

D-Link DFL-600

Firewall/VPN

Manual

Rev. 1.0

D-Link

Building Networks for People

Table of Contents

Introduction.....	4
IP Address Settings and Computer Settings	8
Introduction and Overview.....	9
Using the Configuration Utility	12
Setup Wizard	14
Home	20
LAN Settings.....	26
DHCP Settings	28
NAT.....	31
DMZ.....	32
Advanced Settings.....	38
Connecting PCs to the DFL-600 Router.....	74
Networking Basics	77
Contacting Technical Support.....	91
Limited Warranty and Registration	92

Package Contents



Contents of Package:

- D-Link DFL-600 Firewall/VPN Router
- Manual
- Quick Installation Guide
- Power Adapter, 5V DC, 2.5A*
- CAT-5 UTP Cable

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 5.5 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-600 Broadband VPN Router enables your network to connect to the Internet via a secure, private connection using a Cable or DSL modem. The Virtual Private Network (VPN) that is created on the Internet between your home and a VPN server in your office is secure from interference when you use the DFL-600.

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 secure “connected” environment.

Connect the WAN port on the DFL-600 to the Cable/DSL modem using an Ethernet cable. Your entire LAN can now access the Internet using just one Internet account. The DFL-600 has 3 LAN ports, one DMZ port, and one WAN port. That means that 3 computers can share the benefits of the DFL-600-equipped network and 1 computer can be configured as a server for Internet applications that may conflict with the advanced protection from intrusion offered by your new DFL-600.

For the price of one Internet account, the DHCP-capable DFL-600 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-600, 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-600 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-600.

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 2.5A 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. The DMZ feature can be disabled.
Reset	To reload the factory default settings, press the reset button. Pressing the Reset button will clear the current configuration as reset the DFL-600 to the factory default settings.

Product Features

VPN

Provides Virtual Private Networking when communicating with a VPN server-equipped office, or with another DFL-600-equipped network. Supports IPSEC, PPTP, L2TP, and VPN pass through.

DSL/Cable Modem support

The DFL-600 can connect any Cable or DSL modem to the network.

DHCP

The DFL-600 is a DHCP-capable router. It automatically assigns unique IP Addresses to each network users that is connected to the DFL-600, 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 a 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-600 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-600 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-600 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-600 routes packets between these two subnets and the Internet (or the network connected to the DFL-600'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 – LAN. 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 192.168.0.2 to 192.168.0.254. So computers and other devices connected to these three ports either allow the DFL-600'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-600 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. In addition, you must specify the port number 8081. So, you must enter <http://192.168.0.1:8081> in the address field of your web-browser to access the DFL-600's web-based configuration manager.

The 192.168.1.0 network – DMZ. The port labeled – **DMZ** on both the front and rear panel – is, by default, assigned the IP address range between 192.168.1.2 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-600 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 you can 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 to have 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-600. Computers and devices connected to the **DMZ** port will not have the level of protection that the **LAN** ports can provide, however. It is recommended that computers and devices connected to the DFL-600'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-600 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-600.

It can be useful when configuring your DFL-600 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-600 is either obtained automatically from your ISP (or other network device on the WAN side) or is entered manually. The DFL-600 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, or when the DFL-600 is rebooted.

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

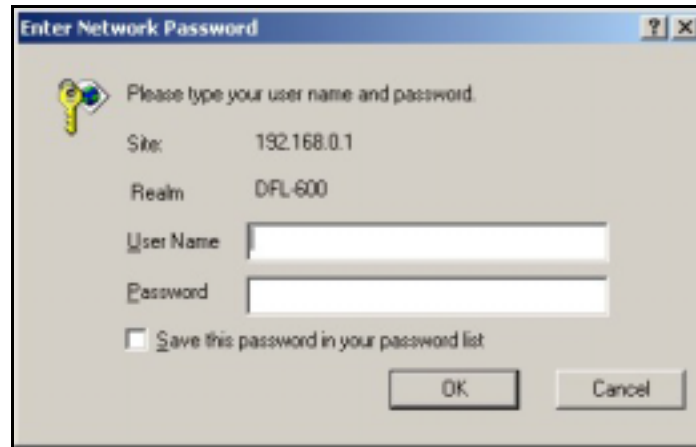
The **Device IP Settings** dialog box allows you to specify the IP address that computers on your LAN will use to access the DFL-600's web-based configuration utility. The default is 192.168.0.1 with a subnet mask of 255.255.255.0. If it becomes necessary to change this IP address, be sure to use an 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-600 from your LAN.

The many other features of the DFL-600 are described in subsequent sections.

Using the Configuration Utility

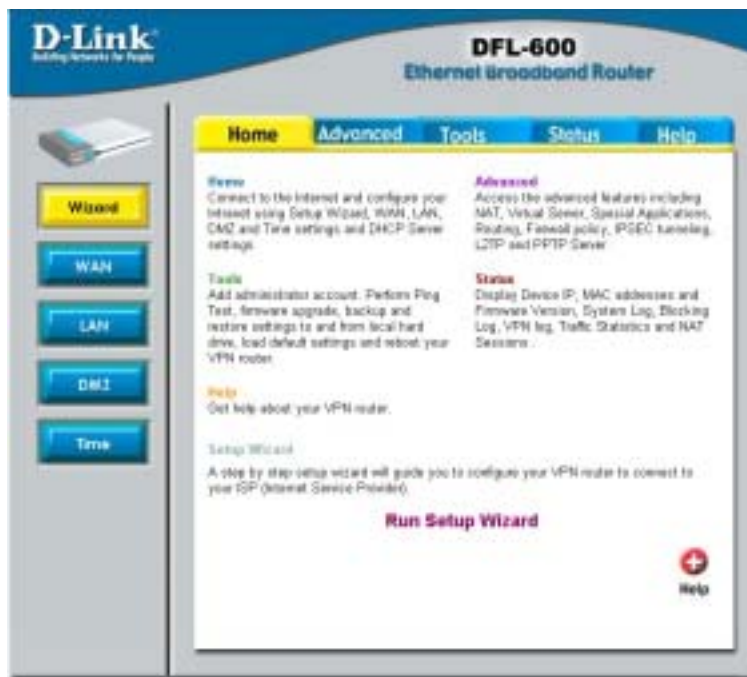
Launch your web browser and type the device IP address and port number (http:// 192.168.0.1:8081) in the browser's address box. This is the default IP address of your DFL-600. Press Enter.

The following dialog-box will appear to prompt you to enter the DFL-600's default User Name and Password. The DFL-600's default User Name is **admin** and the default Password is also **admin** – all lower case.



Click **OK** to open the **Home** menu.

Note: Please make sure that the computer you will use to connect to and configure the DFL-600 is assigned an IP address that is in the same range as the DFL-600. The IP address of the DFL-600 is 192.168.0.1. All computers on your network must be within that range, for instance, the computer IP address could be any IP address from the range 192.168.0.2 to 192.168.0.254, with a subnet mask of 255.255.255.0.



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.

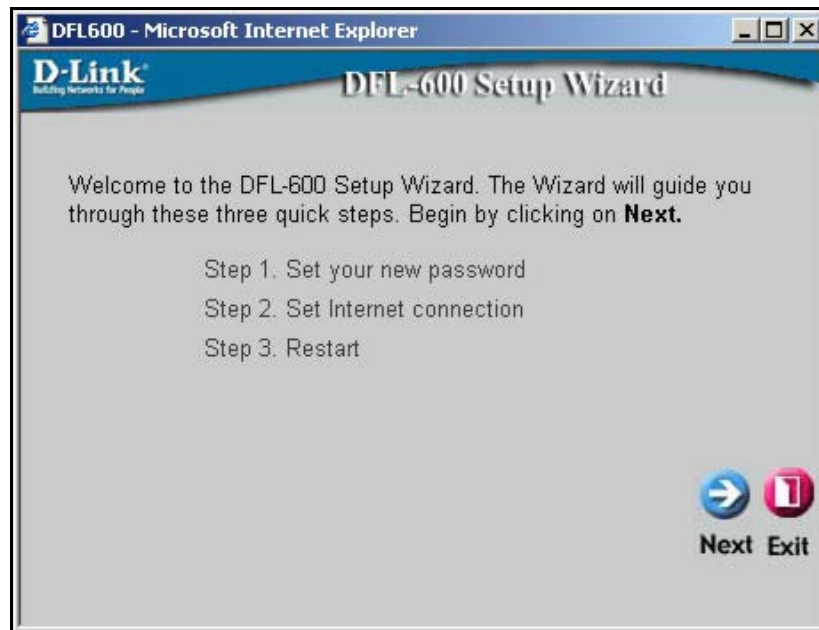
All other setup tasks can be accomplished using the configuration utility from your web browser.

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-600. All other configuration tasks can be accomplished through the web-based manager.

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



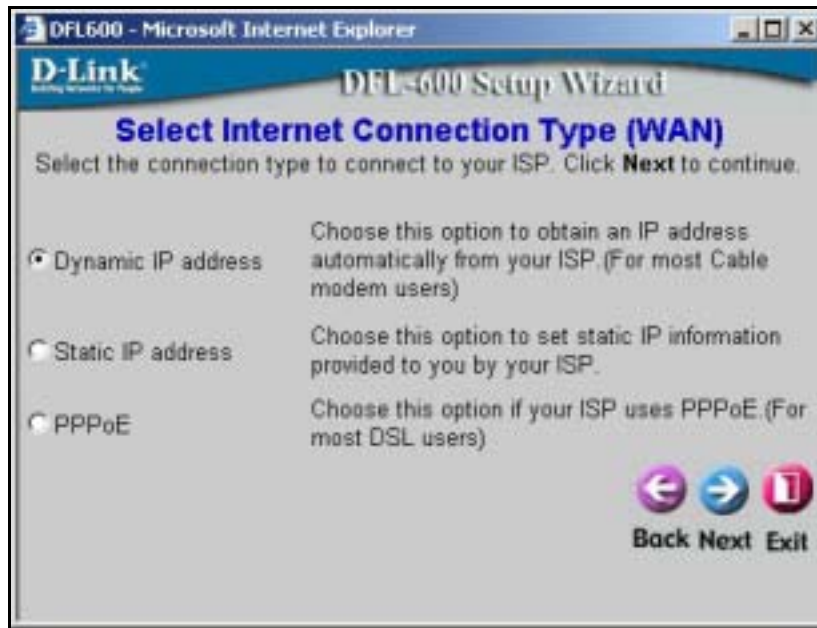
Click **Next** to continue.



Enter a password in the **Password** field, and again in the **Verify Password** field. This will become the logon password for the DFL-600. This password is case-sensitive, so remember to use capital letters when logging on to the DFL-600's web-based manager – if you enter a password with capital letters here. The user name, **admin**, will not be changed here.

***Note:** If you choose to input a password, please remember it. If you lose your password, you will have to manually reset the unit (using the **reset** button on the rear panel of the unit). Resetting the DFL-600 will return all configuration parameters to their factory default values, so all of your settings will be lost and will need to be entered again. The default Username is **admin** with a password that is also **admin**.*

Click **Next** to continue.



This menu allows you to select the type of connection your ISP provides. Many ISPs use the **PPPoE** (Point-to-Point Protocol over Ethernet) for DSL connections, while many 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). DHCP is referred to as **Dynamic IP address** on the DFL-600. 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.

The **Static IP address** click-box is used to enter a permanent IP address that is assigned by your ISP. If your ISP assigns you a permanent IP address, choose this option.

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:



The image shows a screenshot of the D-Link DFL-600 Setup Wizard. The title bar at the top says "D-Link Building Networks the Simple Way". Below that, the window title is "DFL-600 Setup Wizard". The main heading is "Set Static IP address" in blue. Below the heading, there is a instruction: "Enter in the static IP information provided to you by your ISP. Click **Next** to continue." There are five input fields, each with a label and a text box containing "0.0.0.0":

- WAN IP address
- WAN Subnet Mask
- WAN Default Gateway
- Primary DNS Server
- Secondary DNS Server

To the right of the "Secondary DNS Server" field is a checkbox labeled "(Option Disable)". At the bottom right, there are three circular buttons: a left arrow (labeled "Back"), a right arrow (labeled "Next"), and a red square with a white 'X' (labeled "Exit").

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:

DFL600 - Microsoft Internet Explorer

D-Link
Building Networks To People

DFL600 Setup Wizard

Set PPPoE

The service name is optional but may be required by your ISP. Click **Next** to continue.

User Name

Password

Confirm Password

Service Name (optional)

Back Next Exit

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.

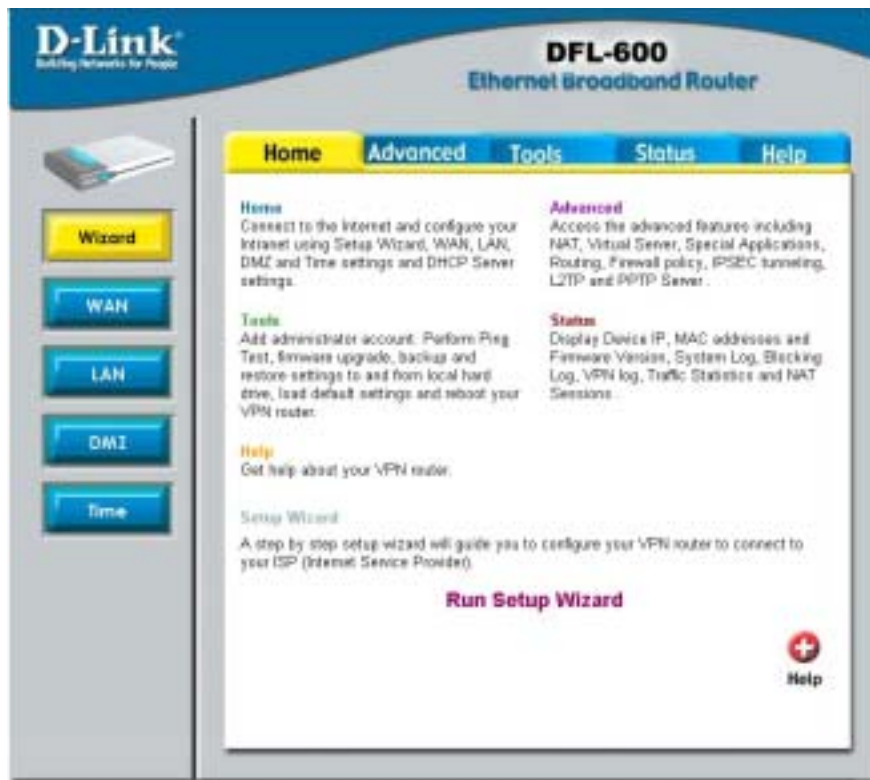
Click **Next** to continue.



You have completed the basic setup Wizard. The configuration now needs to be entered into the DFL-600's flash RAM. Clicking **Restart** will save the configuration and restart the router.

Home

The **Home** menu contains links to all of the setup menus for the DFL-600.



Click on the **WAN** button:

WAN Settings

The **WAN Settings** menu allows you to view the current configuration for your DFL-600, and to choose the protocol by which your DFL-600 will receive its WAN network settings.



The settings listed under **WAN Settings** are the network settings currently in use by the DFL-600. The fields where you will enter the WAN Settings will change depending upon the choice you make in the **IP Settings Mode** drop-down menu. These settings are described below.

IP Settings Mode	<p>This drop-down menu determines how the DFL-600 will obtain its IP address information. The fields where you will enter the information will change, as appropriate, to reflect the mode you have selected. The page shown above is in Dynamic mode.</p> <p>Dynamic allows the DFL-600 to get its IP address information from your ISP using the Dynamic Host Configuration Protocol (DHCP). Use this setting if your ISP instructs you to use DHCP or to automatically obtain an IP address. A server on your ISP's network will then automatically send the necessary IP address information to your DFL-600.</p> <p>Static allows you to manually enter the necessary IP address information. Use this setting if your ISP has permanently assigned an IP address to your connection.</p> <p>PPPoE allows you to enter a Username and Password for a Point-to-Point Protocol over Ethernet (PPPoE) internet connection. Use this setting if your ISP has provided you with an ADSL modem that operates in Bridge mode.</p>
IP Address	<p>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.</p>
Subnet Mask	<p>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-600.</p>
Default Gateway	<p>This is the IP address of a device at your ISP's</p>

	office where packets destined for the Internet – from your home network – are sent, before being forwarded to their final destination. For the DFL-600, 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-600.
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 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-600 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.

WAN Settings

IP settings Mode: Dynamic

DHCP Client Status: Stop

IP address: 0.0.0.0

Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Buttons: Apply Refresh Cancel Help

Buttons: ReNew Release

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:

WAN Settings

IP settings Mode: Static

IP address: 10.54.24.50

Subnet Mask: 255.0.0.0

Default Gateway: 10.254.254.251

Primary DNS Server: 168.95.1.1

Secondary DNS Server: 168.95.1.2 ☐ (Option Disable)

Buttons: Apply Cancel Help

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:

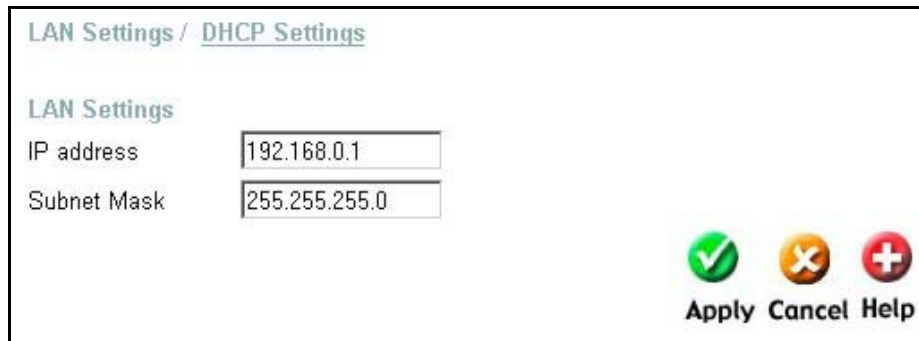
The screenshot shows a 'WAN Settings' window. At the top, 'IP settings Mode' is set to 'PPPoE'. Below this, there are input fields for 'User Name' (containing '84106647@hinet.n'), 'Password' (masked with asterisks), 'Service Name' (optional), 'Host Name' (optional), 'Idle Timeout(sec)' (300), and 'MTU(1000~1492)' (1492). A checkbox for 'Connected On Demand' is checked and labeled 'Enable'. To the right of these fields are four icons: a green checkmark, a purple refresh arrow, an orange 'X', and a red plus sign, with labels 'Apply', 'Refresh', 'Cancel', and 'Help' respectively. Below the settings, the 'PPPoE Status' is 'Disconnected'. A list of network parameters follows: 'IP address' (0.0.0.0), 'Subnet Mask' (0.0.0.0), 'Default Gateway' (0.0.0.0), 'Primary DNS Server' (0.0.0.0), 'Secondary DNS Server' (0.0.0.0), and 'Trigger Packet Header'. At the bottom are 'Connect' and 'Disconnect' buttons.

Field	Value	Notes
IP settings Mode	PPPoE	
User Name	84106647@hinet.n	
Password	[Masked]	
Service Name		(optional)
Host Name		(optional)
Idle Timeout(sec)	300	
MTU(1000~1492)	1492	
Connected On Demand	<input checked="" type="checkbox"/> Enable	
PPPoE Status	Disconnected	
IP address	0.0.0.0	
Subnet Mask	0.0.0.0	
Default Gateway	0.0.0.0	
Primary DNS Server	0.0.0.0	
Secondary DNS Server	0.0.0.0	
Trigger Packet Header		

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.

LAN Settings

The **LAN Settings** allows you to view the current IP address and subnet mask assigned to the DFL-600. It also allows you to change these settings.



LAN Settings / DHCP Settings

LAN Settings

IP address 192.168.0.1

Subnet Mask 255.255.255.0

Apply Cancel Help

If it is necessary to change the **IP Address** or **Subnet Mask** assigned to the DFL-600, 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-600 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-600 from any of these computers. In order to re-establish the connection between a computer on the LAN side and the DFL-600, 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-600. As an alternative, you can configure the DFL-600's DHCP server to give IP addresses from the new IP address range that you will give the DFL-600 here.*

As an example, if your LAN network is to be a 192.168.0.x network with a subnet mask of 255.255.255.0, you might assign the DFL-600 an IP address of 192.168.0.1 and configure the DFL-600's DHCP server to assign addresses in the range between 192.168.0.2 to 192.168.0.100. The default gateway setting for computers on the LAN side will be the DFL-600's IP address – in this case, 192.168.0.1.

Saving all of this information to the DFL-600's flash RAM and restarting the router will make this IP addressing scheme current. When you enable DHCP

(in Windows, “**obtain an IP address automatically**”) and restart the computers connected to the LAN side of the DFL-600, they will automatically be assigned IP addresses from the range 192.168.0.2 to 192.168.0.100.

As an alternative, you could disable the DHCP server on the DFL-600 and manually update the IP address, subnet mask and default gateway information for each computer on the LAN side of the DFL-600.

It is recommended that if you need to change the IP addressing scheme for the DFL-600, that you configure the DFL-600'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-600. That way, a computer on the LAN side of your network can always get the proper network addressing information by DHCP from the DFL-600 simply by being restarted.

DHCP Settings

DHCP (Dynamic Host Configuration Protocol) is a method of automatically assigning IP addresses, subnet masks, default gateway and DNS server IP address to computers on the LAN side of the DFL-600. The DFL-600 can be a DHCP server for your LAN, assigning IP addresses, etc. to computers on your network from a range of addresses you specify below.

LAN Settings / DHCP Settings

DHCP Server

DHCP Server Status ☒ Enable ☐ Disable

Starting IP address

Ending IP address





Lease Time (sec)

Auto Configuration ☒ Enable ☐ Disable

Domain Name

Primary DNS Server

Secondary DNS Server ☐ (Option Disable)

Apply Refresh Cancel Help

DHCP Client Table

Total No. of Entries: 4 / 99

Host Name	IP address	MAC Address	Expire
-----------	------------	-------------	--------

DHCP Server Status	This allows you to Enable or Disable the DHCP Server feature on the DFL-600. The default is Enabled .
Starting IP Address	This is the first IP address in a range that the DFL-600 will assign to a computer on your network. This IP address can not be the same as the IP address assigned to the DFL-600, nor can the IP address assigned to the DFL-600 be contained in the range of IP addresses available for the DFL-600 to assign. In this case, the IP address of the DFL-600 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, but in the DFL-600's default IP addressing scheme, the range is from 192.168.0.0 to 192.168.0.255. Please note that the addresses ending in 0 and 255 are reserved for other uses, so the effective IP address range is 192.168.0.1 to 192.168.0.254. The DFL-600's default IP address is 192.168.0.1.
Ending IP Address	This is the last IP address in a range that the DFL-600 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-600 can assign to the computers on your network.
Lease Time	This is the length of time any computer on your network that is assigned network settings by the DFL-600 – 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 3600 seconds.
Auto Configuration	This field allows you to specify whether or not the DFL-600 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 automatically from your ISP by the DFL-600, and will then be 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	The DFL-600 can provide a domain name 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.
Primary DNS Server	This is the IP address of a server on the Internet that provides the service of changing text URLs into IP address for sites on the Internet. The IP address of this server is provided by your ISP.
Secondary DNS Server	This is 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-600. 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 – assigned by your ISP – usable on the Internet to a *local* IP address – assigned by you – usable on your private network (but not on the Internet.)

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 computers behind one IP address. The NAT function will normally only allow incoming packets that are generated in response to a request from a computer on the LAN.

NAT is automatically applied between the IP addresses assigned to the DFL-600's WAN port (the IP address or addresses assigned to you by your ISP) and the IP addresses assigned to the DFL-600'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.

DMZ

NAT and the firewall features of your DFL-600 may conflict with certain interactive applications such as video conferencing or playing Internet video games. For these applications, a 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, and that computer 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 Settings

The **DMZ Settings** screen allows you to **Enable** and **Disable** the DMZ port on the DFL-600 and to specify the IP address and Subnet Mask that the DMZ port will use. The default DMZ IP address is 192.168.1.1 with a subnet mask of 255.255.255.0.



Global Address	This is the DMZ Global Address assigned to the DFL-600 by your Network Administrator. Every DMZ connection will go through this global address to access the DMZ internal computer.
IP Address	This is the Global IP address assigned to the DFL-600 by your 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-600's **DMZ** port.

DMZ Hosts, sometimes referred to as **Virtual Servers**, are computers on your 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 Settings / DMZ Host

Add DMZ Host

Private IP address: 192.168.1.2

Transport Type: TCP

Protocol: -user defined-

Port Number: 1

Apply Cancel Help

Total No. of Entries: 0 / 8

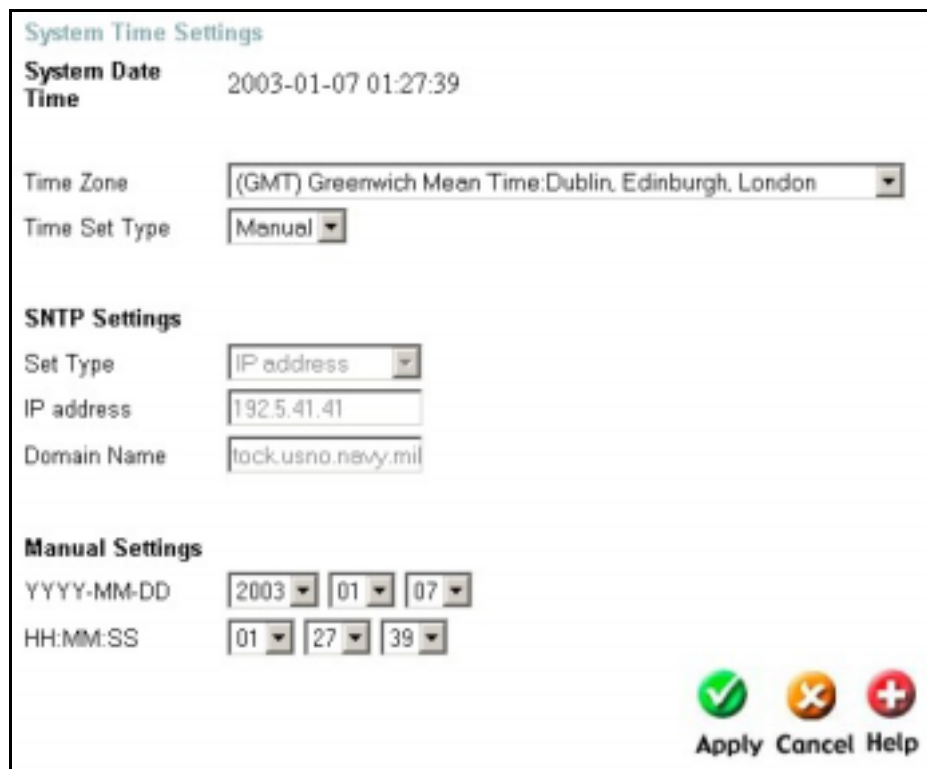
Private IP address	Protocol Type	Port Number	Delete
--------------------	---------------	-------------	--------

Private IP address	This is the IP address you have assigned to your DMZ computer. You will need to manually configure the IP address settings for each computer you connect to the DFL-600's DMZ port. It must be from the same IP address range as you assigned to the DMZ port. The DFL-600's default IP address range for the DMZ port is 192.168.1.2 to 192.168.1.254.
Transport Type	This drop-down menu allows you to specify whether the TCP or UDP protocol will be used by the application on the DMZ computer.
Protocol	This drop-down menu allows you to specify the

	<p>protocol that the application on the DMZ computer will use. ~user defined~ allows you to manually enter the TCP or UDP port number that the application will use to connect to the Internet. The remaining protocols in the list have the appropriate TCP or UDP port number already entered. These are the most commonly used protocols in use by applications. For example, the SMTP (Simple Mail Transfer Protocol) is commonly used by e-mail programs. smtp uses TCP port 25.</p> <p>You can make multiple protocol entries for a single DMZ computer.</p>
Port Number	This allows you to enter the TCP or UDP port number manually, when the ~user defined~ protocol option is used.

Time Settings

The DFL-600 can be set to obtain and distribute the correct time to computers on your LAN using the Simple Network Time Protocol (SNTP). Click on the Time button to open the following page:



System Time Settings

System Date Time 2003-01-07 01:27:39

Time Zone (GMT) Greenwich Mean Time: Dublin, Edinburgh, London

Time Set Type Manual

SNTP Settings

Set Type IP address

IP address 192.5.41.41

Domain Name tock.usno.navy.mil

Manual Settings

YYYY-MM-DD 2003 01 07

HH:MM:SS 01 27 39

Apply Cancel Help

System Date Time	Displays the current system date and time.
Time Zone	This drop-down menu allows you to select the time zone in which your DFL-600 is located.
Time Set Type	This drop-down menu allows you to specify the method the DFL-600 will use to obtain the date and time. Manual allows you to manually enter the date and time. SNTP allows the DFL-600 to obtain the date and time automatically from an SNTP server, as specified below.

Set Type	This drop-down menu allows you to select either the IP address of an SNTP server, or the Domain Name (URL) of an SNTP server that the DFL-600 will contact to obtain the correct date and time.
IP address	Enter the IP address of an SNTP server here.
Domain Name	Enter the Domain Name (URL) of an SNTP server here.
YYYY-MM-DD	These fields allow you to manually enter the date using a year-month-day format.
HH:MM:SS	These fields allow you to manually enter the time using an hour: minute: second format.

Advanced Settings

NAT

Network Address Translation

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 – assigned by your ISP – usable on the Internet to a *local* IP address – assigned by you – usable on your private network (but not on the Internet.)

Virtual Servers

Virtual Servers allow remote users to access services on your LAN such as FTP for file transfers or SMTP and POP3 for e-mail. The DFL-600 will accept remote requests for these services at a Global IP Address you specify, using the specified 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 that the Global IP Address must be within the range specified on the NAT Settings page, and that the Private IP Address must be within the range specified for your LAN.

Virtual Server / Application(ALG)

Add Virtual Server Mapping

Private IP address

0.0.0.0

Transport Type



TCP

Protocol

-user defined-

Port Number

1

Apply Cancel Help

Total No. of Entries: 0 / 8

Private IP address	Protocol Type	Port Number	Delete
--------------------	---------------	-------------	--------

Private IP	This is the IP address of the server on your LAN that will provide the service to remote users.
Transport Type	You can select the transport 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.
Protocol	<p>You can select from a list of commonly used protocols from this drop-down menu. This is the equivalent of entering the correct Transport Type (TCP or UDP) and the correct port number corresponding to a given protocol. The difference here is that the protocol is identified by name.</p> <p>For example, the Simple Mail Transfer Protocol (SMTP in the drop-down menu) is used to send and receive e-mail. It uses the TCP transport protocol and port number 25. This information will be entered for you, if you select SMTP from the Protocol drop-down menu.</p>
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.

Application Gateway (ALG)

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-600 to allow computers on your LAN to access servers on the WAN that require multiple TCP or UDP connections.

Virtual Server / Application(ALG)

Add /Edit Special Application Settings

Application Name:

Trigger Port Range: -

Trigger Type:

Max Activity Interval: (50-30000ms)




Session Chained:

Address Replacement:

Replacement Format:



☒ Allow sessions initiated from/to the 3rd host

Popular Application:

Apply Cancel Help

Total No. of Entries: 1 / 16

Application Name	Port	View	Delete
netmeeting	1720-1720		

Application Name	This is a reference – usually the name of the application. In the above example, Netmeeting is the application, and this is used to name this entry.
Trigger Port Range	This is the TCP or UDP port range 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.
Max Activity Interval	This is the maximum interval, in milliseconds, between the triggering of a protocol session and the protocol's dynamic session.
Session Chained	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 Chained 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-600, the IP address in this packet will be translated between the WAN and LAN side of the DFL-600, if this option is enabled.
Replacement Format	This drop-down menu allows you to specify either the TCP or UDP protocol for the Address Replacement function above.
Allow sessions initiated from/to 3rd host	Click this check box 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 pre-entered into the DFL-600's firmware and can be selected here from the drop-

	<p>down menu. Selecting one of the listed applications is the equivalent of entering the correct settings in the fields above for the specific application. For example, the Netmeeting application requires a Trigger Port Range of 1720 – 1720, a Trigger Type of TCP, and so on. The correct settings for the applications listed in this drop-down menu have been entered into the DFL-600's firmware, for your convenience.</p>
--	---

Static Routing

Your DFL-600 can automatically discover routes to destinations on both your LAN and the WAN (Internet). In addition, you can add entries to the DFL-600's routing table that will be saved to flash RAM. These routes will not age out, and are therefore static.

Static Routing

Add/Edit Static Routing IP

Destination IP Address

0.0.0.0

Subnet Mask

0.0.0.0

Gateway IP address

0.0.0.0

✓

✗

+

Apply

Cancel

Help

Total No. of Static Route Entries: 0 / 8

Destination IP address	Subnet Mask	Gateway IP address	Delete
Page			

The Default and Local Route Entries:

Destination IP address	Subnet Mask	Gateway IP address	Delete
192.168.1.0	255.255.255.0	0.0.0.0	
192.168.0.0	255.255.255.0	0.0.0.0	
10.0.0.0	255.0.0.0	0.0.0.0	
default	0.0.0.0	10.254.254.251	

Destination IP Network	This is the IP address of the remote network that the DFL-600 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-600 and servers on the remote network.

Policy (Firewall Settings)

The DFL-600 allows you to specify a range of IP addresses, MAC addresses, TCP/UDP port numbers, and Domain names for connections between computers on the WAN and computers on your LAN that will be controlled. These IP addresses are entered on the pages under the **Policy** tab.

The default firewall port filter rules on the DFL-600 are:

- Allow all outbound packets to pass through the router to the WAN (Internet).
- Allow inbound packets only for a virtual server on your LAN running the FTP, SSH, TELNET, SMTP, POP3, or LDAP protocols.
- Deny remote access to the DFL-600 from the WAN (Internet)




Policy Rules / [Port Filter](#) / [IP Range Filter](#) / [MAC Filter](#) / [Domain Filter](#)

Port Filter Status (Inbound/Outbound)

IP Range Filter Status (Outbound)

MAC Filter Status (Outbound)

Domain Filter Status (Outbound)




 Apply Cancel Help

Port Filter Status	When Enable is selected from this drop-down menu, the Port Filter will be applied to packets both coming from and going to the WAN. When Disable is selected, the Port Filter is inactive.
IP Range Filter Status	When Enable is selected from this drop-down menu, the IP Filter will be applied to packets going to the WAN. When Disable is selected, the IP Filter is inactive.
MAC Filter Status	When Enable is selected from this drop-down menu, the MAC Filter will be applied to packets going to the WAN. When Disable is selected, the MAC Filter is inactive.
Domain Filter Status	When Enable is selected from this drop-down menu, the Domain Filter will be applied to packets going to the WAN. When Disable is selected, the Domain Filter is inactive.

Firewall Settings – Port Filter Policy

The DFL-600 allows you to specify a range of TCP or UDP ports for connections between computers on the WAN and computers on your LAN that will be controlled. These TCP or UDP ports are entered on the **Port Filter** page.

The screenshot shows the 'Port Filter' configuration page. At the top, there are tabs for 'Policy Rules', 'Port Filter', 'IP Range Filter', 'MAC Filter', and 'Domain Filter'. Below the tabs is the 'Add Port Filter Rules' section. It contains four fields: 'Transport Type' (set to 'TCP'), 'Protocol' (set to '-user defined-'), 'Port Range' (set to '1 - 1'), and 'Direction' (set to 'Inbound'). To the right of these fields are three buttons: a green checkmark for 'Apply', an orange 'X' for 'Cancel', and a red plus sign for 'Help'. Below the buttons, it says 'Total No. of Entries: 19 / 60'. At the bottom, there is a table with four columns: 'Transport Type', 'Port Range', 'Direction', and 'Delete'. The table lists 19 entries, including TCP ports 5190-5190, UDP ports for SNMP Trap(162), SNMP(161), TFTP(69), DNS(53), LDAP(389), Finger(79), SSH(22), ICMP, and POP3(110).

Transport Type	Port Range	Direction	Delete
TCP	5190 - 5190	Outbound	
UDP	SNMP Trap(162)	Inbound	
UDP	SNMP(161)	Inbound	
UDP	TFTP(69)	Inbound	
UDP	DNS(53)	Inbound	
TCP	LDAP(389)	Inbound	
TCP	Finger(79)	Inbound	
TCP	SSH(22)	Inbound	
ICMP	-	Inbound	
TCP	POP3(110)	Inbound	

Transport Type	This drop-down menu allows you to specify the transport protocol that will be filtered by the DFL-600. You can choose from the TCP, UDP, ICMP, IGMP, GRE, AH, ESP, and ICOMP protocols.
Protocol	You can select from a list of commonly used protocols from this drop-down menu. This is the equivalent of entering the correct Transport Type and the correct port number corresponding to a given protocol. The difference here is that

	<p>the protocol is identified by name.</p> <p>For example, the Simple Mail Transfer Protocol (SMTP in the drop-down menu) is used to send and receive e-mail. It uses the TCP transport protocol and port number 25. This information will be entered for you, if you select SMTP from the Protocol drop-down menu.</p>
Port Range	<p>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.</p>
Direction	<p>This allows you to specify the source of network traffic for which the current policy entry will be applied – from the Internet (Inbound), or from your LAN (Outbound).</p>

IP Range Filter

The **IP Range Filter** page allows you to deny access to the WAN (Internet) from specific computers on your LAN, by specifying the computer's IP address on the WAN (Internet).



Policy Rules / Port Filter / IP Range Filter / MAC Filter / Domain Filter

Add IP Range Port Filter

LAN IP Range 192.168.208.1 - 192.168.208.254

Source IP From

Source IP To

Apply Cancel Help

Total No. of Entries: 0 / 20

Source IP From	Source IP To	Destination Port Filter	Delete
----------------	--------------	-------------------------	--------

Source IP Address From	This allows you to specify the first in a range of IP addresses 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.
Source IP Address To	This allows you to specify the last in a range of IP addresses 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.

IPSec Settings

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.



IPSec Pass-through	Click Enable to allow IPSec packets to pass through the router to the destination computer on your LAN. When IPSec Pass-through is enabled, the DFL-600 will allow IPSec packets to reach their destination computer on your LAN.
IPSec Status	Click Enable to make the IPSec settings active.

IPSEC Tunnel Mode

The IPSEC Tunnel Mode page allows you to setup a secure tunnel between your DFL-600 and a remote gateway.

[IPSec Settings](#) / [Tunnel Settings](#) / [Tunnel Table](#) / [IPSec Status](#)

Add/New Tunnel

Tunnel ID:

Termination IP:

Shared Key:

Tunnel Type:

Phase 1 Proposal

Mode: ☒ Main ☐ Aggressive

DH Group:

IKE Life Duration: seconds

IKE Hash:

IKE Encryption:

Phase 2 Proposal

PFS Mode:

IPSec Operation:

IPSec Life Duration: seconds

ESP Transform:

ESP Auth:




AH Transform:

Target Host Range

Type:

Starting Target Host:

Subnet Mask:

Apply Cancel Help

Add/New Tunnel	The following fields will identify the VPN tunnel on the DFL-600.
Tunnel ID	An alphanumeric string that identifies the remote tunnel. A sting of up to 63 characters

	can be entered. The Tunnel ID is sometimes called the Negotiation ID of the remote gateway.
Termination IP	The IP address of the remote gateway.
Shared Key	The encryption key that should be entered exactly the same way on both endpoints in order to establish Phase 1 negotiation.
Tunnel Type	This drop-down menu allows you to select the type of VPN Tunnel you are configuring. You can choose between Public , Private , and Manual . At the time of the writing of this manual, only Public IPSec VPN tunnels are supported.
Phase 1 Proposal	Phase 1 VPN IPSec negotiation allows the two endpoints of a VPN tunnel to communicate in a secure way so that the encryption for the actual VPN tunnel can be accomplished in the Phase 2 negotiation. The following fields will define the way the encryption and decryption of the Phase 1 negotiation is handled.
Mode	You can select between Main and Aggressive modes for the Phase 1 negotiation to establish a VPN IPSec tunnel. In the Main mode, all communication between the two endpoints of an IPSec VPN tunnel are encrypted. In Aggressive mode, there is no encryption in the Phase 1 negotiation.
DH Group	The DH algorithm allows the DFL-600 to generate secret keys for encryption for the Phase 1 negotiation. Group 1 generates a 768-bit key and Group 2 generates a 1024-bit key. The same DH Group must be used on both ends of an IPSec VPN tunnel.
IKE Life Duration	This is the duration (in seconds) the phase 1 key after the tunnel is established. When this duration has past, the two peers will trigger a restart of the phase 1 negotiation to set up a new phase 1 key. Phase 2 negotiation will also be

	triggered to build a new tunnel.
IKE Hash	This drop-down menu allows you to select the algorithm that will be used to ensure that the messages exchanged between the two IPsec VPN tunnel endpoints has been received exactly as it was sent. In other words, a Hash algorithm is used to generate a binary number by a mathematical operation using the entire message. The resulting number is called a message digest. The very same mathematical operation is performed when the message is received, and if there has been any change in the message in transit, the resulting message digest number will be different and the message will be rejected. You can choose between MD5 – a 128-bit message digest, and SHA – which generates a 160-bit message digest. You must have exactly the same IKE Hash algorithm on both ends of a VPN tunnel.
IKE Encryption	This drop-down menu allows you to select the encryption algorithm that will be used to encrypt the messages passed between the VPN tunnel endpoints during the Phase 1 negotiation. You can choose between DES and 3DES encryption methods. The key length for the 3DES algorithm is three times as long as the DES key, and is therefore more likely to be secure. You must choose exactly the same IKE Encryption algorithm on both ends of a VPN tunnel.
Phase 2 Proposal	The following entries will establish the setup for the negotiation between the two endpoints for the encryption of messages once the VPN tunnel has been initiated.
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 , Group 1 , and Group 2 . Group 1



	uses 768-bit encryption, and Group 2 uses 1024-bit encryption. You must use exactly the same PFS encryption mode on both ends of the VPN tunnel.
IPSec Operation	<p>This drop-down menu allows you to select the level of encryption that will be applied to packets that are sent between the two endpoints of a VPN tunnel.</p> <p>ESP – specifies that the entire packet will be encrypted (by the DES or 3DES algorithm, as selected below) and authenticated (by the MD5 or SHA algorithm, as selected below).</p> <p>AH – specifies that only the authentication algorithm (MD5 or SHA, as selected below) will be used. When AH is selected, the data portion of packets sent between the two endpoints of a VPN tunnel will not be encrypted.</p>
IPSec Life Duration	This is similar to the IKE Life Duration, described above. It is the duration, in seconds, of the phase 2 key, after the tunnel is established. When this time has past, the two peers will trigger the phase 2 negotiation to set up a new phase 2 key and rebuild the tunnel.
ESP Transform	<p>This drop-down menu allows you to select the encryption algorithm that will be used when ESP is selected in the IPSec Operation drop-down menu above.</p> <p>You can choose between Null – no encryption, DES – using DES encryption, and 3DES – using triple DES encryption.</p> <p>You must select the exact same ESP transform (encryption algorithm) on both ends of a VPN tunnel.</p>
ESP Auth	This drop-down menu allows you to select the

	<p>encryption algorithm that will be used when ESP is selected in the IPSec Operation drop-down menu above.</p> <p>You can choose between Null – no authorization, MD5 – using MD5 message digest authentication, and SHA – using the SHA authentication method.</p> <p>You must select the exact same ESP authentication method on both ends of a VPN tunnel.</p>
AH Transform	<p>This drop-down menu allows you to select the encryption algorithm that will be used when AH is selected in the IPSec Operation drop-down menu above.</p> <p>You can choose between MD5 – using MD5 message digest authentication, and SHA – using the SHA authentication method.</p> <p>You must select the exact same AH authentication method on both ends of a VPN tunnel.</p>
Target Host Range	<p>The following fields will define the range of IP addresses of computers on the remote LAN (the remote endpoint of the VPN tunnel) that will be allowed to access the VPN.</p>
Type	<p>This drop-down menu allows you to select the type of network definition for the range of IP addresses on the remote LAN that will be allowed to access the VPN. At the time of the writing of this manual, only the Subnet type is supported.</p>
Starting Target Host	<p>This is the first IP address of a subnet range of IP addresses of computers on the remote LAN that will be allowed to access the VPN. In this case, the entire subnet of IP addresses from</p>

	<p>192.168.2.1 to 192.168.2.254 will be allowed to access the VPN.</p> <p>Note that the IP addresses 192.168.2.0 and 192.168.2.255 are reserved for use on the remote network.</p>
Subnet Mask	Enter the subnet mask corresponding to the IP address range entered above.

Tunnel Table

The Tunnel Table displays the current tunnel setup.

IPSec Settings / Tunnel Settings / Tunnel Table / IPSec Status			
		Total No. of Entries: 1 / 16	
Tunnel ID	Termination Address	View	Delete
Remote Gateway	10.44.13.10		

Click on the View icon corresponding to a given Tunnel ID to display its current Tunnel Settings, as shown below.

[IPSec Settings](#) / [Tunnel Settings](#) / [Tunnel Table](#) / [IPSec Status](#)

[Add New Tunnel](#)

Tunnel ID:

Termination IP:

Shared Key:

Tunnel Type:

Phase 1 Proposal

Mode: ☐ Main ☒ Aggressive

OH Group:

IKE Life Duration: seconds

IKE Hash:

IKE Encryption:

Phase 2 Proposal

PFS Mode:

IPSec Operation:

IPSec Life Duration: seconds

ESP Transform:

ESP Auth:




AH Transform:

Target Host Range

Type:

Starting Target Host:

Subnet Mask:

Apply Cancel Help

IPSec Status

Click on the **IPSec Status** link to display the current IPSec status table, as shown below.

[IPSec Settings](#) / [Tunnel Settings](#) / [Tunnel Table](#) / [IPSec Status](#)

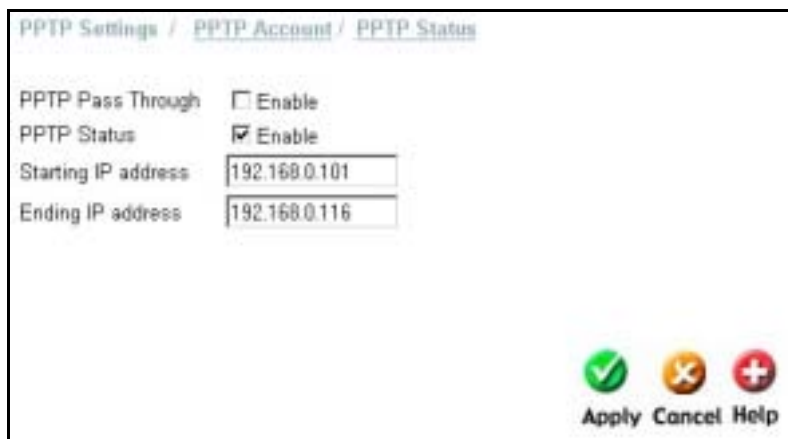
Total No. of Entries: 1 / 16

Tunnel ID	Status	Receive Bytes	Transmit Bytes
Remote Gateway	BROKEN	0	0

VPN-PPTP Settings

The Point-to-Point Tunneling Protocol (PPTP) is another method of establishing a secure tunnel between the DFL-600 and a remote gateway.

The **PPTP Settings** page allows you to enable or disable PPTP on the DFL-600.






PPTP Settings / PPTP Account / PPTP Status

PPTP Pass Through ☐ Enable

PPTP Status ☒ Enable

Starting IP address

Ending IP address

Apply Cancel Help

PPTP Pass Through	Click Enable to allow PPTP packets to pass through the router to the destination computer on your LAN. When IPsec Pass-through is enabled, the DFL-600 will allow PPTP packets to reach their destination computer on your LAN.
PPTP 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

The **PPTP Account** settings page allows you to enter a username and password for a PPTP account. A combined maximum of 64 PPTP and L2TP user accounts can be configured on the DFL-600.

PPTP Settings / PPTP Account / PPTP Status

[Add/New User Account](#)

User Name

Password

Confirm Password

Apply Cancel Help

Total No. of Entries(PPTP / L2TP+PPTP): 1 / 64

User Name	View ID	Delete
olivial04		

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

PPTP Status

Click on the **PPTP Status** link to display the current status of a PPTP tunnel on the DFL-600, as shown below.

PPTP Settings / PPTP Account / PPTP Status

User Name	Peer IP address	Receive Bytes	Transmit Bytes
-----------	-----------------	---------------	----------------

VPN-L2TP Settings

The Layer 2 Tunneling Protocol (L2TP) is another method of establishing a secure tunnel between your DFL-600 and a remote gateway. The L2TP Status page allows you to enable or disable L2TP on the DFL-600.



L2TP Settings / L2TP Account / L2TP Status

L2TP Pass Through ☐ Enable

L2TP Status ☒ Enable

Starting IP address: 192.168.0.117

Ending IP address: 192.168.0.132

Apply Cancel Help

L2TP Pass Through	Click Enable to allow L2TP packets to pass through the router to the destination computer on your LAN. When IPsec Pass-through is enabled, the DFL-600 will allow L2TP packets to reach their destination computer on your LAN.
L2TP 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

The L2TP page allows you enter your username and password for an L2TP account. A combined maximum of 64 PPTP and L2TP user accounts can be configured on the DFL-600.

[L2TP Settings](#) / [L2TP Account](#) / [L2TP Status](#)

Add/New User Account

User Name

Password

Confirm Password







Apply

Cancel

Help

Total No. of Entries(L2TP / L2TP+PPTP): 1 / 64

User Name	View ID	Delete
jirong		

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

L2TP Status

Click on the L2TP Status link to display the current status of an L2TP tunnel on the DFL-600, as shown below.

L2TP Settings / L2TP Account / L2TP Status			
User Name	Peer IP address	Receive Bytes	Transmit Bytes

Tools – Administration

The Admin Settings page allows you to add or edit the Username and Password list to control access to the configuration of the DFL-600.

A default user account is configured with the username **admin**, and a password of **admin**. You can change the password at any time.

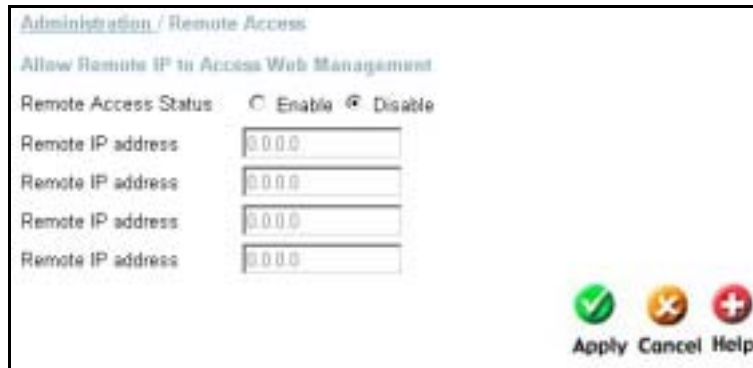


The screenshot shows a web interface titled "Administration / Remote Access". It contains a form with four input fields: "User Name" (containing "admin"), "Old Password", "New Password", and "Confirm New Password". To the right of the form are three circular icons: a green checkmark, an orange 'X', and a red plus sign. Below these icons are the labels "Apply", "Cancel", and "Help".

Username	Enter the username for the account here.
Old Password	Enter the old password 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

Remote Access

The **Remote Access** page allows you to enter the IP addresses of computers on the WAN (Internet) 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 the WAN (all computers) can access the DFL-600's configuration utility – provided they know the correct username and password.



The screenshot shows a web-based configuration interface for 'Administration / Remote Access'. The title is 'Allow Remote IP to Access Web Management'. Below this, there is a 'Remote Access Status' section with two radio buttons: 'Enable' (which is unselected) and 'Disable' (which is selected). Underneath, there are four input fields, each labeled 'Remote IP address', each containing the text '0.0.0.0'. At the bottom right, there are three buttons: a green checkmark icon labeled 'Apply', an orange 'X' icon labeled 'Cancel', and a red plus icon labeled 'Help'.

Tools – System

The **System Settings** page allows you to save the current configuration to the DFL-600's Flash RAM (NVRAM). Clicking the **Apply** button on any given configuration page will make the changes current, but you must execute an **Apply Settings and Restart** from the **System Settings** page to enter the configuration into the DFL-600's NVRAM. If you do not, the DFL-600 will revert to the last saved configuration when it is restarted.

There are two options for restarting the DFL-600 – save settings and restart, or 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-600 will be restored to the same configuration it had when it left the factory.



Tools – Firmware

The Firmware Upgrade page allows you to upgrade the DFL-600's firmware from a new firmware file stored on your local hard drive.

In addition, you can choose to load the DFL-600's current VPN or Firewall settings to a hard drive on a local computer. Clicking on the OK button will initiate a download of either the VPN settings (as a text file named DFL600_vpn.txt) or the Firewall settings (as a text file named DFL600_cw.txt). These files will be uploaded from the DFL-600 to the hard drive of the computer that is accessing the web-based configuration manager. You can choose where on the local computer's hard disk the files will be stored.



Update File	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 OK 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.

Tools – Ping

Ping is a small program that will send a series of test packets to a network device and ask for the device to send the packets back to the source. It is very useful to determine if a given network device is properly connected to the network and is operating properly.

To ping an IP address, enter the IP address in the IP address field, enter the number of packets you want to send in the Count number field (three is usually sufficient) and click the Apply button. The results will be displayed in the field with a scroll bar to the right, as shown below.

Ping Test

Set Type

IP address

Domain Name

Count number <= 10

```


PING 192.168.0.1 (192.168.0.1): 56 data bytes
64 bytes from 192.168.0.1: icmp_seq=0 ttl=255 time=0.5 ms
64 bytes from 192.168.0.1: icmp_seq=1 ttl=255 time=0.3 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=255 time=0.2 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.3/0.5 ms

```

Status – Device Info

The **Device Information** page displays the current network settings and allows you to view the IP address assigned to the DFL-600 by your ISP using DHCP (Dynamic Host Configuration Protocol – the **Dynamic IP Address** setting on the **WAN Settings** page under the **Home** page).

Device Information	
Device Name	DFL-600
Hardware Version	2A1
Firmware Version	1.00.b34
LAN	
MAC Address	00:05:5d:9a:fe:8e
IP address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
WAN	
MAC Address	00:05:5d:9a:fe:8f
Connection Type	Static IP Address
IP address	10.54.24.10
Subnet Mask	255.0.0.0
Default Gateway	10.254.254.251
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.1.2
DMZ	
IP address	192.168.1.1
Subnet Mask	255.255.255.0
 Help	

LAN Status

MAC Address	This is the MAC address of the DFL-600 on the LAN.
IP Address	This is the DFL-600'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-600 on the LAN.
DHCP Server	Displays whether the DFL-600 is currently configured as a DHCP server on the LAN.



WAN Status

MAC Address	This is the MAC address of the DFL-600 on the WAN.
Connection Type	This displays the current connection type between the DFL-600 and your ISP.
IP Address	This is the IP address of the DFL-600 on the WAN.

Subnet Mask	This is the subnet mask corresponding to the IP address above, that is currently in use by the DFL-600 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.

Status – NAT Info

The DFL-600 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:

<div> <div>NAT Information</div> <div>   </div> <div>Refresh Help</div> </div>	
<div> <div>NAT Session Table</div> <div>Total No. of Entries: 2 / 2560</div> </div>	
Private IP address : Port	Peer IP address : Port

Private IP address: Port	This is the IP address and port number of a computer or device on your LAN that has an active NAT session.
Peer IP address: Port	This is the IP address and port number of a computer or device on the WAN that has an active connection with the DFL-600

Status – Log Info

Your DFL-600 can keep logs of the various functions it supports. The Log Status page allows you to enable or disable each of these logs using a series of drop-down menus.

Log Status / [Intrusion Log](#) / [Blocking Log](#) / [Session Log](#) / [Black List](#)
[IPSec Log](#) / [Sys Log](#)

Intrusion Log Status

Blocking Event Log Status

Session Event Log Status



Black List Log Status

  
 Apply Cancel Help

Intrusion 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-600'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:

[Log Status](#) / [Intrusion Log](#) / [Blocking Log](#) / [Session Log](#) / [Black List](#)
[IPSec Log](#) / [Sys Log](#)

 
 Refresh Help

Intrusion Log Table

Total No. of Entries: 0 / 150

Intrusion Type	Source: port	Destination: port
Page		

Intrusion Type	A brief statement of the type of intrusion that was attempted is displayed here.
Source: port	Displays the source IP address and the

	TCP/UDP port that the intrusion was attempted from.
Destination: port	Displays the destination IP address and the TCP/UDP port that the intrusion was attempted to.

Blocking 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-600's firewall. Some of these session types are defined by you under on the **Port Filter Policy** page, under **Policy 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 Log**, as shown below:

[Log Status](#) / [Intrusion Log](#) / [Blocking Log](#) / [Session Log](#) / [Black List](#)
[IPSec Log](#) / [Sys Log](#)




Refresh Help

Blocking Log Table
Total No. of Entries: 50 / 50

Transport Type	Source	Destination: port	Blocking Reason
----------------	--------	-------------------	-----------------

Transport Type	The protocol used to make the connection attempt is displayed here.
Source	
Destination: port	The IP address and the TCP/UDP port number of the computer or device that was the destination of connection attempt to the DFL is displayed here.
Blocking Reason	A brief statement of why the connection attempt was blocked is displayed here

Session Log

Session events (when a computer on your LAN accesses an application of service on the WAN), are logged by the DFL-600 and are displayed on the **Session Log**, as shown below:



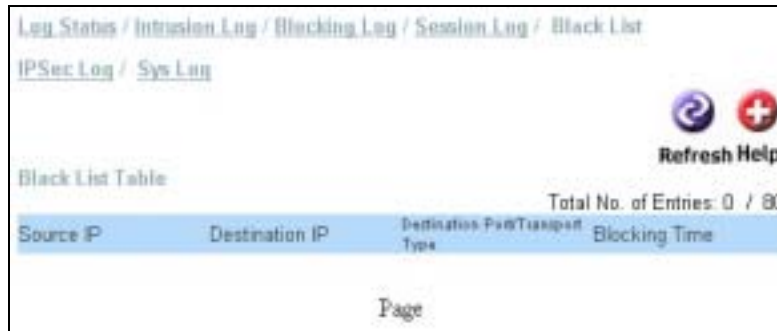
Source: port	The IP address and TCP/UDP port number of the computer or device that initiated the session is displayed here.
Destination: port	The IP address and TCP/UDP port number of the computer or device that responded to the session initiation is displayed here.
Type	The protocol used to conduct the session is displayed here.
Terminate Reason	When the session is terminated, it is displayed here.

Black List

The DFL-600'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-600'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-600) the IP address, the protocol used, and the corresponding port number is determined and entered into the DFL-600's Intruder Blacklist.

Once the intruder's information is entered, the DFL-600's firewall will block packets from this location from crossing the DFL-600 (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-600's Intruder Blacklist, that IP address is blocked from sending packets through the DFL-600.



Source IP	Destination IP	Destination Port/Transport Type	Blocking Time
Page			

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-600 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/Transport Type	The port number or ICMP Type that an intruder used to attempt to make a connection is displayed here.
Blocking Time	This is the amount of time the Source IP has been blocked.

IPSec Log

The DFL-600 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:



Index	<p>This displays the sequence of the IPSec log. There are five categories of status that can be displayed here, as follows:</p> <p>BROKEN NEGOTIATION P1 NEGOTIATION P2 P1_ESTABLISHED P2_ESTABLISHED</p>
Description	<p>A brief description of the log entry will be displayed here.</p>

Sys Log

The DFL-600 can save or transmit Syslog messages to aid in network administration. You must have a Syslog application on one of the computers on your LAN to take advantage of this feature.

Clicking on the **Sys Log** link will open the **Sys Log** configuration page, as shown below.


Save Location	Choose either the Remote Server or the Local Flash option.
Remote Server IP	Enter the IP address of the computer on your LAN that is running the Sys log application.
Sys Log Level	This drop-down menu allows you to select the level of Sys log information that the DFL-600 will send to the Sys log server.


Status – Traffic Log


Your DFL-600 keeps a log of the total number of bytes received and transmitted on to and from the LAN and WAN. This information can be displayed by clicking on the Traffic button to display the Traffic Statistics page, as shown below.

Traffic Statistics

	Received Bytes	Transmitted Bytes
WAN	60	0
LAN	0	0

 Refresh

 Clear

 Help

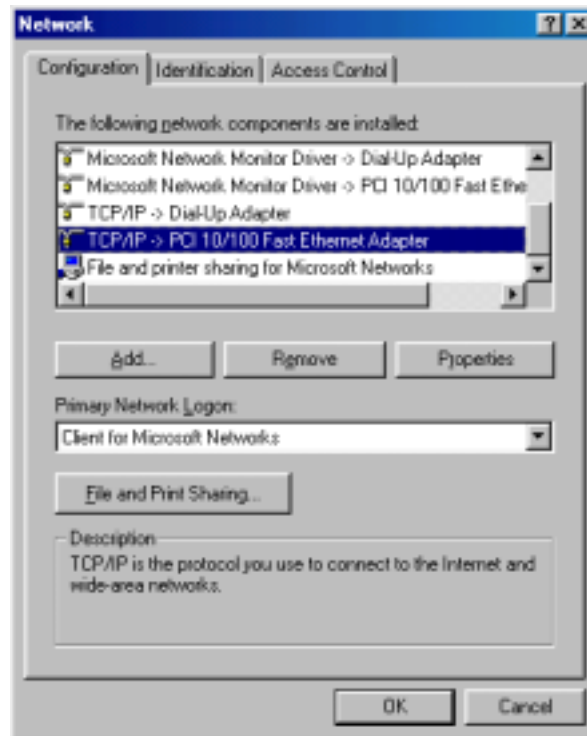
Connecting PCs to the DFL-600 Router

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 then 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/adaptor. 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 address automatically**.



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

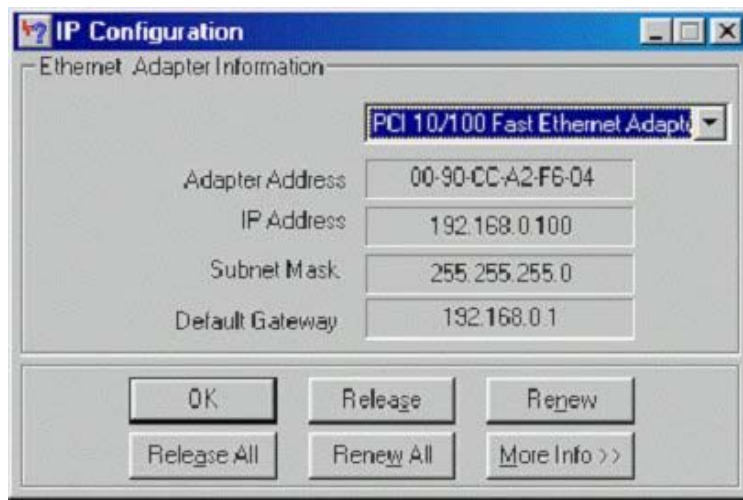
CONFIRM YOUR PC'S IP CONFIGURATION

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)**

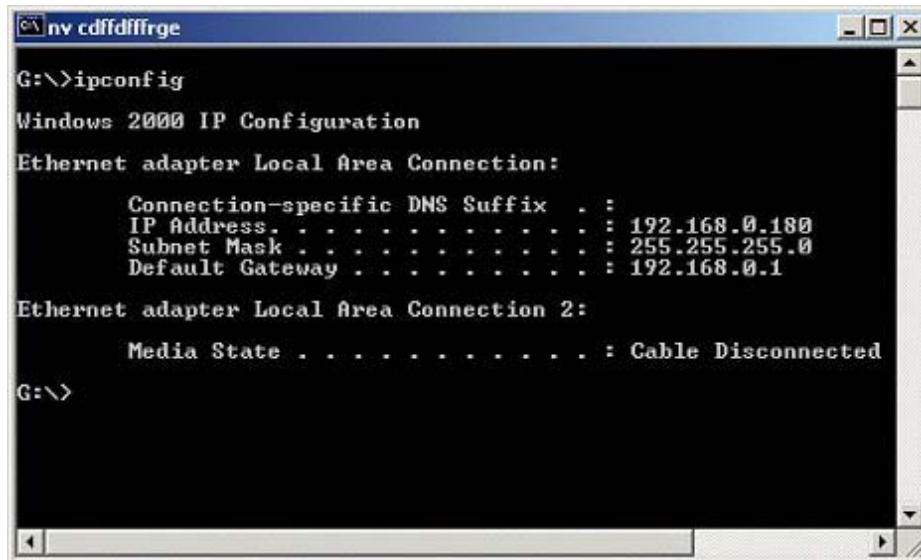
Inside the windows 95/98 Start button, select Run and type winipcfg. In the example below this computer has an IP address of 192.168.0.100 and the default gateway is 192.168.0.1. The default gateway should be the network device IP address. The MAC address in windows 95/98 is called the Adapter Address.

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.



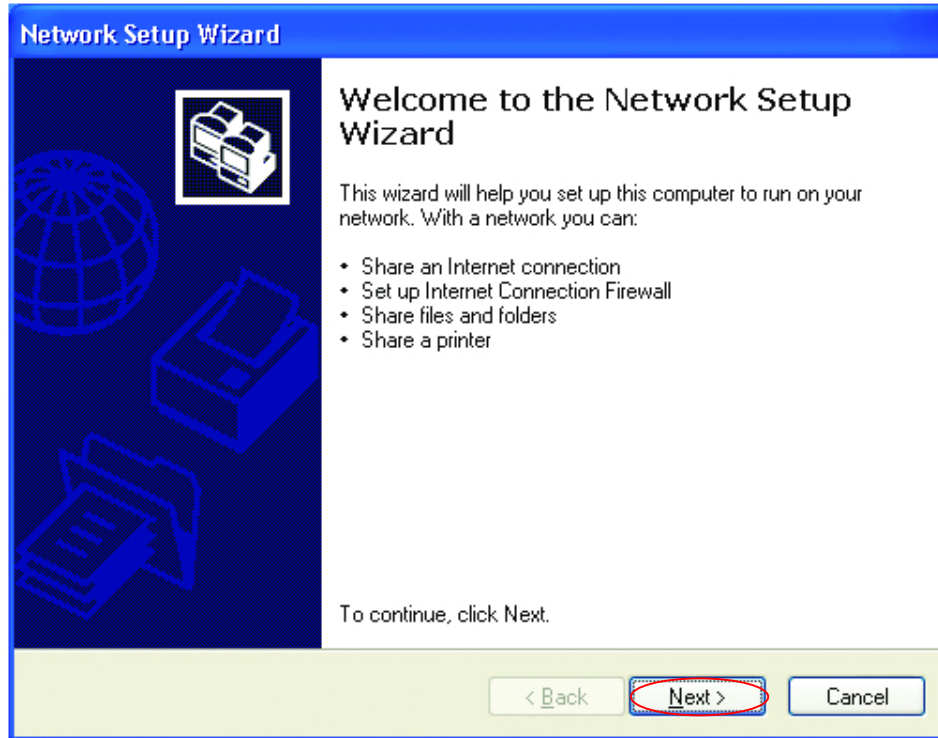
Networking Basics

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.

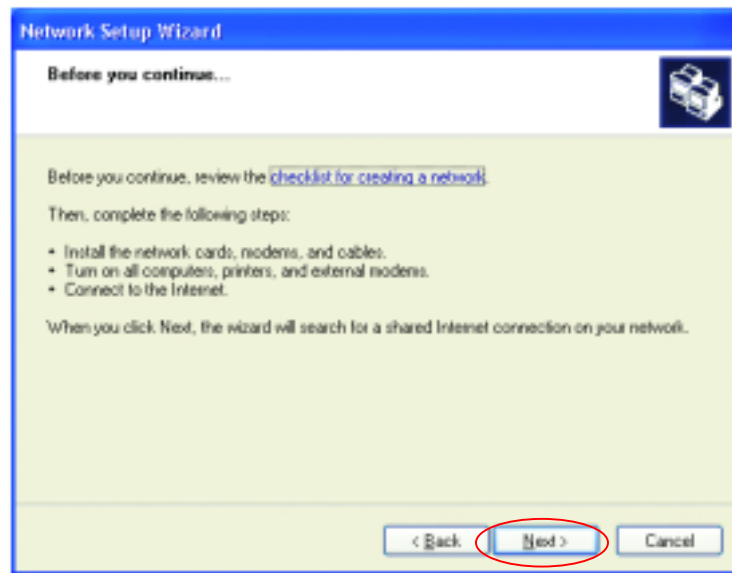
Note: Please refer to websites such as <http://www.homenethelp.com> and <http://www.microsoft.com/windows2000> for information about networking computers using Windows 2000, ME or 98.

Go to START>CONTROL PANEL>NETWORK CONNECTIONS
Select Set up a home or small office network



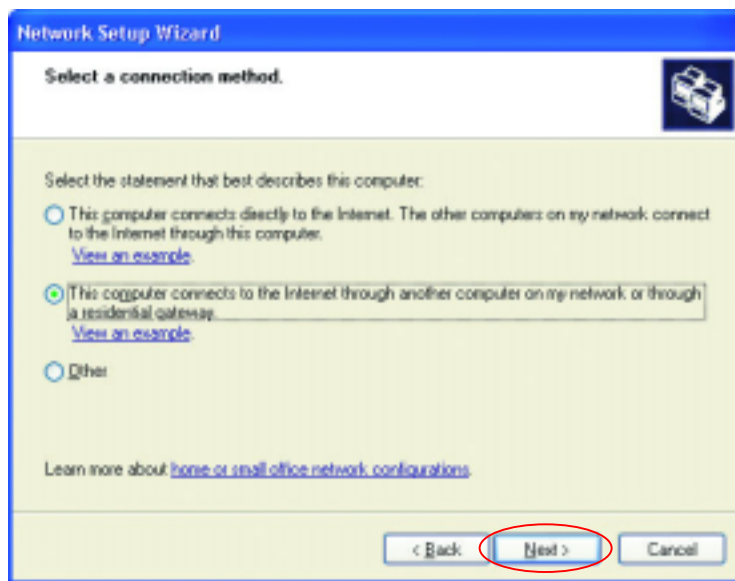
When this screen appears, Click **Next**.

Please follow all the instructions in this window:



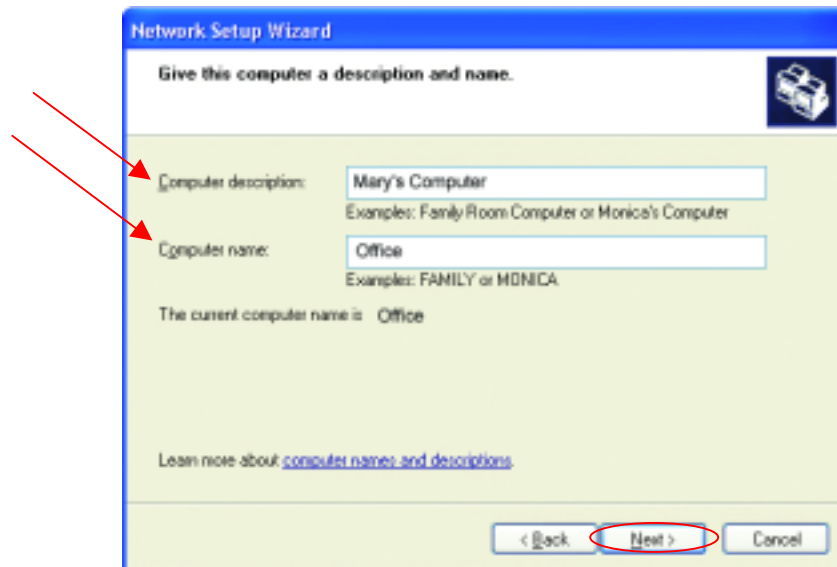
Click Next

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.



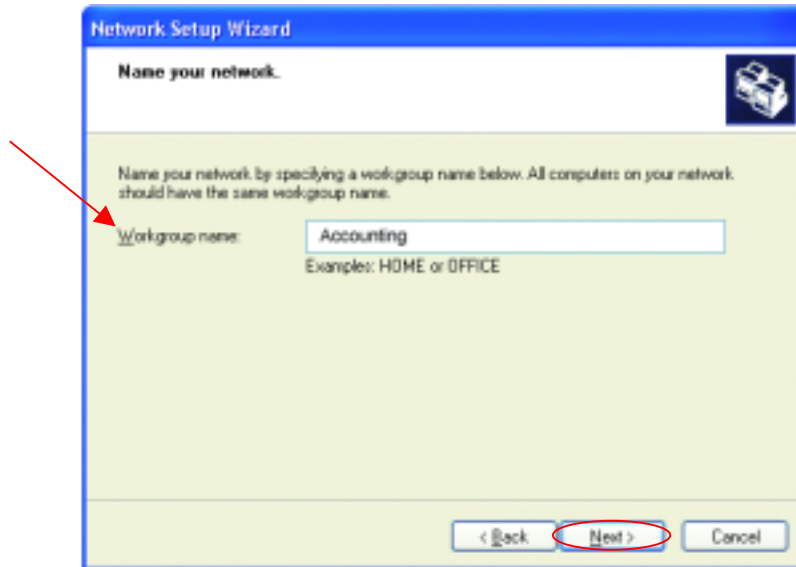
Click **Next**

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



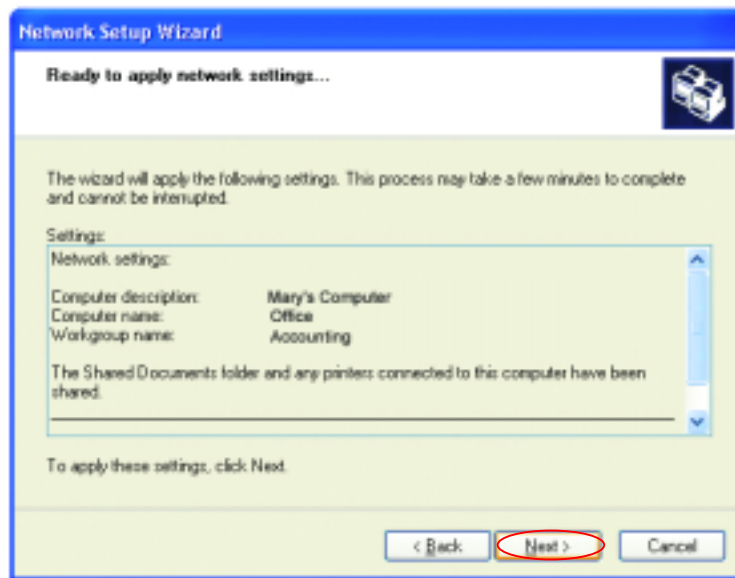
Click **Next**

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



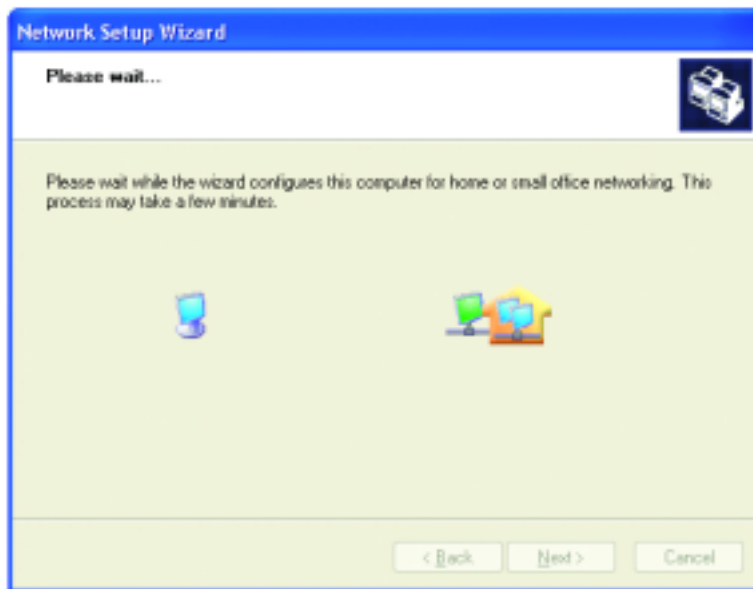
Click **Next**

Please wait while the wizard applies the changes.

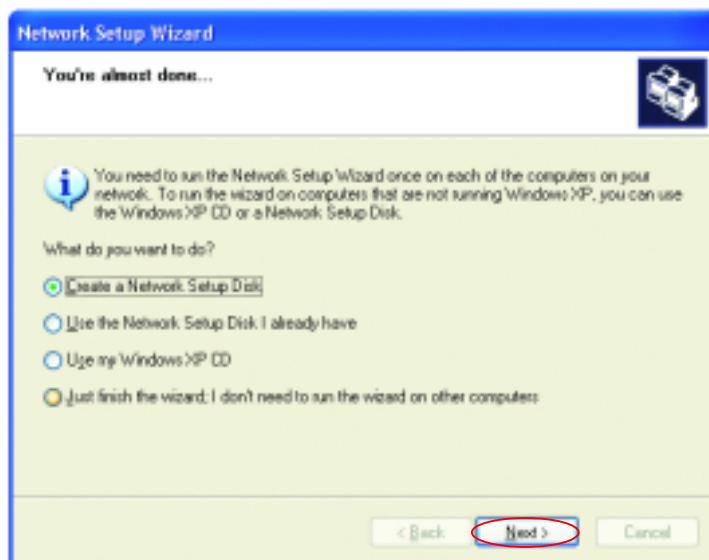


When the changes are complete, Click **Next**.

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:”



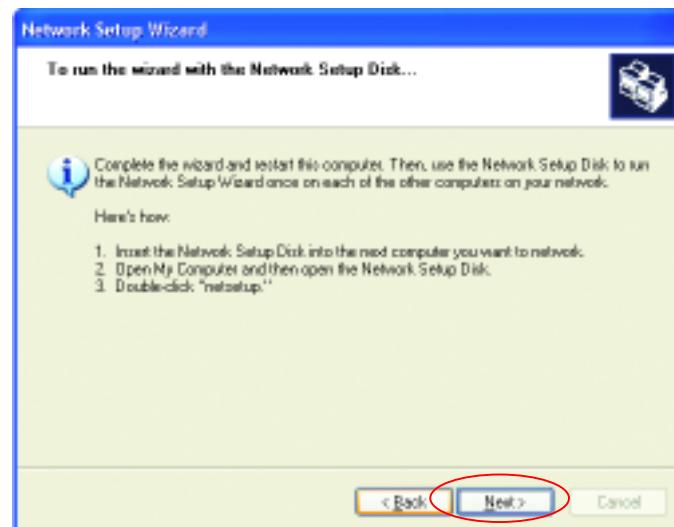
Format the disk if you wish, and Click **Next**.

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.

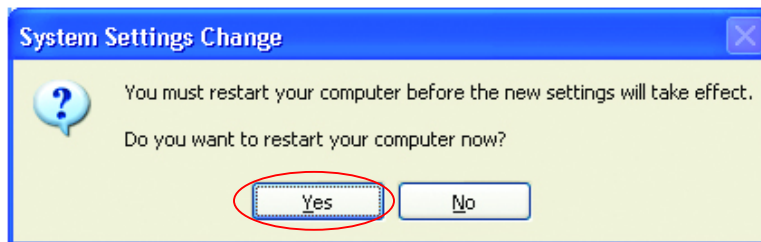
To continue Click **Next**



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

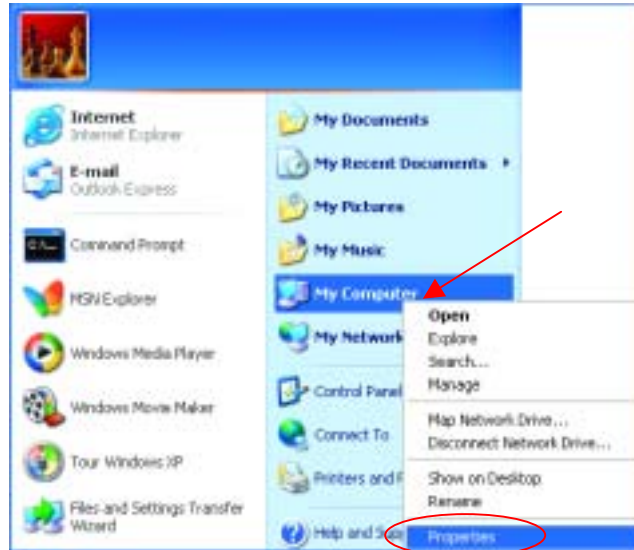
Naming your computer is optional. If you would like to name your computer please follow these directions:

In Windows XP:

Click **START** (in the lower left corner of the screen)

Right-click on **My Computer**

Select **Properties**

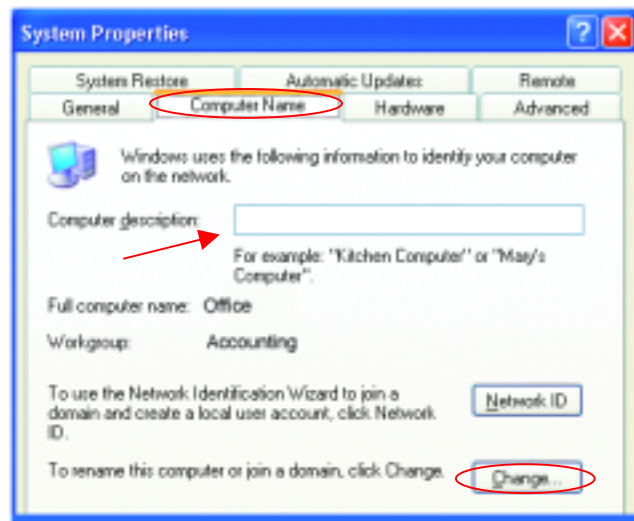


- Select the **Computer Name Tab** in the **System Properties** window.

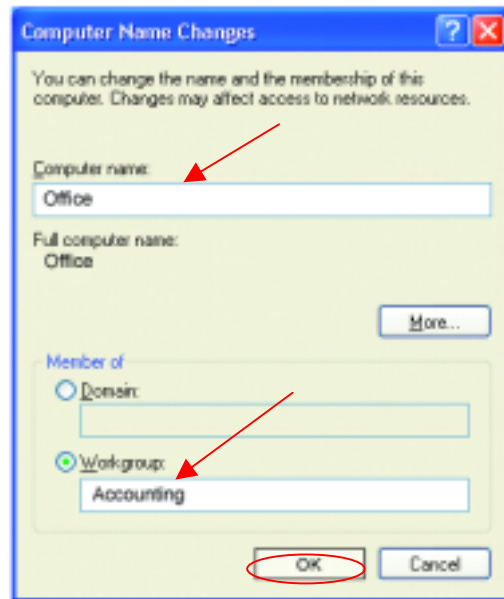
You may enter a Computer description if you wish, this field is optional.

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**

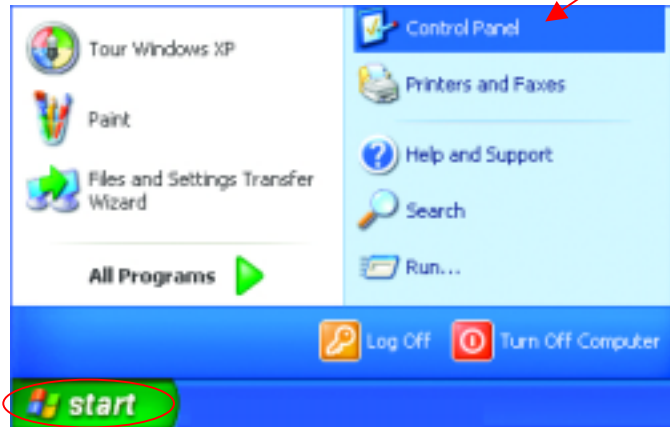


Assigning a Static IP Address

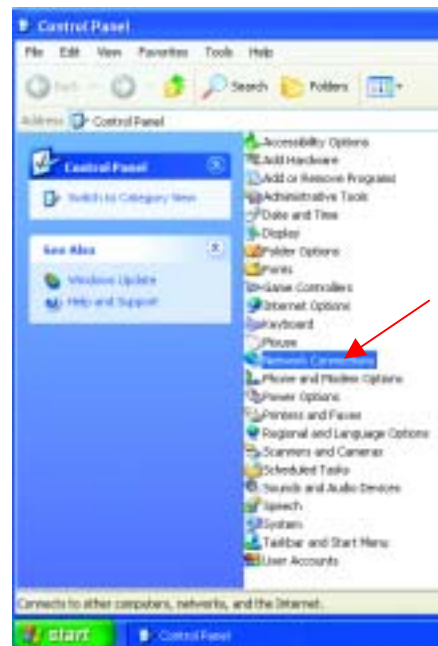
Note: Residential Gateways/Broadband Routers will automatically assign IP Addresses to the computers on the network, using DHCP (Dynamic Host Configuration Protocol) technology. If you are using a DHCP-capable Gateway/Router you will not need to assign Static IP Addresses.

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



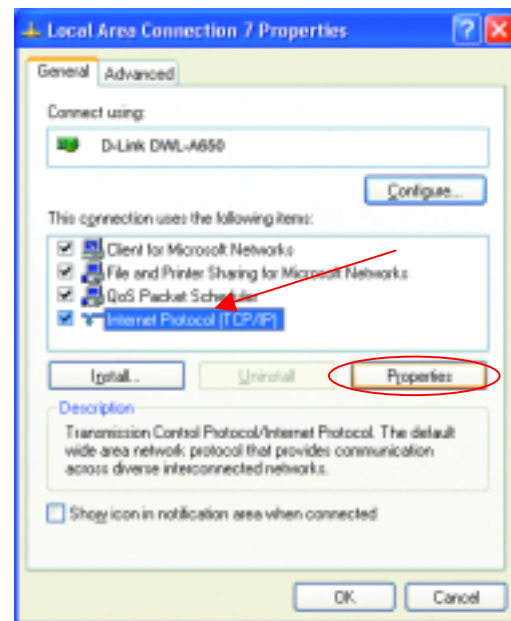
Right-click on **Local Area Connections**.

Double-click **Properties**



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

Click **Properties**

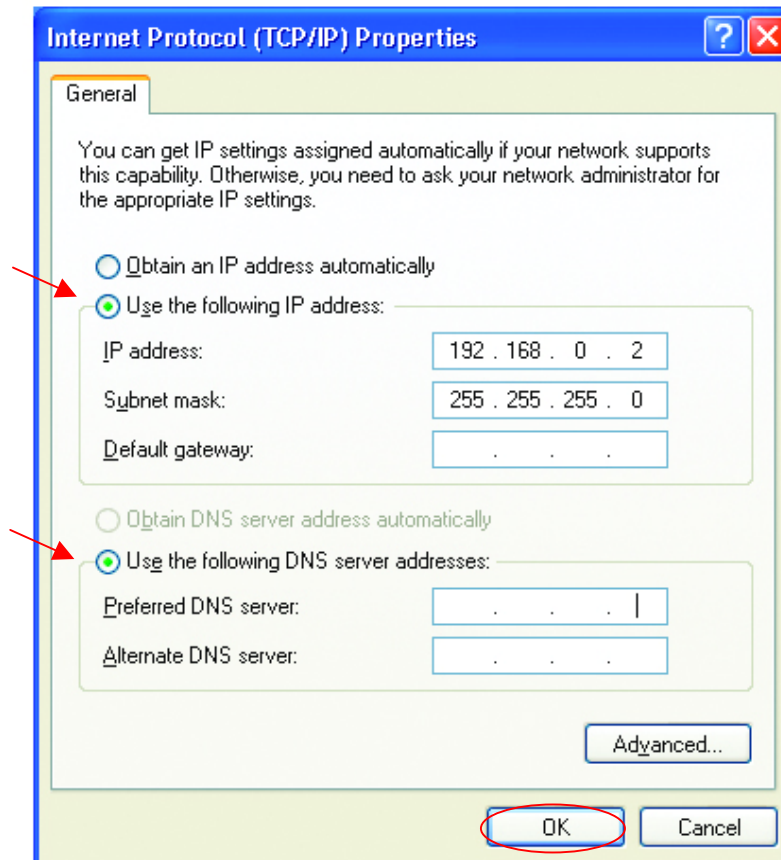


Select **Use the following IP address** in the Internet Protocol (TCP/IP) Properties window.

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



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© 2001 D-Link Corporation. Contents subject to change without prior notice. D-Link is a registered trademark of D-Link Corporation/D-Link Systems, Inc. All other trademarks belong to their respective proprietors.

Copyright Statement

No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from D-Link Corporation/D-Link Systems Inc., as stipulated by the United States Copyright Act of 1976.

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>