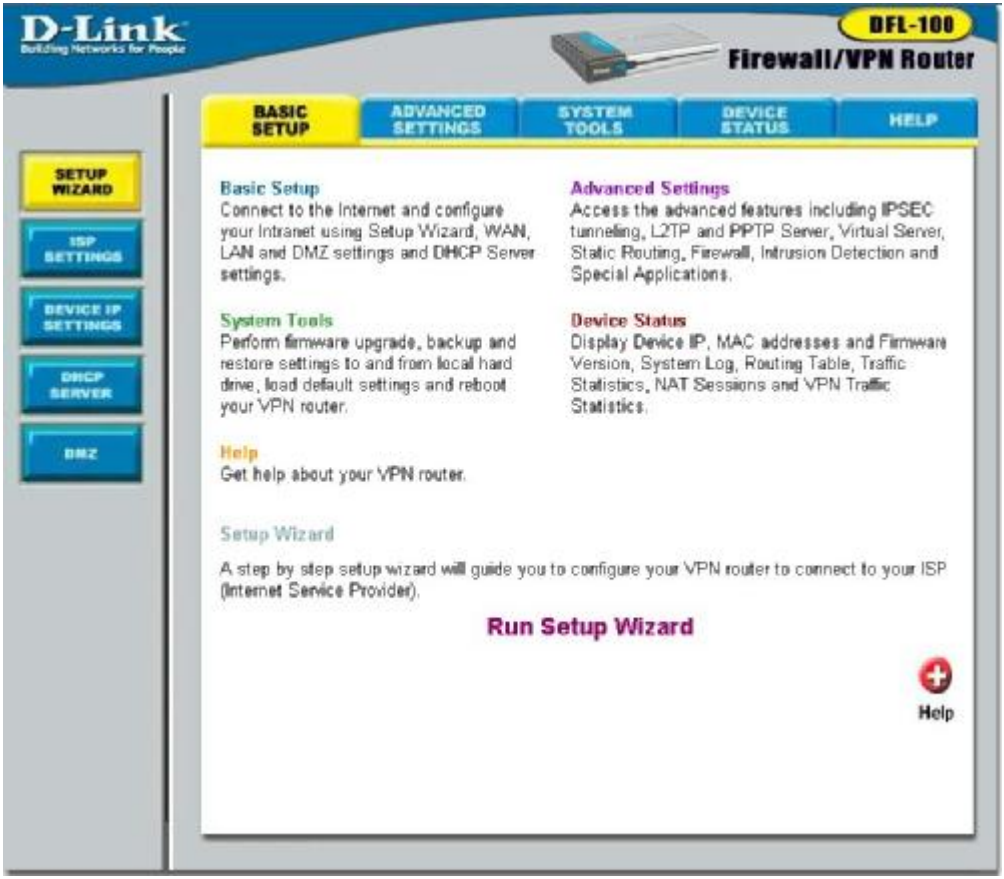
This screen will allow you to enter the PPPoE information, if your ISP uses the PPPoE protocol for your Internet account. Your ISP must provide this information.

Click **Next** to continue.

You have completed the basic setup Wizard. The configuration now needs to be entered into the DFL-100's non-volatile RAM. Clicking **Restart** will save the configuration and restart the router.

Basic Setup

The **Basic Setup** menu contains links to all of the setup menus for the DFL-100.



Click on the **ISP Settings** button:

ISP Settings

The **ISP Settings** menu allows you to view the current configuration for your DFL-100, and to choose the protocol by which your DFL-100 will receive its WAN network settings.

The settings listed under **Current WAN Information** are the network settings currently in use by the DFL-100. These settings are defined below.

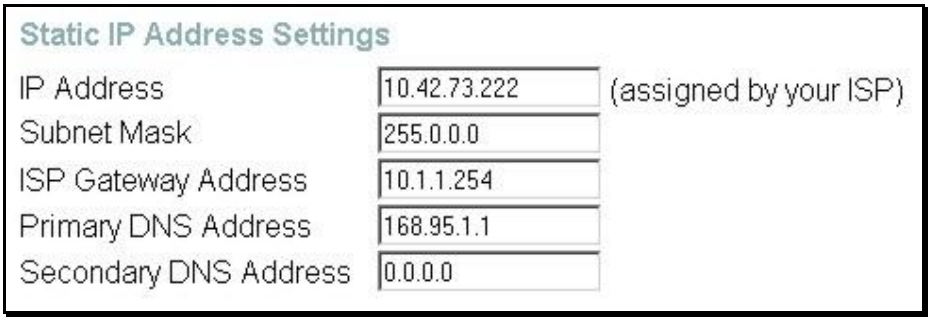
IP Address	This is the current IP address used to identify your 'location' on the Internet. It is assigned by your ISP, or entered statically by you. IP addresses work in combination with a subnet mask, described below.
Subnet Mask	A subnet mask is a number, in the same form as an IP address, that is used to mathematically separate a range of IP addresses into a Network portion and a Node portion. The Node portion identifies a specific device on the Network – in this case, the DFL-100.
Default Gateway	This is the IP address of a device at your ISP's

	office where packets destined for the Internet – from your home network – are sent, before being forwarded to their final destination. For the DFL-100, the Default Gateway address is provided by your ISP. For computers on your home network, their Default Gateway is the IP address of your DFL-100.
Primary DNS Server	This is the IP address of a computer on the Internet that provides the service of changing text URLs into IP address for sites on the Internet. The IP address of this device is provided by your ISP.
Secondary DNS Server	This is a the IP address of a second DNS server, to be used in case there is a problem with the Primary DNS Server. A secondary DNS server IP address is optional.

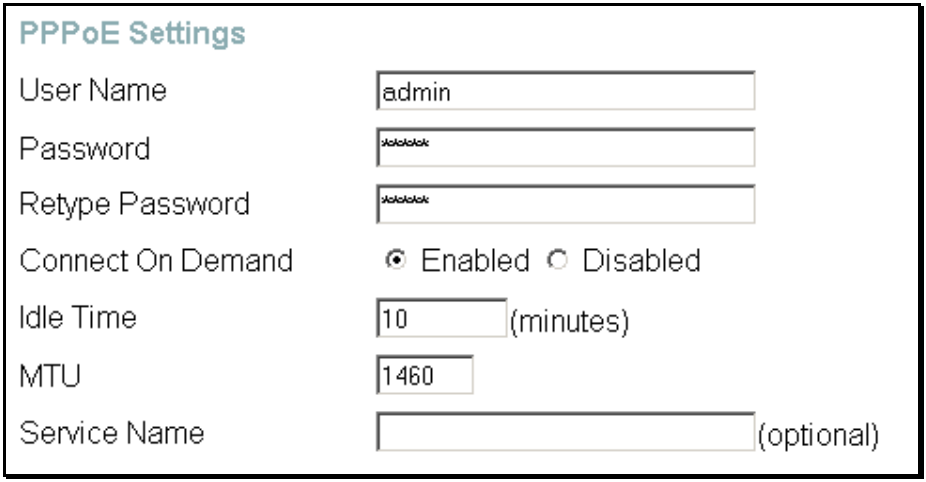
The ISP Settings page allows you to modify the way that the DFL-100 obtains its network settings from your Internet Service Provider (ISP). The entry fields on the page will change depending upon which of the following options you choose: Dynamic IP Address, Static IP Address, and PPPoE.

Dynamic IP Address – If your ISP uses the Dynamic Host Configuration Protocol (DHCP) to assign an IP address, subnet mask, default gateway and Domain Name Server (**DNS**) addresses, choose this option. Some ISPs require the use of an assigned Host Name for the device that will make the WAN connection, you can enter this name into the Host Name field. This is the page shown above.

Static IP Address - If your ISP has assigned you an IP address that will never change, choose this option. When this option is chosen, the following fields appear to allow you to enter the network address information:



PPPoE – If your ISP uses Point-to-Point Protocol over Ethernet (**PPPoE**), choose this option. When this option is chosen, the following fields appear to allow you to enter the network address information:



Connect on Demand – allows the PPPoE WAN connection to be active only when a computer on your LAN makes a connection request. This is similar to the way a dial-up modem initiates a connection.

Device IP Settings

The **Device IP Settings** allows you to view the current IP address and subnet mask assigned to the DFL-100. It also allows you to change these settings.

If it is necessary to change the **IP Address** or **Subnet Mask** assigned to the DFL-100, enter the new values in the appropriate fields, and press **Apply** to make the changes current.

Note: *if you assign an IP address and subnet mask to the DFL-100 that is different from the IP address range assigned to the computers connected to the LAN ports, you will no longer be able to connect to the DFL-100 from any of these computers. In order to re-establish the connection between a computer on the LAN side and the DFL-100, you will need to assign at least one computer on the LAN side an IP address from the same range as the IP address you assign to the DFL-100. As an alternative, you can configure the*

DFL-100's DHCP server to give IP addresses from the new IP address range that you will give the DFL-100 here.

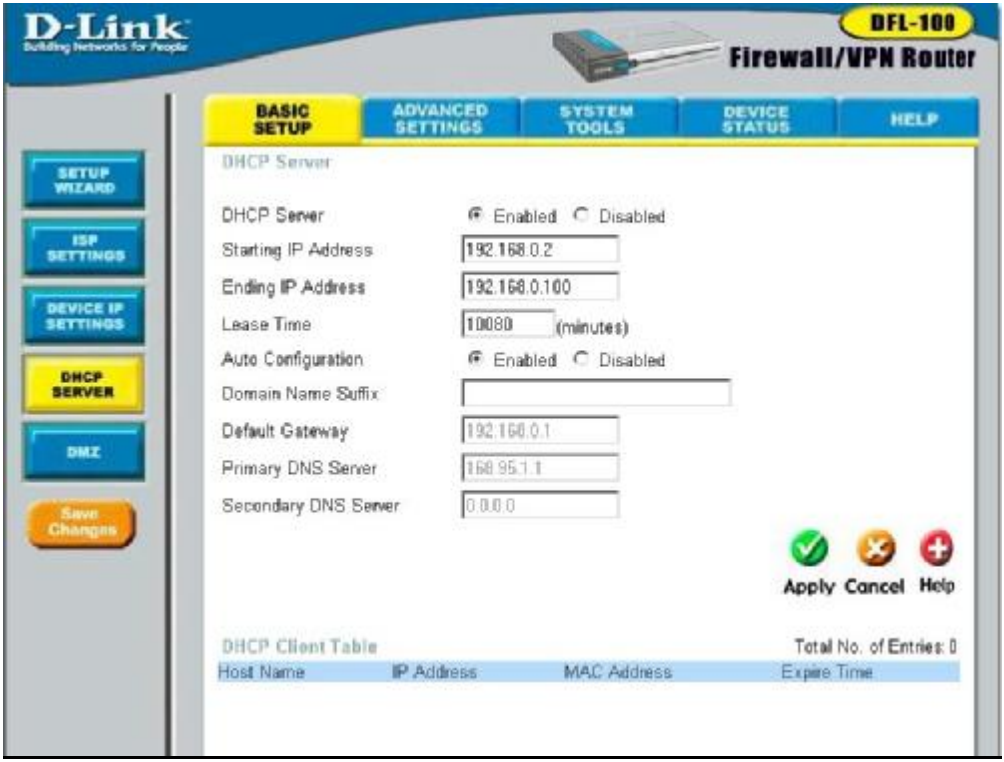
As an example, if your LAN network is to be a 10.x.x.x network with a subnet mask of 255.0.0.0, you might assign the DFL-100 an IP address of 10.0.0.1 and configure the DFL-100's DHCP server to assign addresses in the range between 10.0.0.2 to 10.0.0.100. Saving all of this information to the DFL-100's non-volatile RAM and restarting the router will make this IP addressing scheme current. When you restart the computers connected to the LAN side of the DFL-100, they will automatically be assigned IP addresses from the proper range.

As an alternative, you could manually update the IP address and subnet mask for each computer on the LAN side of the DFL-100.

It is recommended that if you need to change the IP addressing scheme for the DFL-100, that you configure the DFL-100's DHCP server with the appropriate IP address range and subnet mask first, and then assign an IP address from the same range to the DFL-100. That way, a computer on the LAN side of your network can always get the proper network addressing information by DHCP from the DFL-100 simply by being restarted.

DHCP Server

DHCP (Dynamic Host Configuration Protocol) is a method of automatically assigning IP addresses, subnet masks, default gateway and DNS server IP addresses to computers on a LAN or WAN. The DFL-100 can be a DHCP server for your network, assigning IP addresses, etc. to computers on your network from a range of addresses you specify, below:



DHCP Server	This allows you to **Enable** or **Disable** the DHCP Server feature on the DFL-100. The default is **Enabled**.
Starting IP Address	This is the first IP address in a range that the DFL-100 will assign to a computer on your network. This IP address can not be the same as the IP address assigned to the DFL-100, nor can the IP address assigned to the DFL-100 be contained in the range of IP addresses available

	for the DFL-100 to assign. In this case, the IP address of the DFL-100 is 192.168.0.1, so the first IP address in the range is 192.168.0.2. IP addresses can range from 0.0.0.0 to 255.255.255.255.
Ending IP Address	This is the last IP address in a range that the DFL-100 will assign to a computer on your network. In this case, the range of IP addresses between 192.168.0.2 to 192.168.0.100 gives 99 different IP addresses that the DFL-100 can assign to the computers on your network.
Lease Time	This is the length of time any computer on you network that is assigned network settings by the DFL-100 – through the DHCP protocol – can keep its network settings. If the lease expires while a computer is logged on to your network, that computer will request a new set of network settings. The default is 10080 minutes.
Auto Configuration	This field allows you to specify whether or not the DFL-100 will assign the following network settings to the computers on your network. If you choose to **Enable** Auto Configuration, the following network settings will be obtained from your ISP by the DFL-100, and then assigned to computers on your network. If you choose to **Disable** Auto Configuration, the network settings you enter in the fields below will be assigned to computers on your network.
Domain Name Suffix	The DFL-100 can provide a domain name suffix to computers on your network. This domain name suffix can be provided automatically by your ISP, or you can enter it statically here. This suffix will then be automatically added to URL requests for access to your ISP's servers.
Default Gateway	This is the IP address of a device at your ISP's office where packets destined for the Internet – from your home network – are sent, before being forwarded to their final destination. For the

	DFL-100, the Default Gateway address is provided by your ISP. For computers on your home network, their Default Gateway is the IP address of your DFL-100.
Primary DNS Server	This is the IP address of a computer on the Internet that provides the service of changing text URLs into IP address for sites on the Internet. The IP address of this device is provided by your ISP.
Secondary DNS Server	This is a the IP address of a second DNS server, to be used in case of a problem with the Primary DNS Server, above. A secondary DNS server IP address is optional.

NAT

Network Address Translation

Note: ***NAT is automatically applied between the WAN and the LAN sides of the DFL-100. It does not require any user configuration.***

Network Address Translation (NAT) is a routing protocol that allows your network to become a *private* network that is isolated from, yet connected to the Internet. It does this by changing the IP address of packets from a *global* IP address usable on the Internet to a *local* IP address usable on your private network (but not on the Internet) and vice-versa. The DFL-100 VPN Router allows up to 128 host IP addresses.

NAT has two major benefits. First, NAT allows many users to access the Internet using a single global IP address. This can greatly reduce the costs associated with Internet access and helps alleviate the current shortage of Internet IP addresses. Secondly, the NAT process creates an added degree of security by hiding your private network behind one IP address. The NAT function will normally only allow incoming packets that are generated in response to a request from a host within the LAN.

NAT is automatically applied between the IP addresses assigned to the DFL-100's WAN port (the IP address or addresses assigned to you by your ISP) and the IP addresses assigned to the DFL-100's LAN ports (the 192.168.0.x subnet). NAT is not used between the WAN port and the DMZ port.

Complications with Using NAT and Some Applications

NAT is a simple IP address mapping function (that is, it only looks at IP address headers) and is therefore unaware of the application data embedded in packets that pass through it. Computers on your LAN running applications that may conflict with NAT can be connected to the DFL-100's DMZ port. NAT is not applied to the DMZ port.

DMZ

NAT may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a NAT bypass can be set up using the DMZ port and a corresponding DMZ IP address. The DMZ IP address is “visible” to the Internet (or WAN) and does not benefit from the full protection of the NAT function. Therefore it is advisable that other security precautions be enabled to protect the DMZ device and other computers and devices on the LAN that may be exposed. It may be wise to run some sort of firewall software on these computers and devices.

For example, if you want to use video conferencing and still use NAT, you can use the DMZ port and DMZ IP address. In this case, you must have a PC or server through which video conferencing will take place, that is assigned the DMZ IP address.

By default, the DMZ IP address is 192.168.1.1 with a subnet mask of 255.255.255.0. Note that the DMZ IP address is on a different subnet (the 192.168.1.x subnet) than the LAN ports (by default, the LAN ports are assigned to the 192.168.0.x subnet).

DMZ Status

The **DMZ Status** screen allows you to **Enable** and **Disable** the DMZ port on the DFL-100 and to specify the IP address and Subnet Mask that the DMZ port will use.

IP Address	This is the WAN IP address assigned to the DFL-100 by your ISP or network administrator. If a range of IP addresses have been assigned, then you will have to pick one IP address to connect to the DMZ device.
Subnet Mask	This is the subnet mask corresponding to the DMZ IP address specified above. It must be the same subnet mask as assigned to the LAN ports.

DMZ Host Settings

The **DMZ** port maps one global IP address – an IP address that is valid on the Internet, usually assigned by your ISP – to one local IP address from the IP address range assigned to the DFL-100's **DMZ** port.

DMZ Hosts, sometimes referred to as **Virtual Servers**, are computers on you LAN that are connected to the **DMZ** port and are configured to act as servers to connections to the WAN or Internet. The IP address must be from the same range as the IP address of the DMZ port. The default DMZ IP address is 192.168.1.1, so DMZ Servers must be from the IP address range from 192.168.1.2 to 192.168.1.254, with a subnet mask of 255.255.255.0.

DMZ Host Status	A DMZ Host that has been previously configured on the DFL-100 can be **Enabled** or **Disabled** by clicking the appropriate click-box and then clicking the **Apply** button.
Global IP Address	The WAN IP address assigned to the DFL-100 by your ISP or network administrator. If a range of IP addresses have been assigned, then you will have to pick one IP address to connect to the DMZ device.
DMZ Host IP Address	This is the IP address of the DMZ device (the device connected to the DMZ port). It must be on the same subnet as that assigned to the DMZ port – 192.168.1.x with a subnet mask of 255.255.255.0, by default.

Advanced Settings

IPSec

IPSec (Internet Protocol Security) is a group of protocols designed to allow flexible, secure and interoperable communication over the Internet. IPSec is used to establish an encrypted – and therefore, secure – connection between two points on a network.

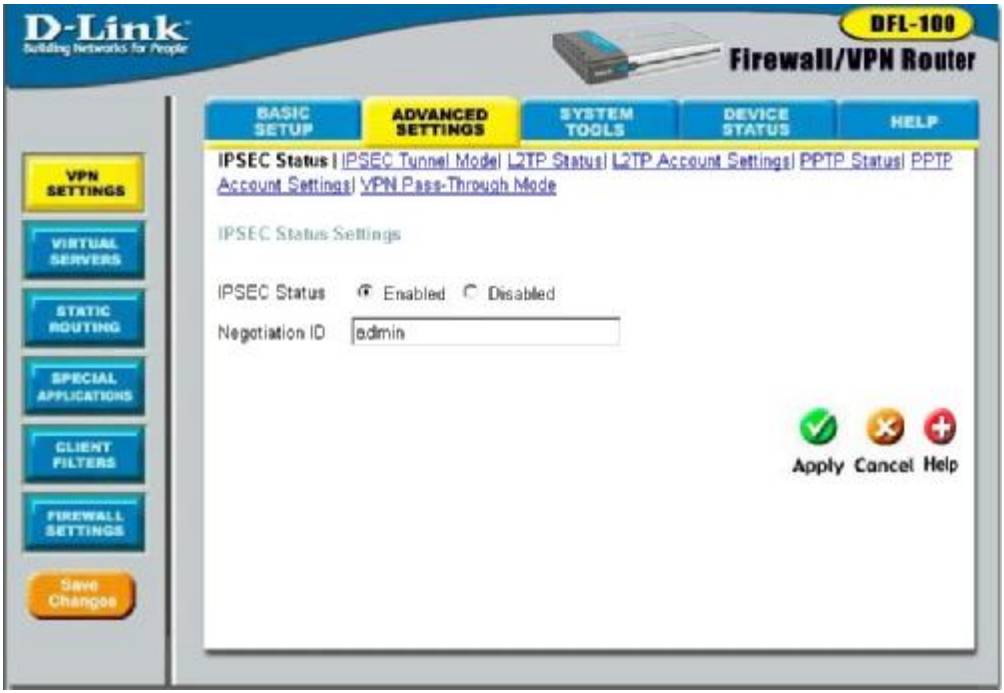
IPSec provides access control, connectionless data integrity, data origin authentication, protection against replay attacks and confidentiality for each IPSec packet. This is achieved by using headers and trailers on each packet, which provide core pieces of information pertaining to authentication, data integrity, and confidentiality. The AH (Authentication Header) addresses data origin authentication, data integrity, and replay protection. The ESP (Encapsulating Security Payload) header addresses the same features and also includes data confidentiality or encryption capabilities. By default, IPSec uses the AH as a minimum level for its capabilities. If data confidentiality is desired, the AH is replaced with an ESP header for the encryption feature and the authentication and data integrity components that the AH offer as well.

VPN Settings

The **VPN Settings** page allows you to create tunnels between the DFL-100 (the local endpoint of the tunnel) and remote gateways (the remote end of the tunnel.) Data passing through this tunnel between the two endpoints is encrypted, and therefore secure.

IPSEC Status

IPSec (Internet Protocol Security) is a group of protocols designed to allow flexible, secure and interoperable communication over the Internet. IPSec is used to establish an encrypted – and therefore, secure – connection between two points on a network. The IPSEC Status page allows you to enable or disable IPsec on the DFL-100. In addition, a **Negotiation ID** can be entered to identify your local end of the tunnel to the remote gateway.

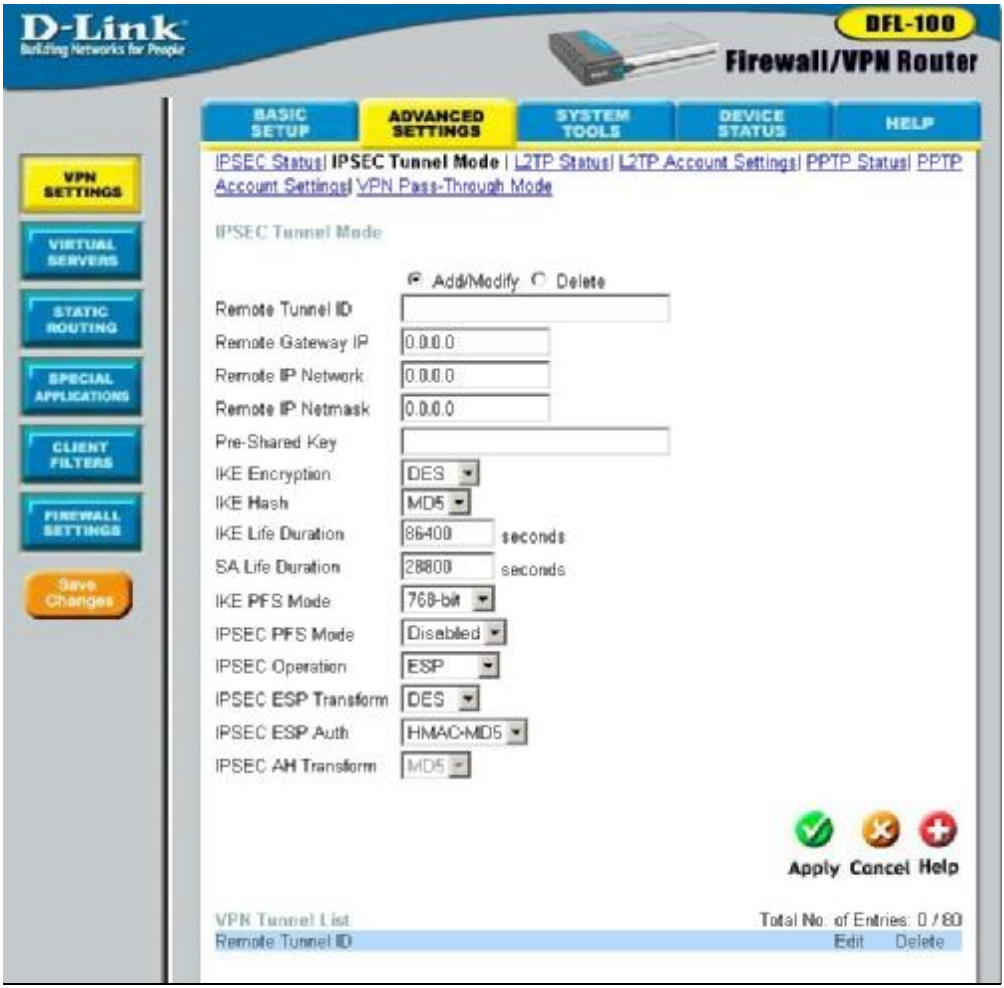


IPSEC Status	The IPsec feature can be **Enabled** or **Disabled** on the DFL-100 by clicking the appropriate click-box followed by clicking the **Apply** button.
Negotiation ID	This is an alphanumeric ID that is used in a

	similar way to a password. It is used to verify that the DFL-100 is authorized to make an IPsec connection with a remote gateway. Both ends of an IPsec connection must use the same **Remote Tunnel ID**.

IPSEC Tunnel Mode

The IPSEC Tunnel Mode page allows you to setup a secure tunnel between your DFL-100 and a remote gateway.

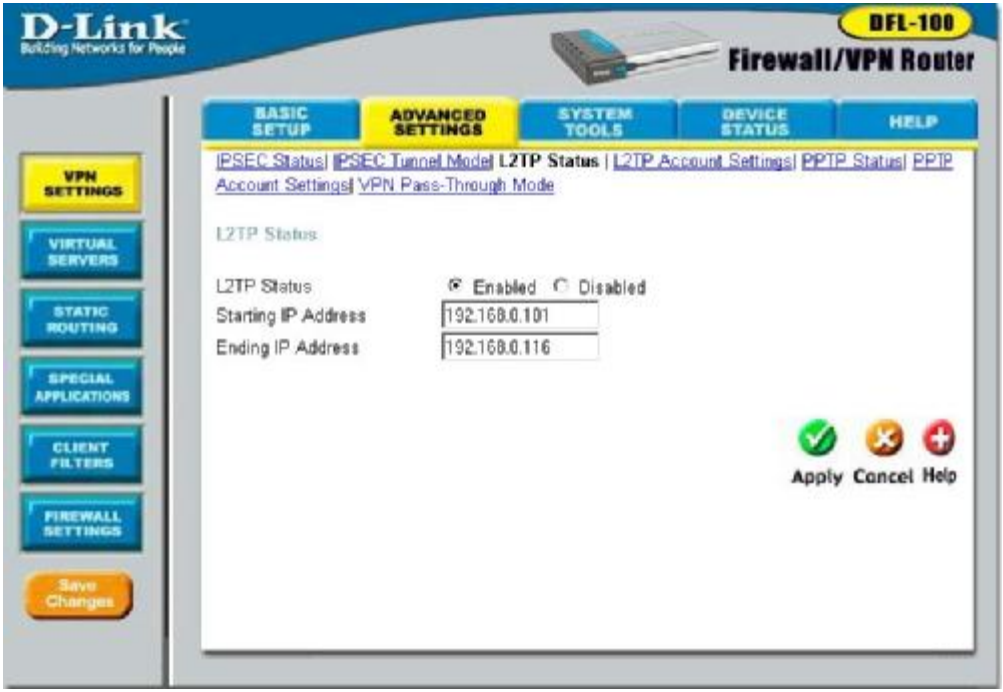


IPSEC Tunnel Mode	IPsec tunnels can be added, modified, or deleted from the DFL-100 by clicking the appropriate click-box and then the **Apply** button.
Remote Tunnel ID	An alphanumeric string that identifies the remote tunnel. A sting of up to 63 characters can be entered.
Remote Gateway IP	Enter the IP address of the remote gateway on the other end of the IPsec connection.
Remote IP Network	Enter the IP address of the remote network. This is a reserved IP address from the range of IP addresses assigned to the remote network. For example, if the remote network uses an IP address range of 192.168.0.0 to 192.168.0.255 and a subnet mask of 255.255.255.0 would use the first IP address of the range as its network address – 192.168.0.0.
Remote IP Netmask	Enter the subnet mask used by the remote network here.
Pre-Shared Key	This is an encryption key used to encrypt packets sent between the two ends of the IPsec tunnel.
IKE Encryption	You can select the encryption used to provide the IPsec function using the drop-down menu. The choices are **DES,** and **3DES**. The exact same encryption algorithm must be used on both ends of the IPsec connection.
IKE Hash	You can select the algorithm the IPsec connection will use to verify that packets have not been altered in transit. The choices are **MD5,** and **SHA**. The exact same **IKE Hash** algorithm must be used on both ends of the IPsec connection.
IKE Life Duration	This is used to specify the length of time that the IKE key can be in use before being updated with a new key. The default is 86400 seconds.
SA Life Duration	This is used to specify the length of time that the IKE Security Association (SA) can be in effect before being updated. The default is 28800 seconds.

IKE PFS Mode	This drop-down menu allows you to specify the mode of operation for IKE Perfect Forward Security (PFS). The options are **768-bit** and **1024-bit**.
IPSEC PFS Mode	This drop-down menu allows you to specify the mode that will be used for IPSec Perfect Forward Security (PFS). The choices are **Disabled**, **768-bit**, and **1024-bit**.
IPSEC Operation	This drop-down menu allows you to specify the mode of operation for IPsec on the DFL-100. The choices are **ESP**, **AH**, and **ESP-AH**.
IPSEC ESP Transform	This drop-down menu allows you to specify the algorithm the DFL-100 will use to provide secrecy information for the Encapsulated Security Protocol. The choices are **DES**, **3DES**, **RC4** and **Null**.
IPSEC ESP Auth	This drop-down menu allows you to specify the algorithm the DFL-100 will use to provide authorization for ESP. The choices are **HMAC-MD5, HMAC-SHA, DES-MAC** and **Null**.
IPSEC AH Transform	This drop-down menu allows you to specify the algorithm the DFL-100 will use to provide integrity protection for the Authorization Header (AH) transform. **MD5** is the only choice, if the **IPSEC Operation** mode is set to **ESP**, above. If the **IPSEC Operation** mode is set to either AH or ESP-AH, the choices are **MD5, SHA**, and **DES**..

L2TP Status

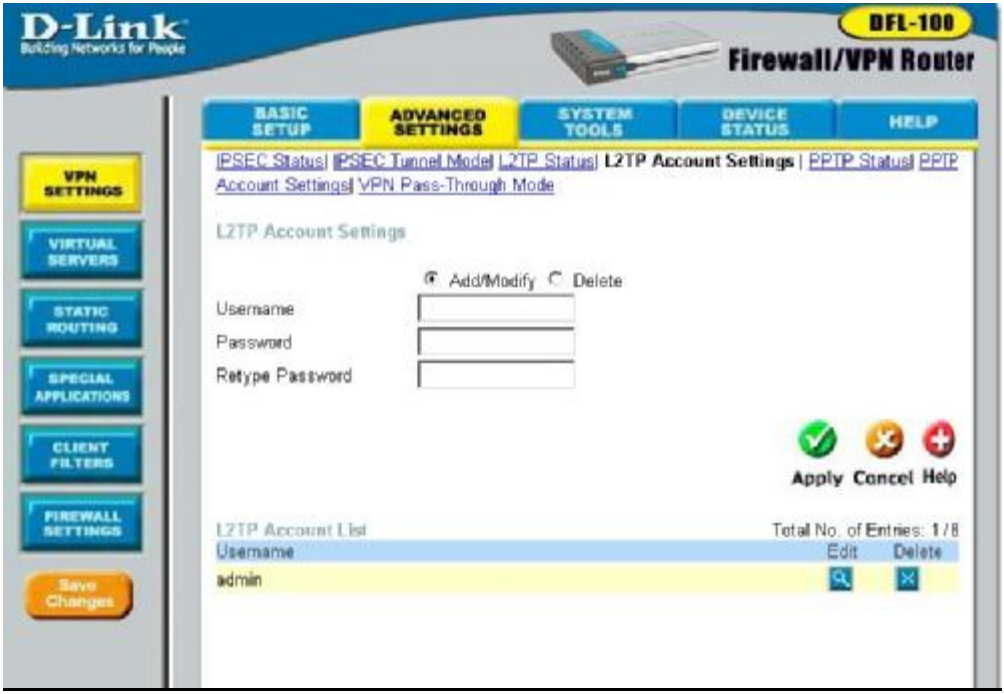
The Layer 2 Tunneling Protocol (L2TP) is another method of establishing a secure tunnel between your DFL-100 and a remote gateway. The L2TP Status page allows you to enable or disable L2TP on the DFL-100.



L2TP Server Status	L2TP can be **Enabled** or **Disabled** by clicking the appropriate click-box and the clicking the **Apply.**
Starting IP Address	This allows you to specify a range of IP addresses for servers on your network that can use the L2TP protocol. If you have only one IP address, enter this address in both the **Starting IP Address** and **Ending IP Address** fields.
Ending IP Address	This allows you to specify a range of IP addresses for servers on your network that can use the L2TP protocol. If you have only one IP address, enter this address in both the **Starting IP Address** and **Ending IP Address** fields.

L2TP Account Settings

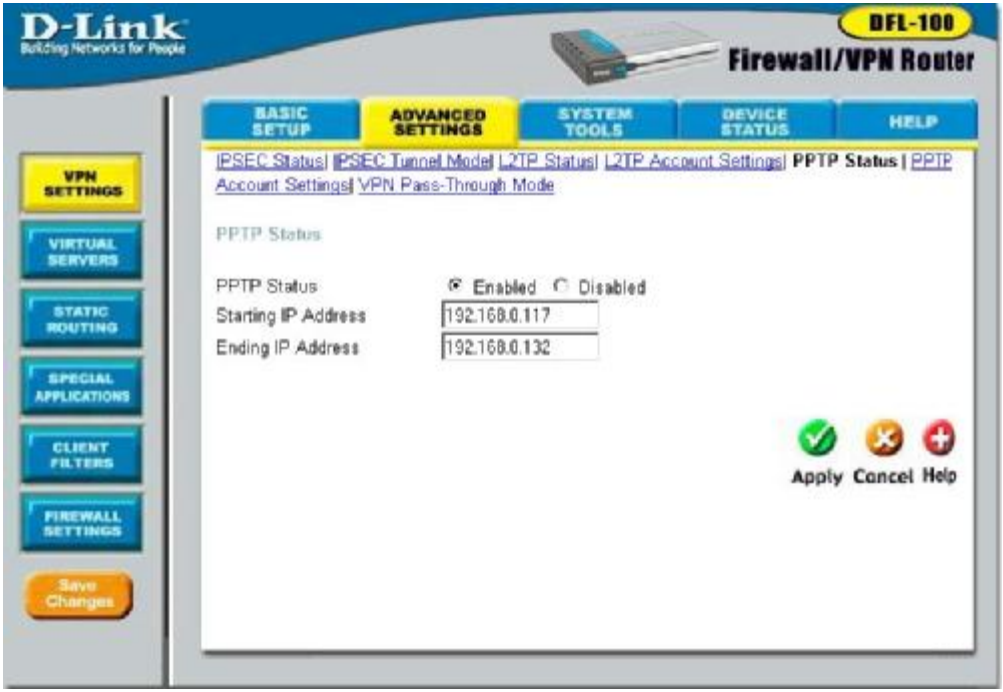
The L2TP page allows you enter your username and password for an L2TP account.



Username	Enter your L2TP account username here.
Password	Enter your L2TP account password here.
Retype Password	Re-enter your L2TP account password here to verify it has been entered correctly.

PPTP Status

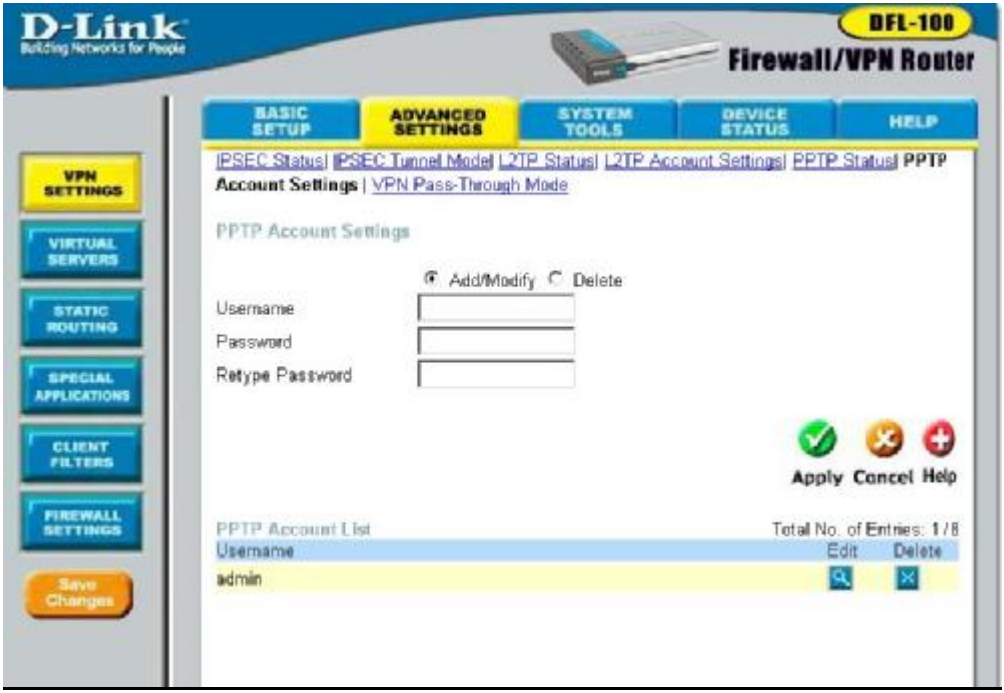
The Point-to-Point Tunneling Protocol (PPTP) is another method of establishing a secure tunnel between the DFL-100 and a remote gateway. The PPTP Status page allows you to enable or disable PPTP on the DFL-100.



PPTP Server Status	PPTP can be **Enabled** or **Disabled** by clicking the appropriate click-box and the clicking the **Apply.**
Starting IP Address	This allows you to specify a range of IP addresses for servers on your network that can use the PPTP protocol. If you have only one IP address, enter this address in both the **Starting IP Address** and **Ending IP Address** fields.
Ending IP Address	This allows you to specify a range of IP addresses for servers on your network that can use the PPTP protocol. If you have only one IP address, enter this address in both the **Starting IP Address** and **Ending IP Address** fields.

PPTP Account Settings

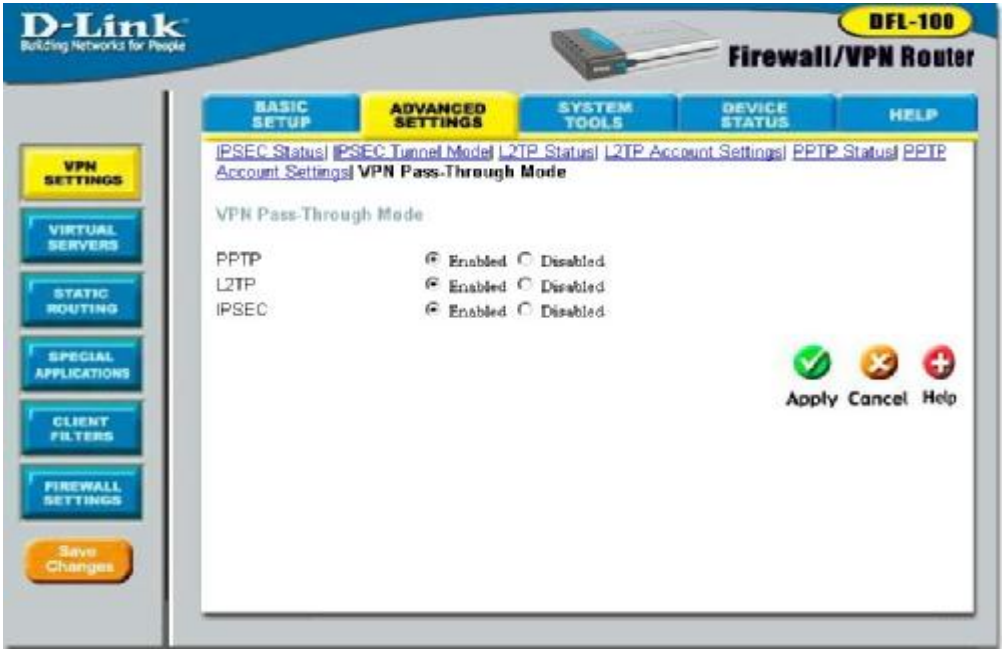
The PPTP Account Settings page allows you to enter a username and password for a PPTP account.



Username	Enter the appropriate username for your PPTP account here.
Password	Enter the appropriate password for your PPTP account here.
Retype Password	Retype the password your entered above here to confirm that it has been entered correctly.

VPN Pass-Through Mode

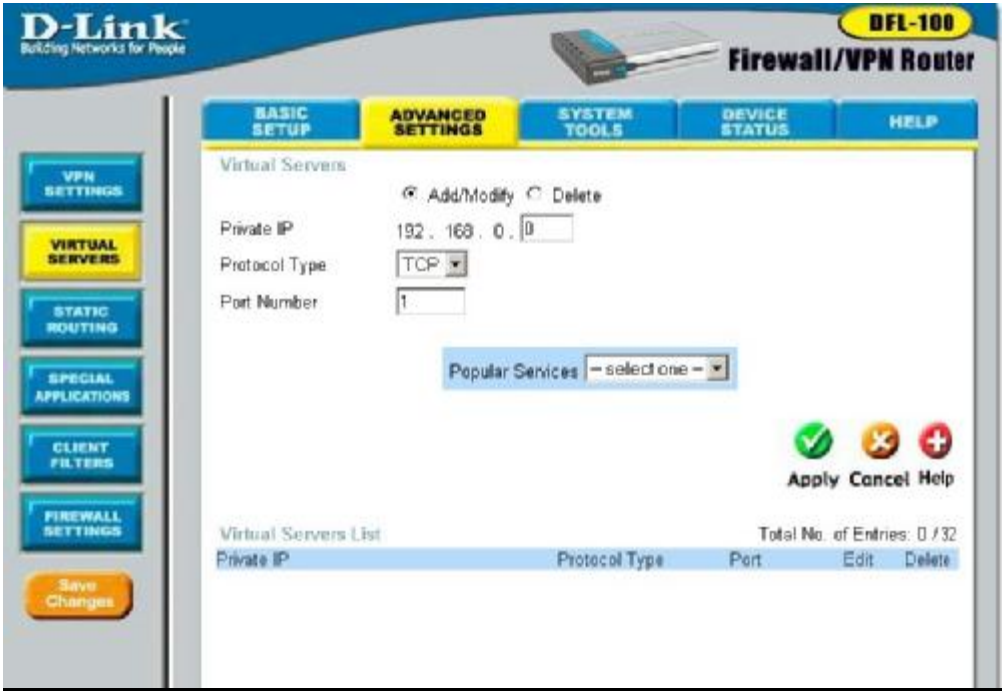
The VPN Pass-Through page allows you to enable or disable VPN Pass-Through for PPTP, L2TP, and IPSEC protocols.



PPTP	Passing of PPTP packets through the DFL-100 to a computer on the LAN side can be **Enabled** or **Disabled** on the DFL-100 by clicking the appropriate click-box and the clicking the **Apply** button.
L2TP	Passing of L2TP packets through the DFL-100 to a computer on the LAN side can be **Enabled** or **Disabled** on the DFL-100 by clicking the appropriate click-box and the clicking the **Apply** button.
IPSEC	Passing of IPSEC packets through the DFL-100 to a computer on the LAN side can be **Enabled** or **Disabled** on the DFL-100 by clicking the appropriate click-box and the clicking the **Apply** button.

Virtual Servers

Virtual Servers allow remote users to access services on your LAN such as FTP for file transfers or STMP and POP3 for e-mail. The DFL-100 will accept remote requests for these services at the Global IP Address you specify, using the TCP or UDP protocol and port number, and then redirect these requests to the server on your LAN with the Private IP address you specify. Remember, the Private IP Address must be within the range specified for your LAN.



Private IP	This is the IP address of the server on your LAN that will provide the service to remote users.
Protocol Type	You can select the protocol (TCP or UDP) that the application on the virtual server will use for its connections. The choice of this protocol is dependent on the application that is providing

	the service. If you do not know which protocol to choose, check your application's documentation.
Port Number	Select the TCP or UDP port number the application will use for its connections. The choice of this protocol is dependent on the application that is providing the service. If you do not know which protocol to choose, check your application's documentation.
Popular Services	The protocol type (TCP/UDP) and port number (a number between 1 and 65535) for several popular services that you might want to set up a virtual server for are listed here. The Protocol Type and Port Number will automatically be entered when you choose one of these entries.

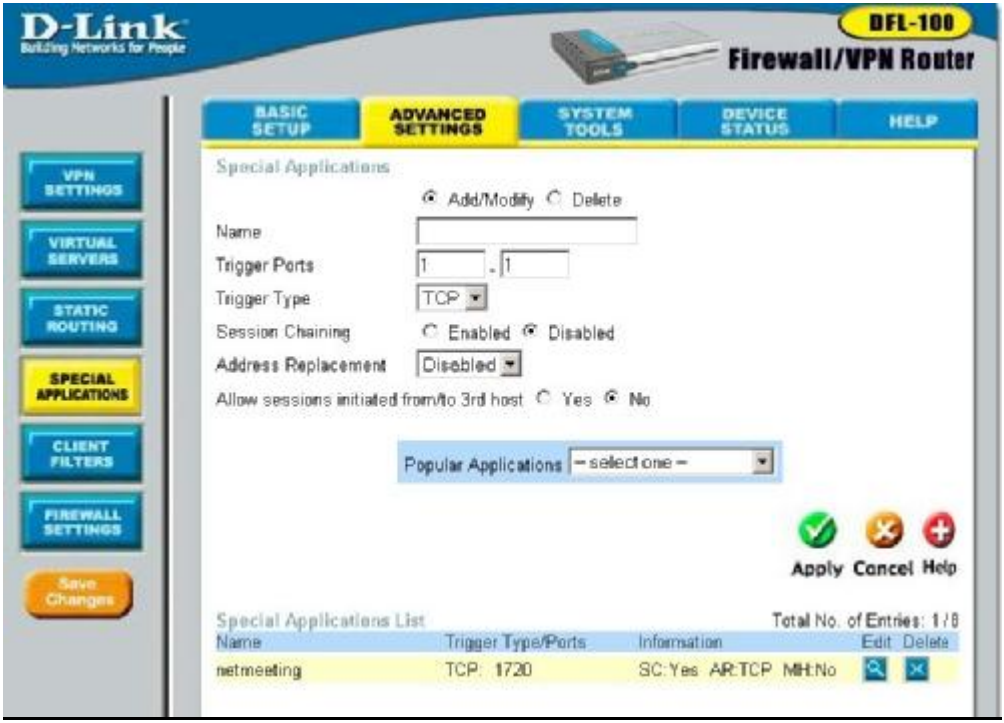
Static Routing

You can add entries to the DFL-100's routing table that will be saved to non-volatile RAM. These routes will not age out, and are therefore static.

Destination IP Network	This is the IP address of the remote network that the DFL-100 will route service requests to.
Subnet Mask	This is the corresponding subnet mask for the remote network.
Gateway IP Address	This is the IP address of the gateway on the remote network that will provide the connection between your DFL-100 and servers on the remote network.

Special Applications

Some applications require multiple TCP or UDP ports to function properly. Applications such as Internet gaming, video conferencing, and Internet telephony are some examples of applications that often require multiple connections. These applications often conflict with NAT, and therefore require special handling. The Special Applications page allows you to configure your DFL-100 to allow computers on your LAN to access servers on the WAN that require multiple TCP or UDP connections.

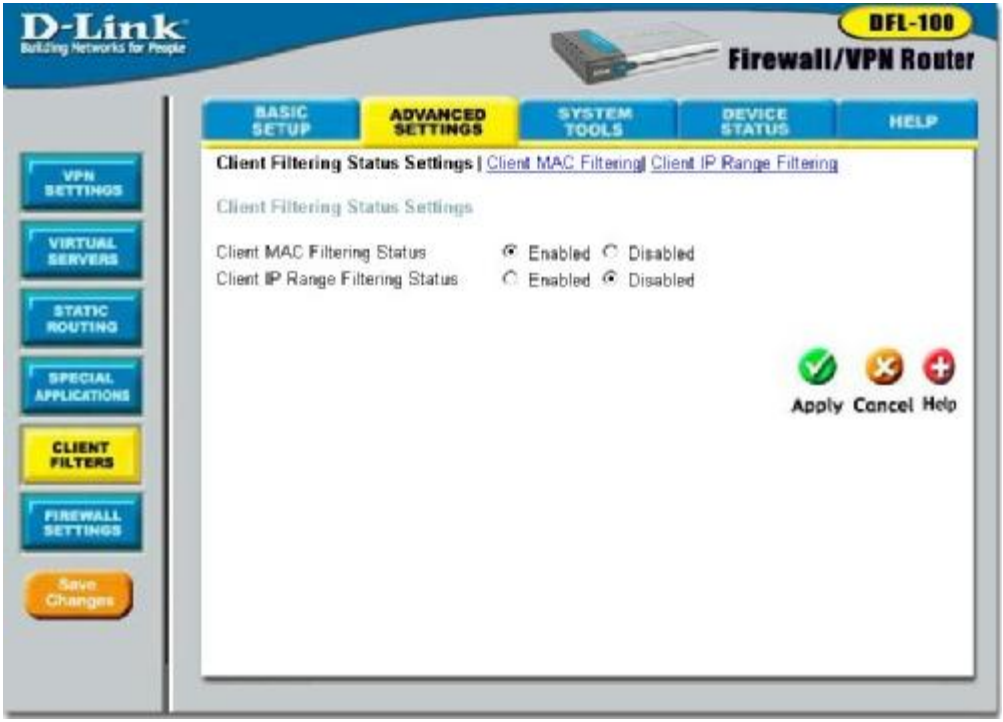


Name	This is a reference – usually the name of the application. In the above example, **netmeeting** is the application, it is used to name this entry.
Trigger Ports	This is the TCP or UDP port used to trigger, or start, the application. It can be a single port, or a range of ports. If only a single port is used, enter the same port number in both the starting and

	ending port number fields.
Trigger Type	This is the protocol (TCP or UDP) that the application uses to make the connection.
Session Chaining	If the application allows a dynamic session (connections) to trigger a new session, set this to **Enabled**. If an application uses protocols in addition to the TCP/UDP protocols (like many interactive Internet games), then this application will likely create additional sessions (using these additional protocols) that will need to associate with the first session. Again, **Session Chaining** should be set to **Enabled**, for this type of application,
Address Replacement	This option is used in Network Address Translation (NAT) to translate a binary IP address in a TCP/UDP packet. When a TCP or UDP packet is received by the DFL-100, the IP address in this packet will be translated between the WAN and LAN side of the DFL-100, if this option is enabled.
Allow sessions initiated from/to 3rd host	Set this option to **Yes** if your application allows a new session to be started with a different computer than the one that started the first session. For example, MSN file transfer requires a connection with a remote host, but this connection is not direct. There are other MSN servers between your PC and the MSN file server.
Popular Applications	The settings for a range of popular applications have been entered into the DFL-100's firmware and can be selected here from the drop-down menu.

Client Filters

The Client Filters page allows you to deny access to the WAN (Internet) to specific computers on your LAN, by specifying the computer's MAC or IP address. Once the addresses you want to filter have been entered into the DFL-100, these filters can be **Enabled** or **Disabled** from the following screen.

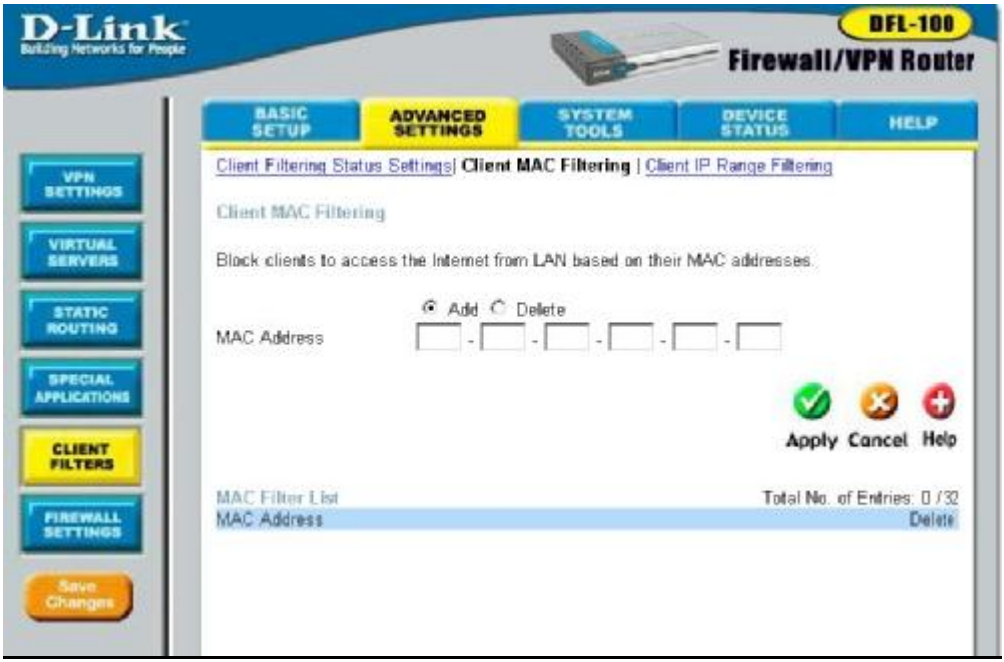


To **Enable** or **Disable** the filtering of MAC addresses previously entered into the DFL-100's filtering database, click the appropriate click-box, and then click the **Apply** button.

To **Enable** or **Disable** the filtering of a range of IP addresses previously entered into the DFL-100's filtering database, click the appropriate click-box, and then click the **Apply** button.

Client Filters - MAC Filtering

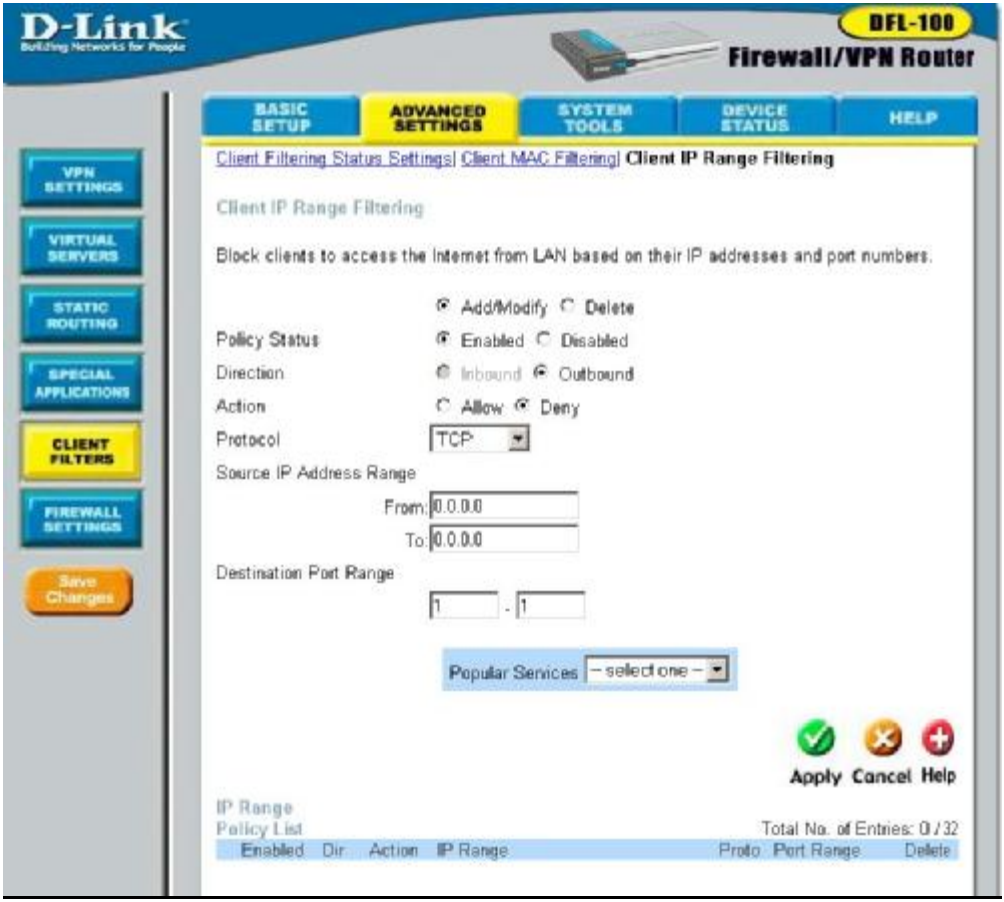
The Client Filters page allows you to deny access to the WAN (Internet) to specific computers on your LAN, by specifying the computer's MAC address.



MAC Address	Enter the MAC address of the computer on your LAN that you want to prevent from accessing the WAN (Internet).

Client IP Range Filtering

The Client Filters page allows you to deny access to the WAN (Internet) to specific computers on your LAN, by specifying the computer's MAC address.

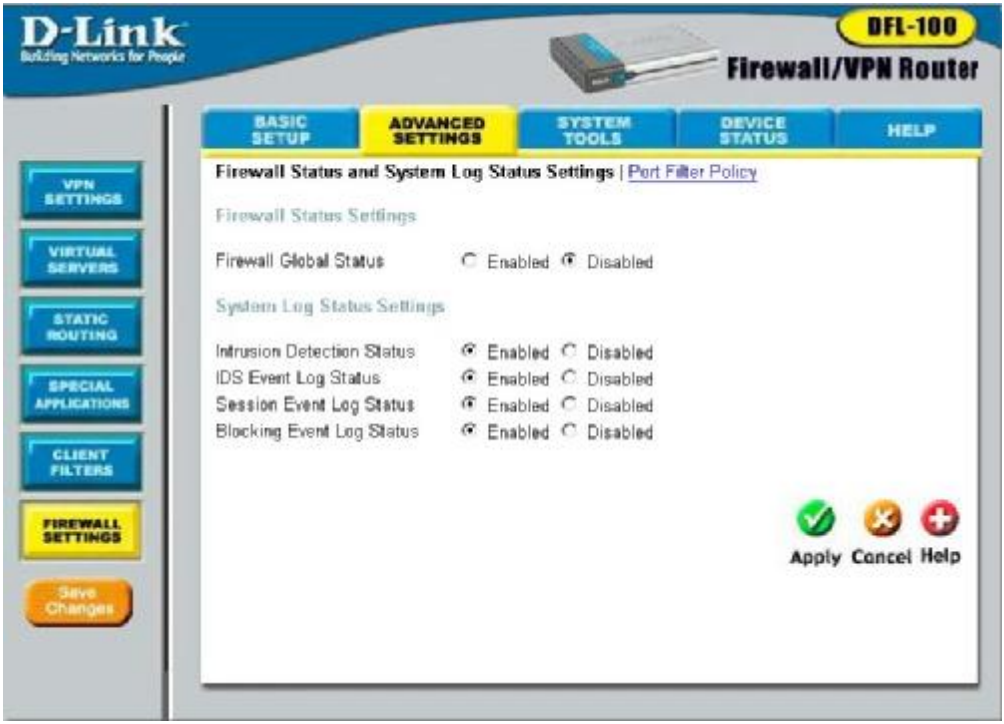


To set an IP address filtering policy, click the **Add/Modify** click-box, select Enabled under Policy Status, and then either **Allow** or **Deny** under **Action**. You can then select the protocol that will be in use for this IP address filtering policy, and enter the range of IP addresses in the **From** and **To** fields under **Source IP Address Range**. In addition, you can select a range of port numbers that will be used with the policy under **Destination Port Range**.

Block clients	This allows you to Add/Modify a new or existing policy. Delete allows you to remove a previously entered IP address filtering policy.
Policy Status	You can Enable or Disable a policy by clicking the appropriate click-box.
Direction	Currently, the only direction for which an IP address filtering policy can be configured is Outbound. This is from computers on your LAN to the WAN (Internet).
Action	You can specify whether the IP address policy is to **Allow** or to **Deny** the specified connection.
Protocol	This drop-down menu allows you to specify the protocol that the IP filter policy will be applied to. The choices are **TCP**, **UDP, ICMP**, and **Any**.
Source IP Address Range	This allows you to specify a range of IP address that the IP filter policy will be applied to. If you have only one IP address that you want to filter, enter this address if both the **From:** and **To:** fields.
Destination Port Range	This allows you to specify a range of port numbers (for the TCP and UDP protocols) that the IP filter policy will be applied to. If you have only one port number that you want to filter, enter this port number in both the **From:** and **To:** fields.
Popular Services	The protocol and corresponding port numbers for some popular applications or services have been pre-entered into the DFL-100. Any of these applications or services can be selected from this drop-down menu.

Firewall Settings

The firewall in your DFL-100 protects your LAN by blocking certain network traffic that may contain harmful code. You can enable or disable the Firewall using the Firewall Global Status.



Firewall Global Status	You can enable or disable the firewall on the DFL-100 here.
Intrusion Detection Status	The DFL-100 firewall includes protection from specific types of common Internet-based attacks. These include: SYN Flooding, TCP Hijacking, LAND Attack, WinNuke/OOBNuke, Christmas Tree, SYN/FIN (Jackal), SYN/FIN (zero-sized DNS zone payload), BackOffice (UDP port number 31337), NetBus, Smurf, Tear Drop, ICMP Flooding, and Trojan Horse. You can enable or disable the Intrusion

	Detection System here.
IDS Event Logging Status	If this option is enabled, the Intrusion Detection System (IDS) will keep a record of Intrusion events. This log is accessed on the **Intrusion Detection Log** page under the **Device Status** page.
Session Event Log Status	If this option is enabled, the DFL-100 will keep a record of session events. This log is accessed on the **Session Event Log** page under the **Device Status** page.
Blocking Event Log Status	If this option is enabled, the DFL-100 will keep a record of blocking events. This log is accessed on the **Blocking Event Log** page under the **Device Status** page.

Firewall Settings - Port Filter Policy

The DFL-100 allows you to specify a range of ports for connections between computers on the WAN and computers on your LAN that will be controlled. These IP addresses are entered on the **Port Filter Policy** page. Once entered, each Port Filter Policy can be enabled or disabled here.

Policy Status	This allows you to enable or disable the selected policy.
Direction	This allows you to specify the source of network traffic for which the current policy entry will be applied – from the Internet (Inbound), from your LAN (Outbound), or Both.

Action	This allows you to Allow or Deny access to the specified ports for the current policy entry.
Protocol	You can choose the protocol that will use the port specified for the entry. The choices are: **Any, ICMP, TCP**, and **UDP**.
Destination Port Range	You can enter a range of port numbers for which the current policy rules will be applied. If you have only one port number to enter, enter it in both fields.
Popular Services	The protocol and port number settings for several popular applications have been entered into the DFL-100's firmware and can be accessed from this drop-down menu.

System Tools

The System Tool tab provides links to utilities for the maintenance of your DFL-100.

Admin Settings

The Admin Settings page allows you to add or edit the Username and Password list to control access to the configuration of the DFL-100. There are two levels of access privilege – Root and User. A Root-level user can access all of the configuration options. A User-level user has read-only privileges. Up to 8 users can be configured with a username and password.

A default user account with the username **admin**, no password, and Root-level access is configured at the factory.

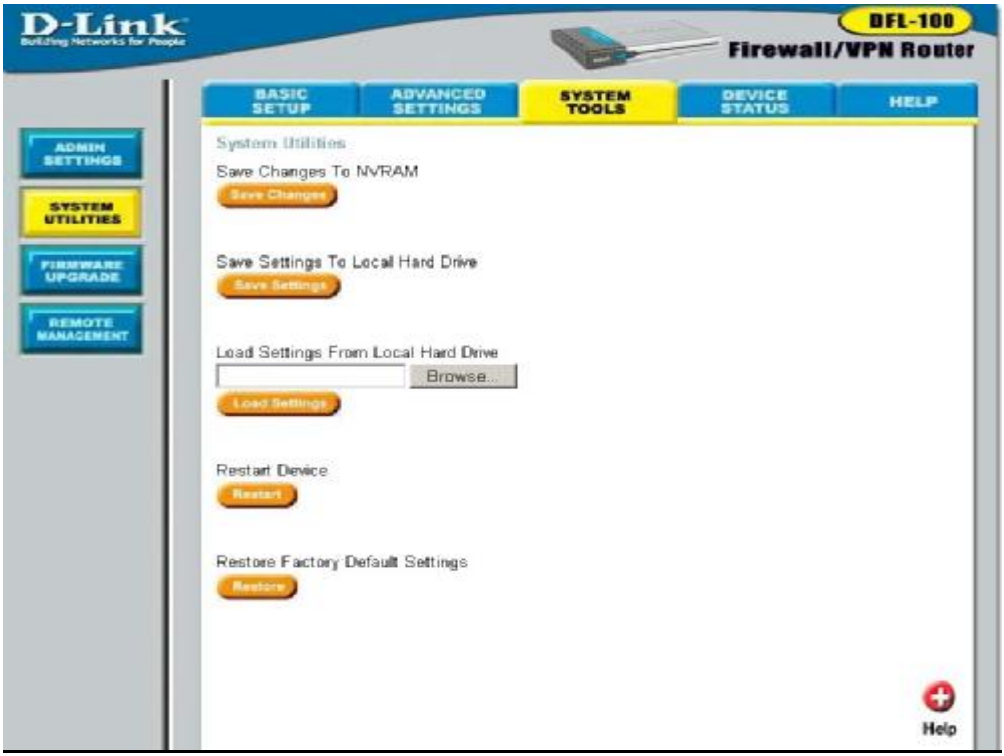
Username	Enter the username for the account here.
New Password	Enter the new password for the account here.
Confirm Password	Enter the new password again here to verify that the password has been entered correctly
Access Level	This drop-down menu allows you to specify the

	level of access privilege for the account. **Root** will give the user full access to all of the configuration options, while **User** will give the user read-only privileges.

System Utilities

The System Utilities page allows you to save the current configuration to the DFL-100's Non-Volatile RAM (NVRAM), to your local hard drive as a file. In addition, you can upload a configuration file from your local hard drive.

There are two options for restarting the DFL-100 – a simple restart, or a restart to the factory default settings. If you choose the **Restore Factory Default Settings** option, all of the configuration settings you have entered will be erased and the DFL-100 will be restored to the same configuration it had when it left the factory.



Save Changes to NVRAM	This will enter the current configuration into the DFL-100's Non-Volatile RAM (NVRAM).
Save Settings To Local Hard Drive	This option will save the current configuration as a file on your local hard drive.
Load Settings From Local Hard Drive	This option will up load a configuration from your local hard drive to the DFL-100.
Restart Device	This option will restart the DFL-100 with the configuration last entered into NVRAM.
Restore Factory Default Settings	This option will restart the DFL-100 with the factory default settings. All configuration information you have entered will be lost.

Firmware Upgrade

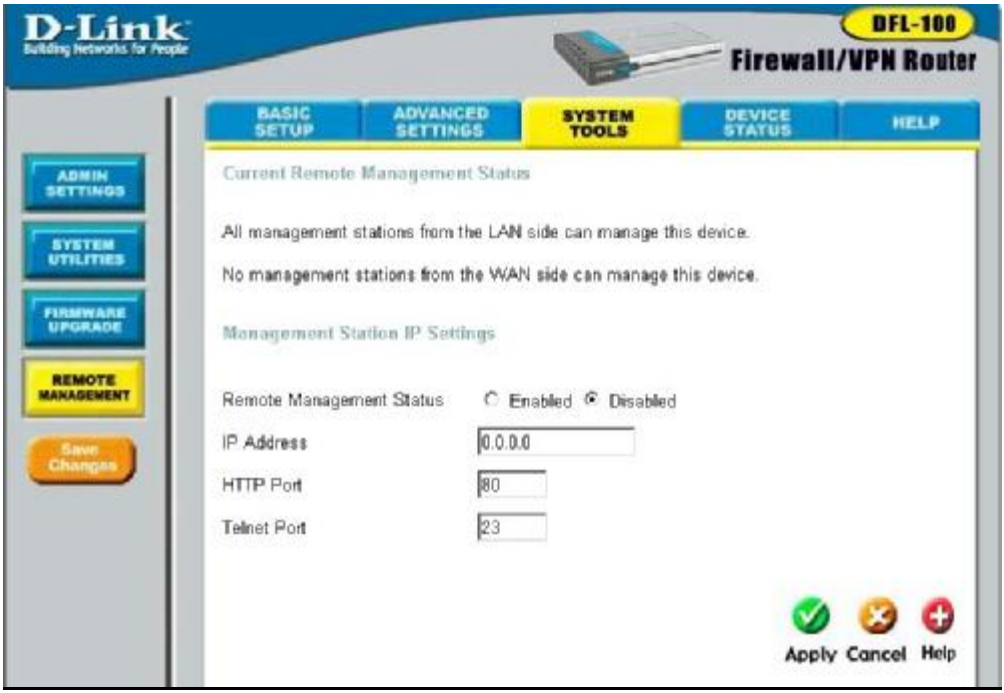
The Firmware Upgrade page allows you to upgrade the DFL-100's firmware from a new firmware file stored on your local hard drive.

In addition, a link to the D-Link website is provided so you can check to see if a new firmware version has been released for your DFL-100.

Path and Filename Field	Enter the full DOS path and filename to the new firmware file on your local hard drive. For example, if the file is in the root directory of your C drive, enter **C:\newfile.had** and click the **Apply** button to begin the file transfer.
Browse	If you are unsure about the location of the new firmware file on your local hard drive, click the **Browse** button to open a Windows Explorer window to look for this file.

Remote Management

The Remote Management page allows you to enter the IP addresses of computers on your LAN that will be allowed to access the configuration utility. If you do not enter any IP addresses on this page, then all IP addresses on your LAN (all computers) can access the DFL-100's configuration utility.



IP Address	Enter the IP address of a management station on the WAN side of the DFL-100 in this field. If no IP addresses are entered, then remote management of the DFL-100 will not be possible.
HTTP Port	This field allows you to specify which HTTP Port number a remote management computer can use to contact your DFL-100. The default port number is 80.
Telnet Port	This field allows you to specify which Telnet Port number a remote management computer can use to contact your DFL-100. The default port number is 23.

Device Status

The Device Status page displays the current network settings and allows you to view the IP address assigned to the DFL-100 by your ISP using DHCP (Dynamic Host Configuration Protocol – the **Dynamic IP Address** setting on the **ISP Settings page** under **Basic Setup**).

LAN Status

MAC Address	This is the MAC address of the DFL-100 on the LAN.
IP Address	This is the DFL-100's current IP address on the LAN.
Subnet Mask	This is the subnet mask corresponding to the IP address above, that is currently in use by the DFL-100 on the LAN.
DHCP Server	Displays whether the DFL-100 is currently configured as a DHCP server on the LAN.

WAN Status

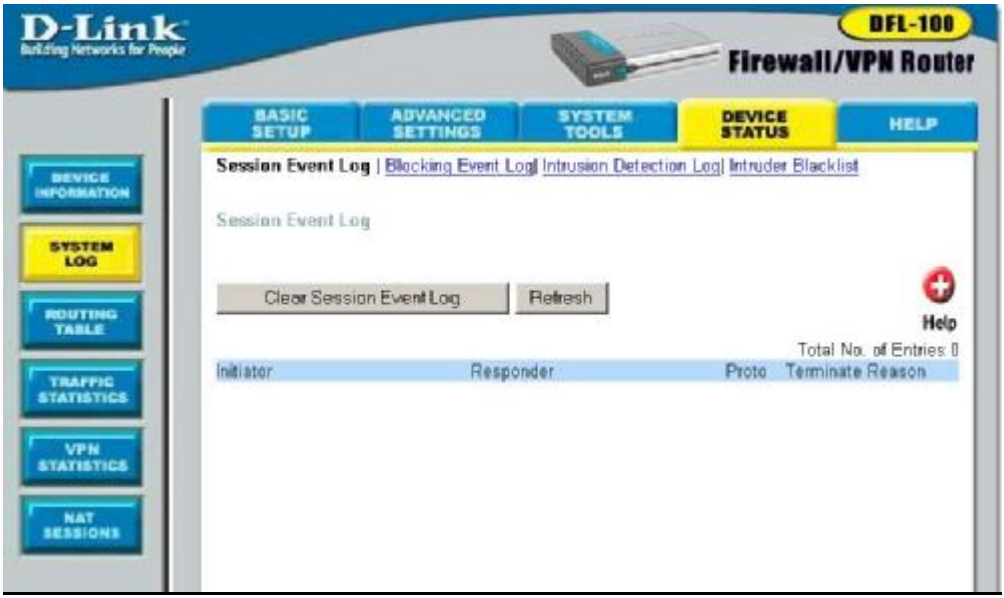
MAC Address	This is the MAC address of the DFL-100 on the WAN.
Connection Type	This displays the current connection type between the DFL-100 and your ISP.
IP Address	This is the IP address of the DFL-100 on the WAN.
Subnet Mask	This is the subnet mask corresponding to the IP address above, that is currently in use by the DFL-100 on the WAN.
Default Gateway	Displays the IP address of the default gateway on the WAN.
Primary DNS	Displays the IP address of the primary DNS on the WAN.
Secondary DNS	Displays the IP address of the secondary DNS on the WAN.

DMZ Status

DMZ Status	Displays whether the DMZ port is enabled or disabled on the DFL-100.
IP Address	Displays the IP address assigned to the DMZ port.
Subnet Mask	This is the subnet mask corresponding to the IP address above, that is currently in use by the DFL-100 on the LAN.

System Log - Session Event Log

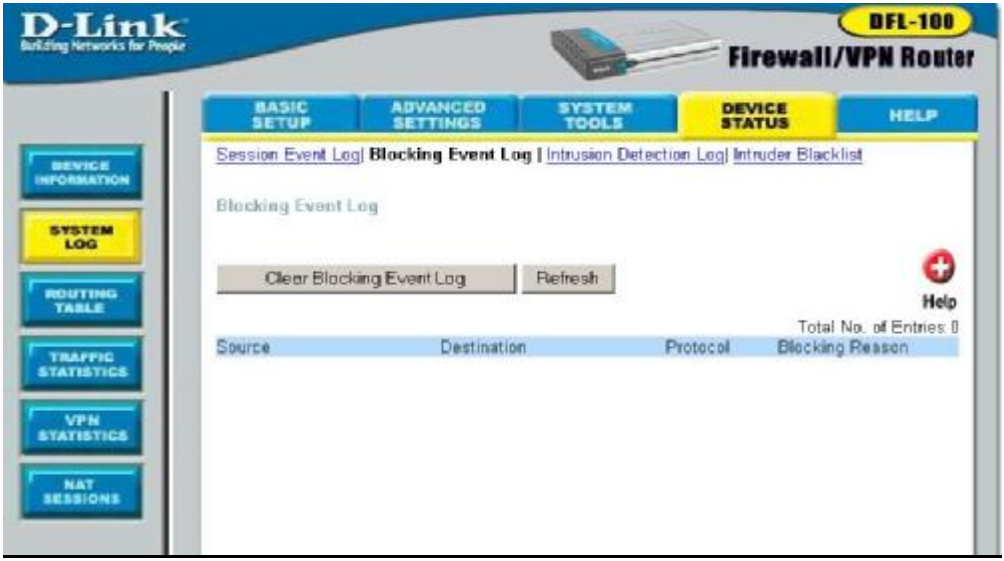
Session events (when a computer on your LAN accesses an application of service on the WAN), are logged by the DFL-100 and are displayed on the **Session Event Log**, as shown below:



Initiator	The IP address of the computer or device that initiated the session is displayed here.
Responder	The IP address of the computer or device that responded to the session initiation is displayed here.
Proto	The protocol used to conduct the session is displayed here.
Terminate Reason	When the session is terminated, it is displayed here.

System Log - Blocking Event Log

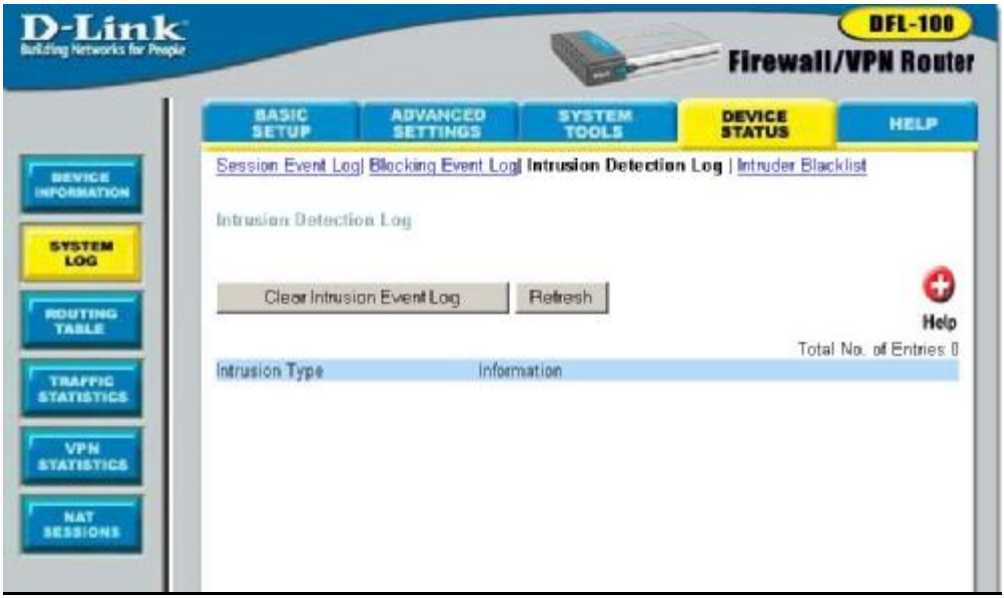
Certain sessions between computers on your LAN and the WAN have the potential to cause a disruption in the function of your computers and are blocked by the DFL-100's firewall. Some of these session types are defined by you under on the **Port Filter Policy** page, under **Firewall Settings** from the **Advanced Settings** tab. Events blocked (attempts to connect to computers on your LAN, between computers on your LAN, or between computers on your LAN and the WAN) because they met the criteria you entered on the **Port Filter Policy** page, are recorded here, in the **Blocking Event Log**, as shown below:



Source	The IP address of a computer or device that has had a connection attempt to the DFL-100 blocked is displayed here.
Destination	The IP address of the computer or device that was the destination of connection attempt to the DFL is displayed here.
Protocol	The protocol used to make the connection attempt is displayed here.
Blocking Reason	A brief statement of why the connection attempt was blocked is displayed here.

System Log - Intrusion Detection Log

Certain sessions between computers on your LAN and the WAN have the potential to cause a disruption in the function of your computers and are blocked by the DFL-100's firewall. Some of these session types are pre-defined by the factory, and are commonly used intrusion methods. Events blocked (attempts to connect to computers on your LAN, between computers on your LAN, or between computers on your LAN and the WAN) because they meet the criteria pre-defined at the factory as being a commonly used intrusion method, are recorded here, in the **Intrusion Detection Log**, as shown below:



Intrusion Type	A brief statement of the type of intrusion that was attempted is displayed here.
Information	Any relevant information about the attack is displayed here.

System Log - Intruder Blacklist

The DFL-100's firewall is pre-programmed to recognize and block many commonly used intrusion methods from computers on the WAN (Internet,) from one computer to another on the LAN, and from computers on your LAN to the WAN. In addition, you can define a Port Filter Policy, that will set additional intrusion criteria for the DFL-100's firewall to block connections. When a serious intrusion attempt is detected (that is, when a large number of packets consistent with a commonly used intrusion method are detected by the DFL-100) the IP address, the protocol used, and the corresponding port number is determined and entered into the DFL-100's Intruder Blacklist. Once the intruder's information is entered, the DFL-100's firewall will block packets from this location from crossing the DFL-100 (from the WAN to the LAN, from two computers on the LAN, or from the LAN to the WAN).

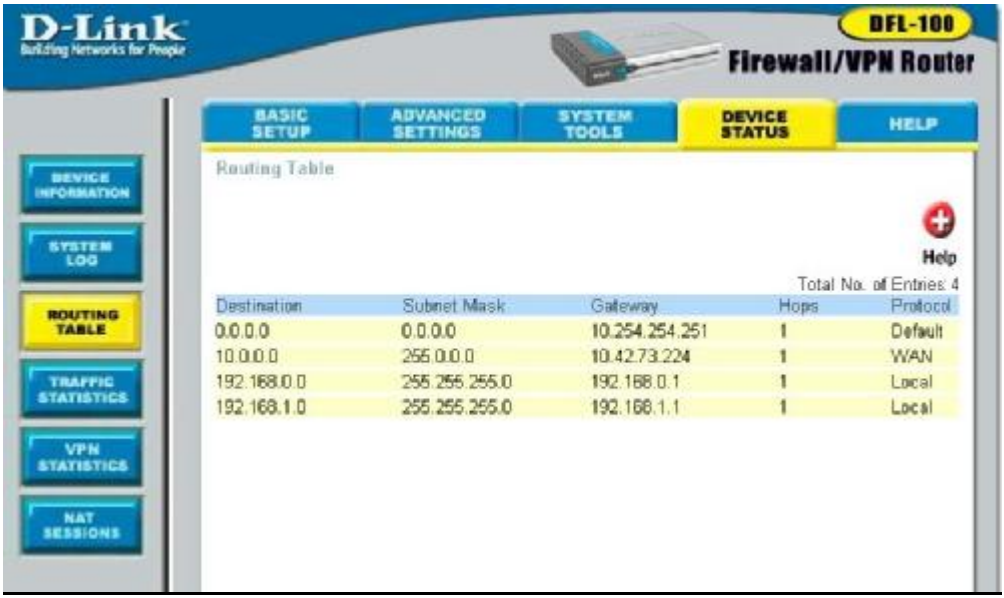
Once an intruder's IP address is listed in the Intruder Blacklist, it will remain until it times out. Each new intrusion attempt will reset the timer, and the intruder's IP address will remain in the Intruder Blacklist for an additional amount of time. While the intruder's IP address is on the DFL-100's Intruder Blacklist, that IP address is blocked from sending packets through the DFL-100.

You can clear the Intruder Blacklist at any time by clicking the **Clear** button.

Source IP	The IP address of a computer or device that will not be allowed to make a connection from the WAN to the DFL-100 is displayed here.
Destination IP	The IP address of the computer or device that the intruder has tried to connect to is displayed here.
Destination Port/ICMP Type	The port number or ICMP Type that an intruder used to attempt to make a connection is displayed here.

Routing Table

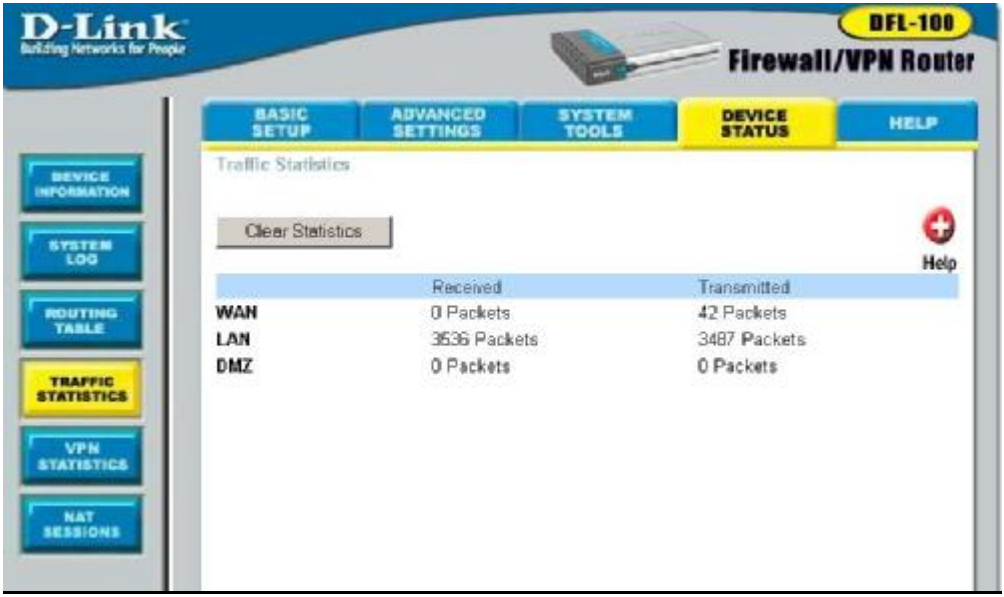
The DFL-100 maintains a table of source and destination IP addresses between computers on your LAN and the WAN (Internet). These addresses are used to determine where to send packets so that the various computers connected to the DFL-100 can communicate with each other and with computers on the WAN. This list is called the Routing Table, and can be viewed on the **Routing Table** page, as shown below:



Destination	The network address of the route's destination is displayed here.
Subnet Mask	This is the subnet mask corresponding to the network address above.
Gateway	The IP address of the gateway for the corresponding route is displayed here.
Hops	The number of routers between the DFL-100 and the Destination is displayed here.
Protocol	The protocol in use for the corresponding route is displayed here.

Traffic Statistics

The DFL-100 maintains a table containing the number of packets received and transmitted on the three networks that it interconnects: the **WAN**, the **LAN**, and the **DMZ**. These statistics can be viewed on the **Traffic Statistics** table, as shown below:



WAN	The total number of packets Received and Transmitted between the WAN and the DFL-100 are displayed here.
LAN	The total number of packets Received and Transmitted between the LAN and the DFL-100 are displayed here.
DMZ	The total number of packets Received and Transmitted between the DMZ and the DFL-100 are displayed here.

VPN Statistics

IPSEC Statistics

The DFL-100 maintains a table containing statistics concerning the IPSec protocol connection between the WAN and the LAN. These statistics can be viewed on the **IPSEC Statistics** table, as shown below:

IPSEC (Internet Protocol Security) uses the Internet Key Exchange (IKE) protocol to perform a two-phase negotiation. The two phases are creatively termed Phase 1 (also called Main Mode) and Phase 2 (also called Quick Mode). The purpose of Phase 1 is to protect the security negotiations by establishing a Security Association (called an IPSEC SA). Phase 2 begins upon completion of Phase 1 negotiation. The messages exchanged during Phase 2 negotiations are protected by a previously established IPSEC SA, the secure channel or tunnel created in Phase 1.

Phase 1 negotiation involves three basic steps:

1. Negotiation of protection protocol
2. Key exchange
3. Authentication

During Phase 2 negotiation, keying material is refreshed or, if necessary, new keys are generated. Terms for protecting specific types of IP traffic may also be negotiated. Phase 2 is dependent upon a previous Phase 1 negotiation.

Remote Tunnel ID	This displays the Tunnel ID of the device on the remote end of a VPN tunnel.
Status	This displays whether the VPN tunnel is active or not. There are five categories of status that can be displayed here, as follows: **Negotiation P1** – Phase 1 negotiation is in progress. **Negotiating P2** – Phase 2 negotiation is in progress. **Phase 1 Est** – Phase 1 is completed (i.e. an IPSEC SA is established and a secure tunnel exists). **Phase 2 Est** – Phase 2 is completed, that is, the terms are set for secure transfer of data using the tunnel established in Phase 1. **Broken** – The IPSEC SA is terminated, expired or can not be established.
Received	This displays the total number of packets received across the corresponding VPN tunnel.
Transmitted	This displays the total number of packets transmitted across the corresponding VPN tunnel.

L2TP Statistics

The DFL-100 maintains a table containing statistics concerning the L2TP protocol connection between the WAN and the LAN. These statistics can be viewed on the **L2TP Statistics** table, as shown below:

Remote Tunnel ID	This displays the Tunnel ID of the device on the remote end of a VPN tunnel.
Status	This displays whether the VPN tunnel is active or not.
Received	This displays the total number of packets received across the corresponding VPN tunnel.
Transmitted	This displays the total number of packets transmitted across the corresponding VPN tunnel.

PPTP Statistics

The DFL-100 maintains a table containing statistics concerning the PPTP protocol connection between the WAN and the LAN. These statistics can be viewed on the **PPTP Statistics** table, as shown below:

Remote Tunnel ID	This displays the Tunnel ID of the device on the remote end of a VPN tunnel.
Status	This displays whether the VPN tunnel is active or not.
Received	This displays the total number of packets received across the corresponding VPN tunnel.
Transmitted	This displays the total number of packets transmitted across the corresponding VPN tunnel.

NAT Sessions

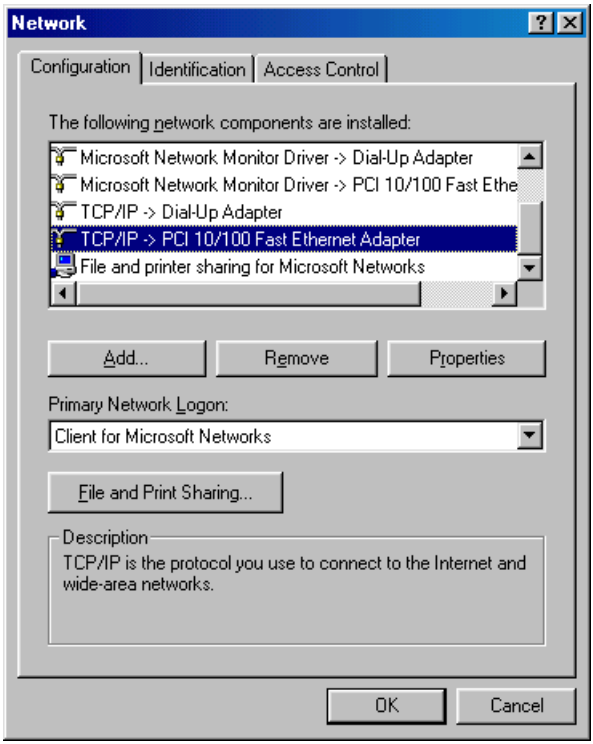
The DFL-100 maintains a table containing statistics concerning the Network Address Translation (NAT) applied between the WAN and the LAN. These statistics can be viewed on the **NAT Sessions** table, as shown below:

Internal IP: Port	This is the IP address and port number of a computer or device on your LAN that has an active NAT session.
Pseudo IP: Port	This is the IP address of the DFL-100 and port number that is translated between the LAN and the WAN to make a connection with the DFL-100.
Peer IP: Port	This is the IP address and port number of a computer or device on the WAN that has a active connection with the DFL-100
Transport	Displays the protocol used to transport packets.

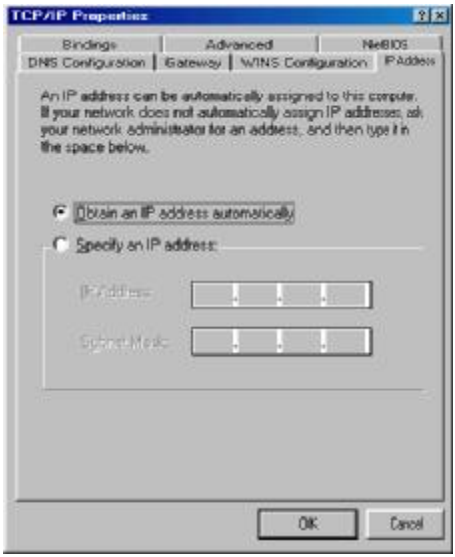
Connecting PCs to the DFL-100 Router

If you **do not** wish to set the static IP address on your PC, you will need to configure your PC to request an IP address from the gateway.

Click the Start button, select Settings, select Control Panel.
Double-click the Network icon.
In the configuration tab, select the TCP/IP protocol line that has been associated with your network card/adapter. If there is no TCP/IP line listed, you will need to install TCP/IP now.



Click the **Properties** button, then choose the **IP ADDRESS** tab. Select **Obtain an IP automatically**.



After clicking **OK**, windows might ask you to restart the PC. Click **Yes**.

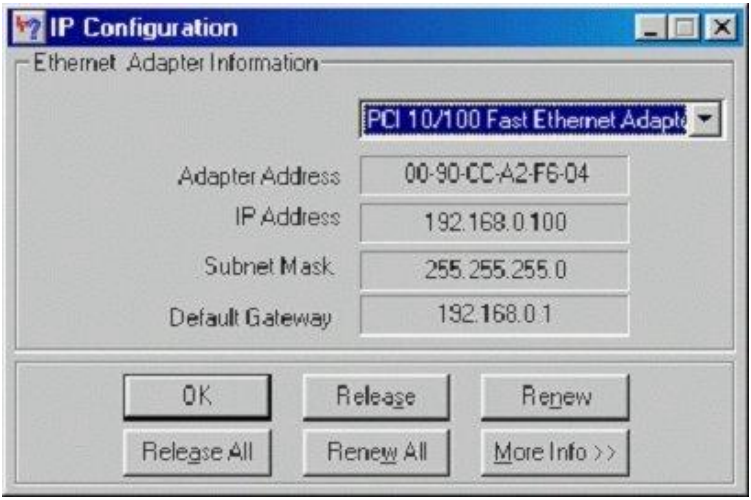
CONFIRM YOUR PC'S IP CONFIGURATION

There are two tools which are great for finding out a computer's IP configuration: MAC address and default gateway.

- **WINIPCFG (for Windows 95/98)**

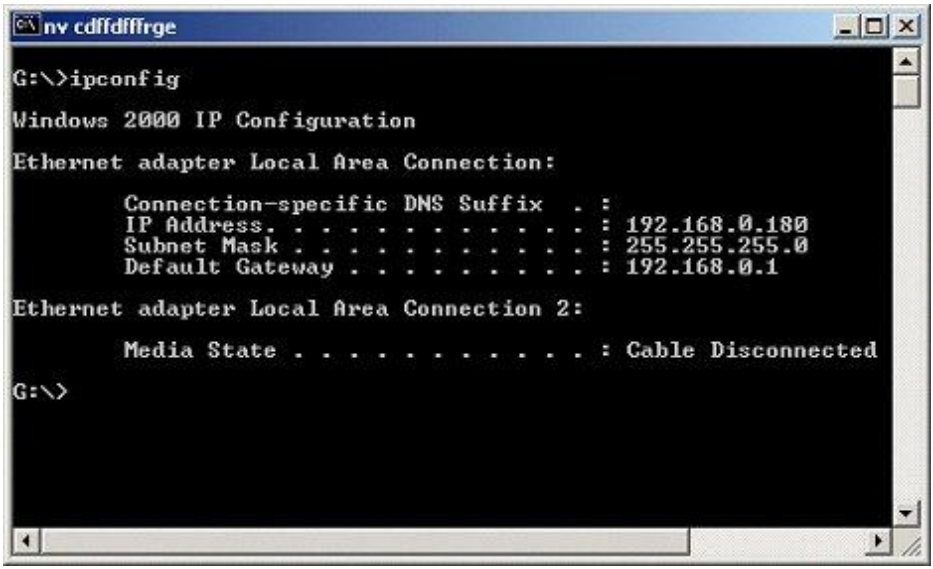
Inside the windows 95/98 Start button, select Run and type winipcfg. In the example below this computer has an IP address of 192.168.0.100 and the default gateway is 192.168.0.1. The default gateway should be the network device IP address. The MAC address in windows 95/98 is called the Adapter Address.

NOTE: You can also type **winipcfg** in the DOS command prompt.



- IPCONFIG (for Windows 2000/NT/XP)

In the DOS command prompt type **IPCONFIG** and press **Enter**. Your PC IP information will be displayed as shown below.

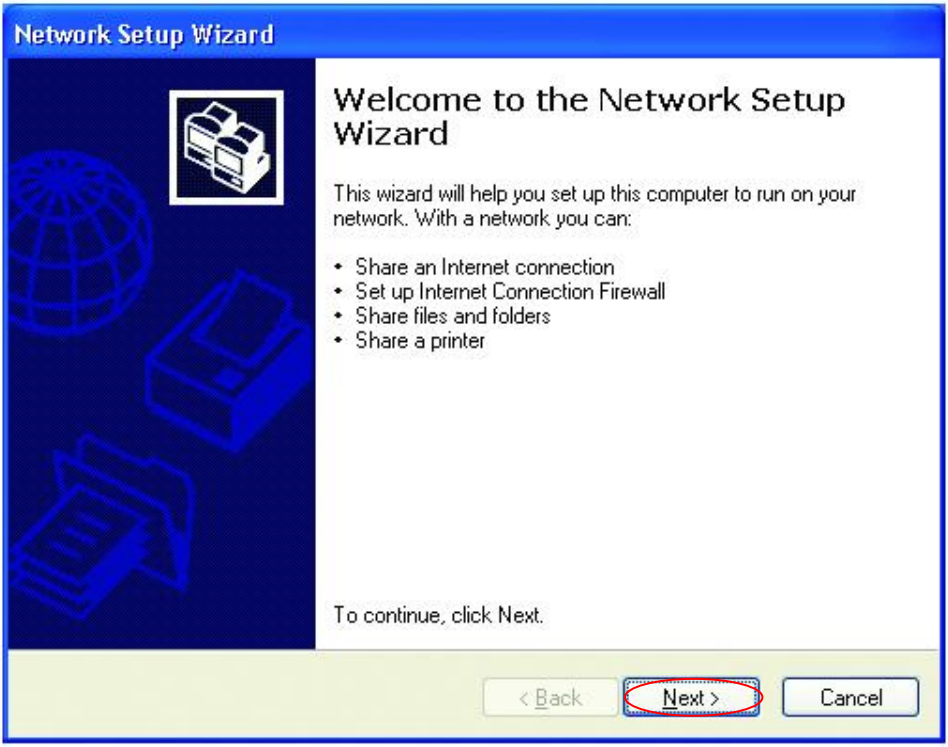


Networking Basics

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

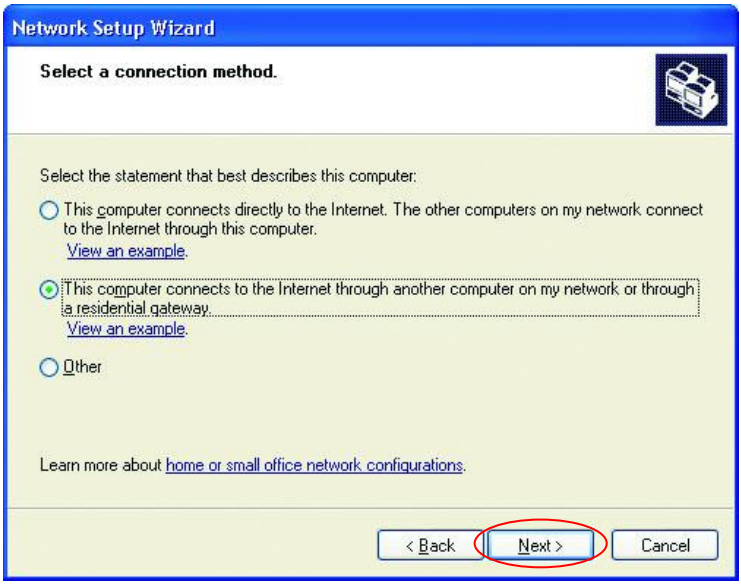


When this screen appears, Click **Next**.

Please follow all the instructions in this window:

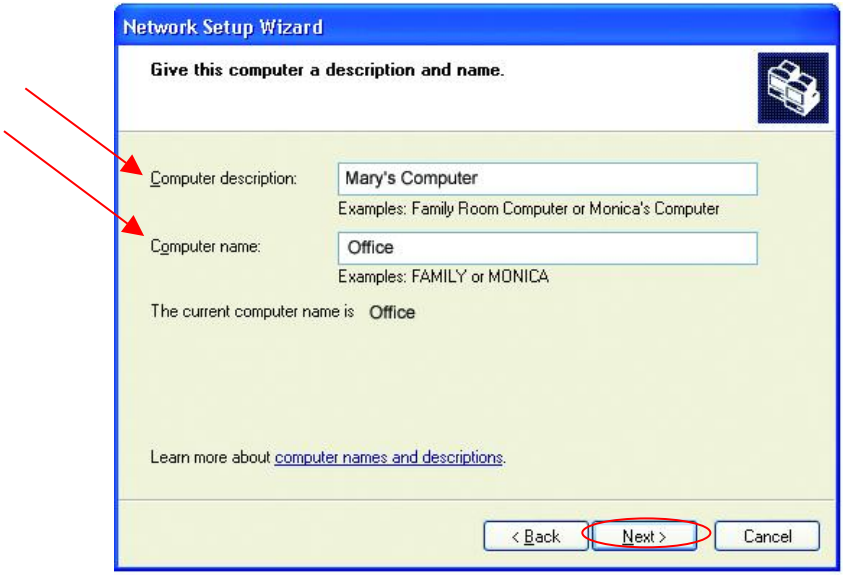
Click **Next**

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



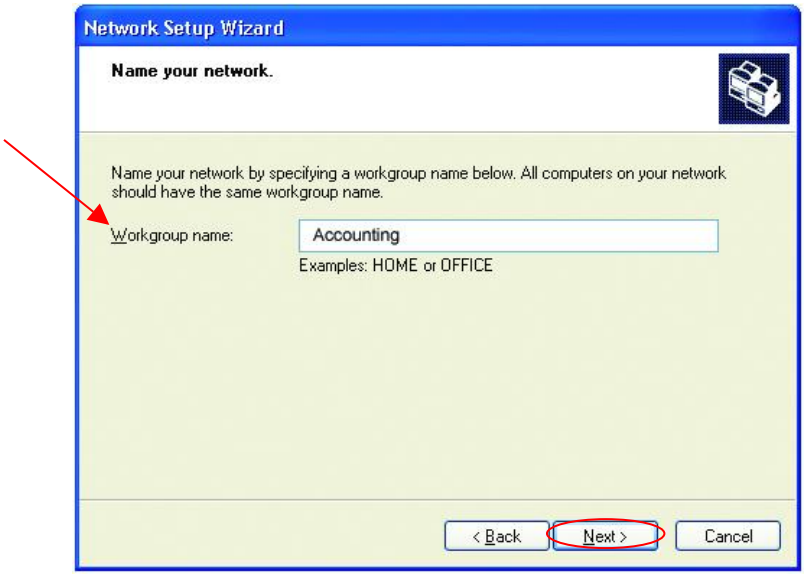
Click **Next**

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



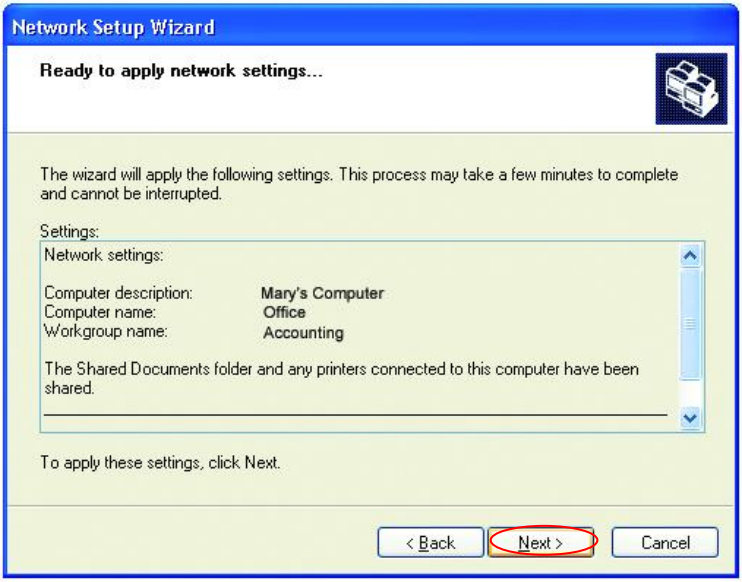
Click **Next**

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



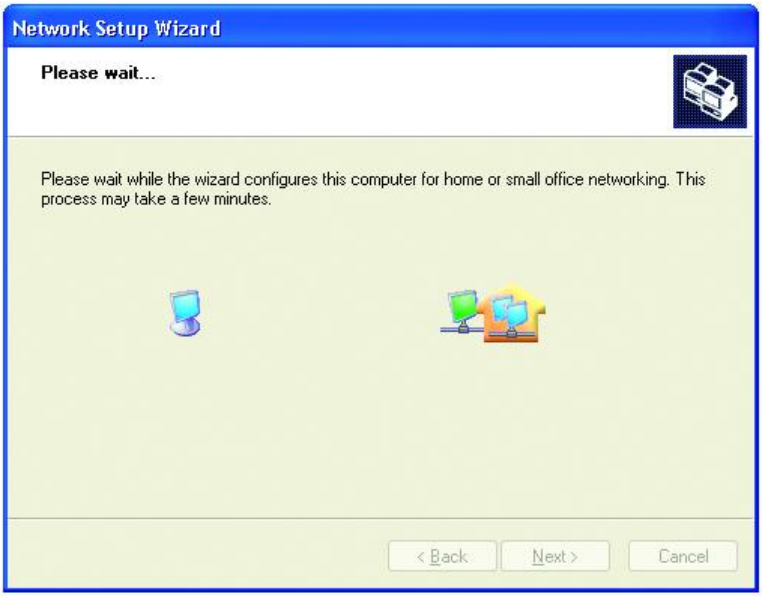
Click **Next**

Please wait while the wizard applies the changes.



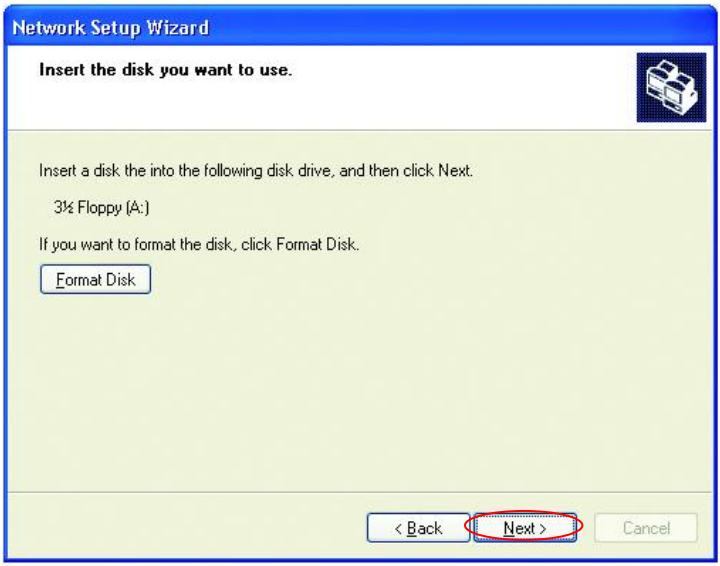
When the changes are complete, Click **Next**.

Please wait while the wizard configures the computer.
This may take a few minutes.



In the window below, select the best option. 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:”

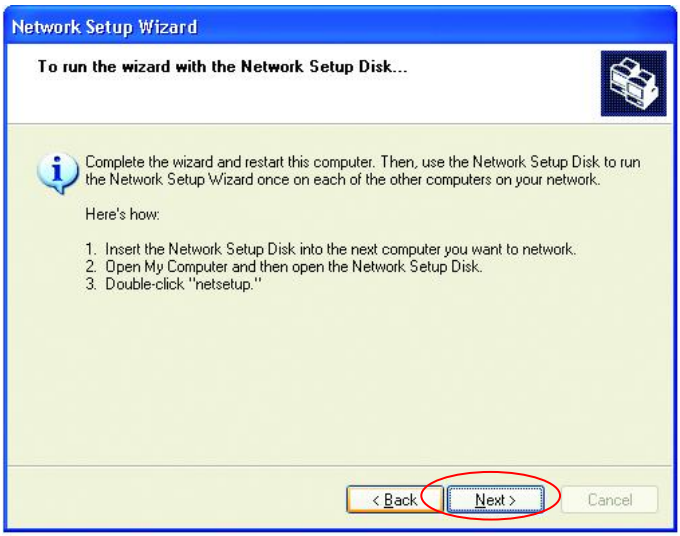


Format the disk if you wish, and Click **Next**.

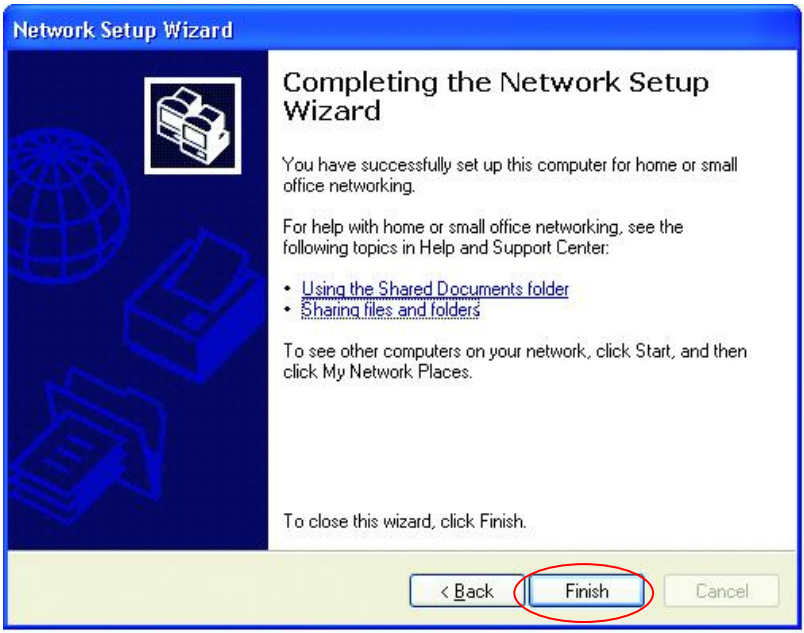
Please wait while the wizard copies the files.

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

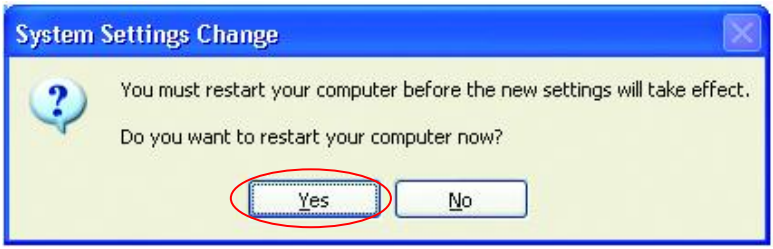
To continue Click **Next**



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



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



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

Naming your Computer

Naming your computer is optional. If you would like to name your computer please follow these directions:

In Windows XP:

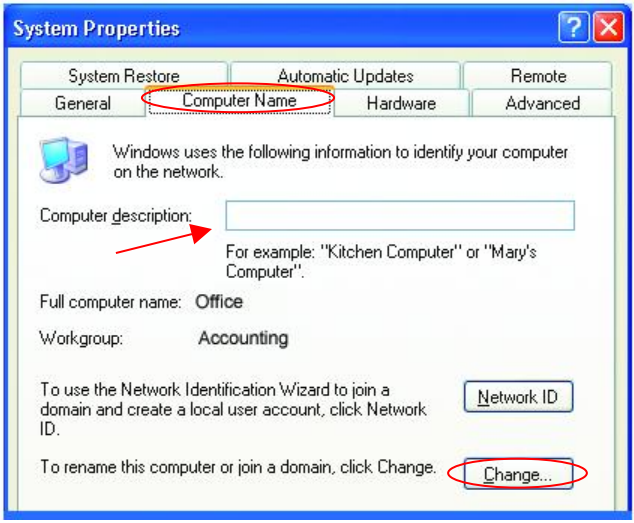
Click **START** (in the lower left corner of the screen)
Right-click on **My Computer**
Select **Properties**

- Select the **Computer Name Tab** in the **System Properties** window.

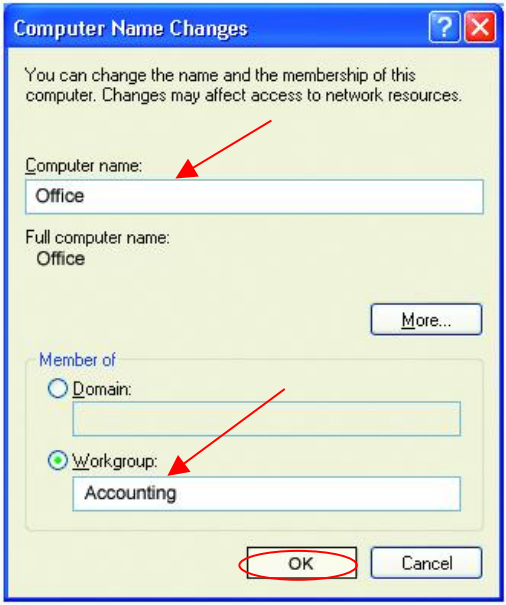
You may enter a Computer description if you wish, this field is optional.

To rename the computer and join a domain:

- Click **Change**



- 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**

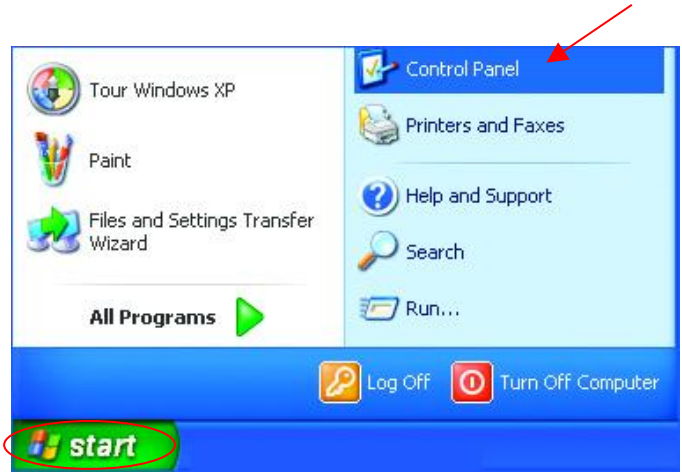


Assigning a Static IP Address

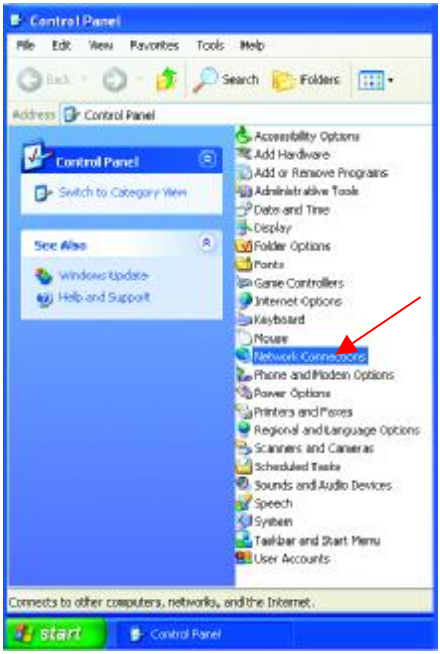
Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.

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

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

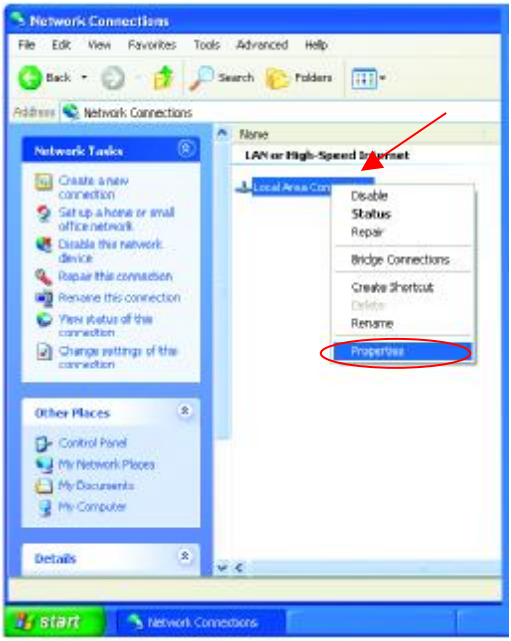


Double-click on
Network Connections



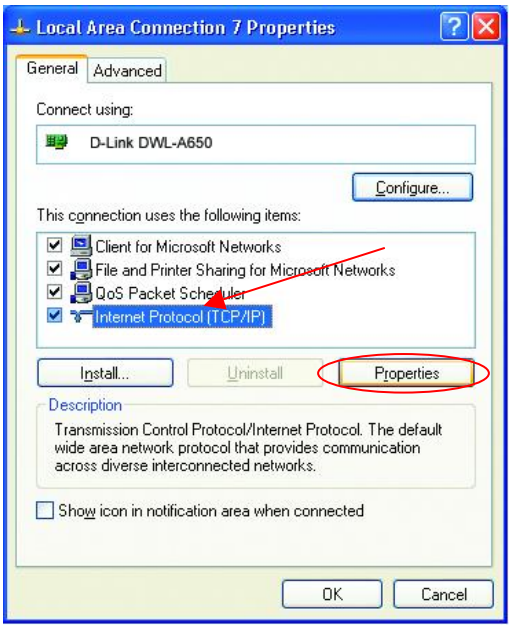
Right-click on **Local Area Connections**.

Double-click **Properties**



Highlight **Internet Protocol (TCP/IP)**

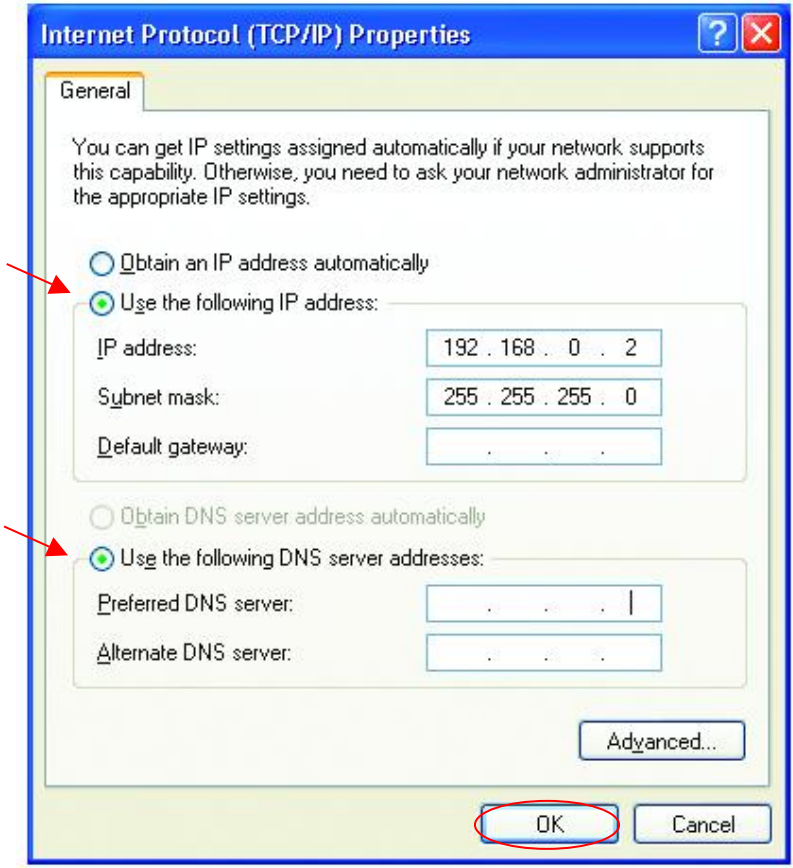
Click **Properties**



Select **Use the following IP address** in the Internet Protocol (TCP/IP) Properties window.

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

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



Click **OK**

You have completed the assignment of a Static IP Address. (You do not need to assign a Static IP Address if you have a DHCP-capable Gateway/Router.)

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:

(800) 758-5489

24 hours a day, seven days a week.

D-Link Technical Support over the Internet:

http://support.dlink.com

When contacting technical support, please provide the following information:

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

Limited Warranty and Registration

D-Link

1-Year

Limited Warranty

D-Link Systems, Inc. ("D-Link") provides this 1-Year warranty for its product only to the person or entity who originally purchased the product from:

- D-Link or its authorized reseller or distributor.
- Products purchased and delivered with the fifty United States, the District of Columbia, US Possessions or Protectorates, US Military Installations, addresses with an APO or FPO.

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

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

- Hardware (including 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 at no charge to the original owner. 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 of an identical make, model or part; D-Link may in its 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. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. 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 delivery of the Software for a period of ninety (90) days ("Warranty Period"), if 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. 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. The Warranty Period shall extend for an additional ninety (90) days after any replacement Software is delivered. 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.

What You Must Do For Warranty Service:
Registration is conducted via a link on our Web Site (http://www.dlink.com/). Each product purchased must be individually registered for warranty service within ninety (90) days after it is purchased and/or licensed.

FAILURE TO PROPERLY TO REGISTER MAY AFFECT THE WARRANTY FOR THIS PRODUCT.

Submitting A Claim. Any claim under this limited warranty must be submitted in writing before the end of the Warranty Period to an Authorized D-Link Service Office.

- The customer must submit 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.

- The customer is responsible for all shipping charges to and from D-Link (No CODs allowed). Products sent COD will become the property of D-Link Systems, Inc. Products should be fully insured by the customer and shipped to **D-Link Systems Inc., 53 Discovery Drive, Irvine CA 92618**.

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 that 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; and Any hardware, software, firmware or other products or services provided by anyone other than D-Link.

Disclaimer of Other Warranties: EXCEPT FOR THE 1-YEAR LIMITED WARRANTY SPECIFIED HEREIN, THE PRODUCT IS PROVIDED "AS-IS" WITHOUT ANY WARRANTY OF ANY KIND 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, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, 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.

GOVERNING LAW: This 1-Year Warranty shall be governed by the laws of the state of California. Some states do not allow exclusion or limitation of incidental or consequential damages, or limitations on how long an implied warranty lasts, so the foregoing limitations and exclusions may not apply. This limited warranty provides specific legal rights and the product owner may also have other rights which vary from state to state.

Trademarks

Copyright Statement

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 Your D-Link Product Online at http://www.dlink.com/sales/reg