D-Link **DFL-600**

Firewall/VPN

Manual

Rev. 4.0

D-Link

Building Networks for People

Download from Www.Somanuals.com. All Manuals Search And Download.

Table of Contents

Download from Www.Somanuals.com. All Manuals Search And Download.

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 7.1 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Introduction

The D-Link DFL-600 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 Ethernet port on your 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.

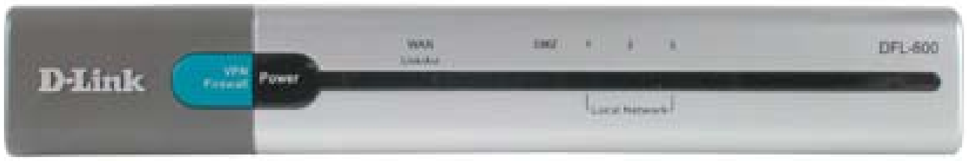
For the price of one Internet account, the DHCP-capable DFL-600 will automatically provide unique IP Addresses for all the computers on the network. *(DHCP stands for Dynamic Host Configuration Protocol. It is a protocol for assigning IP Addresses automatically. With a DHCP router like the DFL-600, there is no need to assign static IP Addresses, or purchase multiple addresses from your 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 and 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

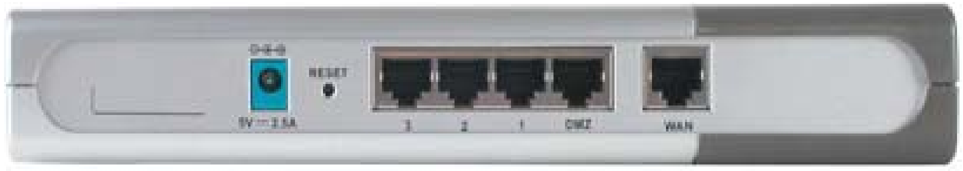
Front View



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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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, with a subnet mask of 255.255.255.0.*

Dynamic IP Settings:

It is recommended that you allow your PC's IP settings be automatically assigned by a DHCP server. By default, your new DFL-600 VPN Firewall functions as a DHCP server, and it will give your PC the necessary IP settings, every time you boot your PC.

Download from Www.Somanuals.com. All Manuals Search And Download.

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). An Internet Service Provider (ISP) or a network administrator provides the network address information on the WAN network.

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. To connect to the DFL-600's web-based management utility, type the IP address *https://192.168.0.1* into the *Address* field of your web browser. The *https* specifies the secure version of http.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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 Internet). 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 (optional) 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.

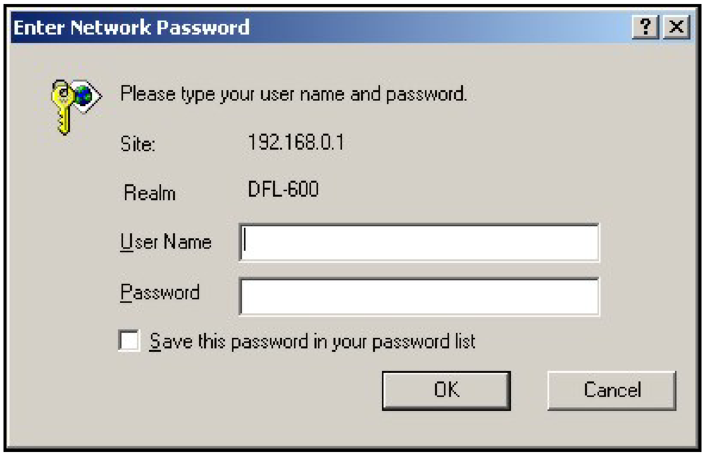
The many other features of the DFL-600 are described in subsequent sections.

Download from Www.Somanuals.com. All Manuals Search And Download.

Using the Configuration Utility

Launch your web browser and type the device IP address (*https://192.168.0.1*) 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.



Please type your user name and password.

Site: 192.168.0.1

Realm DFL-600

User Name

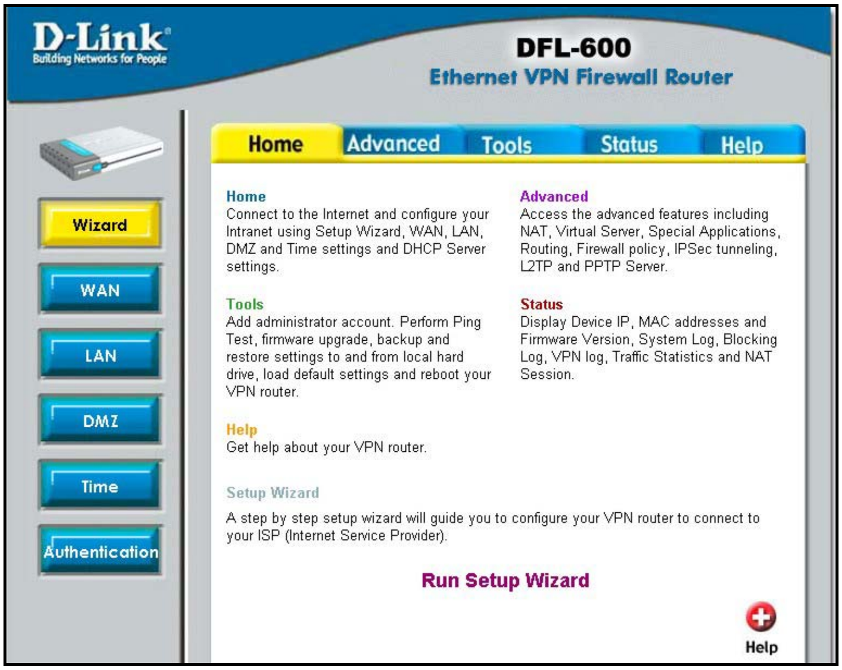
Password

□ Save this password in your password list

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.

Download from Www.Somanuals.com. All Manuals Search And Download.



Home
Connect to the Internet and configure your Intranet using Setup Wizard, WAN, LAN, DMZ and Time settings and DHCP Server settings.

Advanced
Access the advanced features including NAT, Virtual Server, Special Applications, Routing, Firewall policy, IPSec tunneling, L2TP and PPTP Server.

Tools
Add administrator account. Perform Ping Test, firmware upgrade, backup and restore settings to and from local hard drive, load default settings and reboot your VPN router.

Status
Display Device IP, MAC addresses and Firmware Version, System Log, Blocking Log, VPN log, Traffic Statistics and NAT Session.

Help
Get help about your VPN router.

Setup Wizard

A step by step setup wizard will guide you to configure your VPN router to connect to your ISP (Internet Service Provider).

Run Setup Wizard

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.

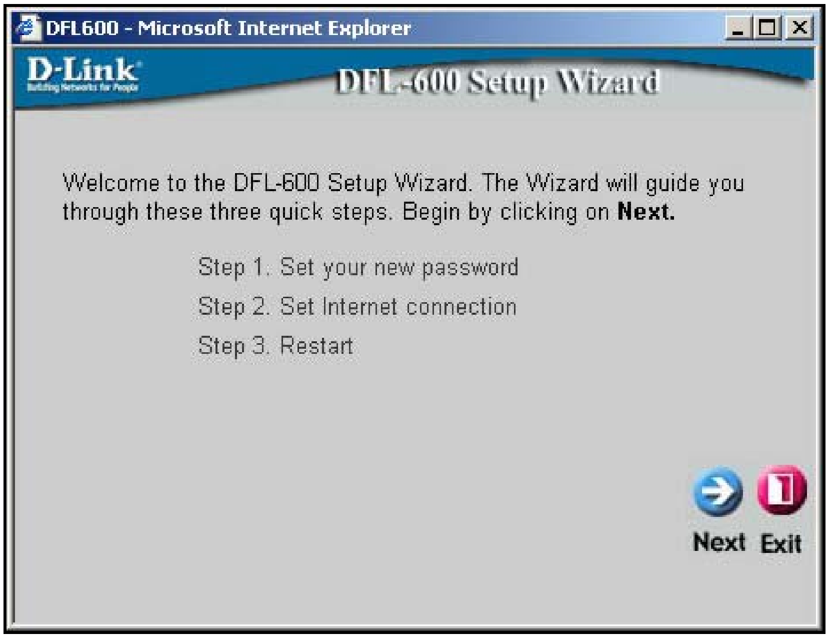
All other setup tasks can be accomplished using the configuration utility from your web browser.

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.


DFL600 - Microsoft Internet Explorer
D-Link
Building Networks for People
DFL-600 Setup Wizard
Next
Exit

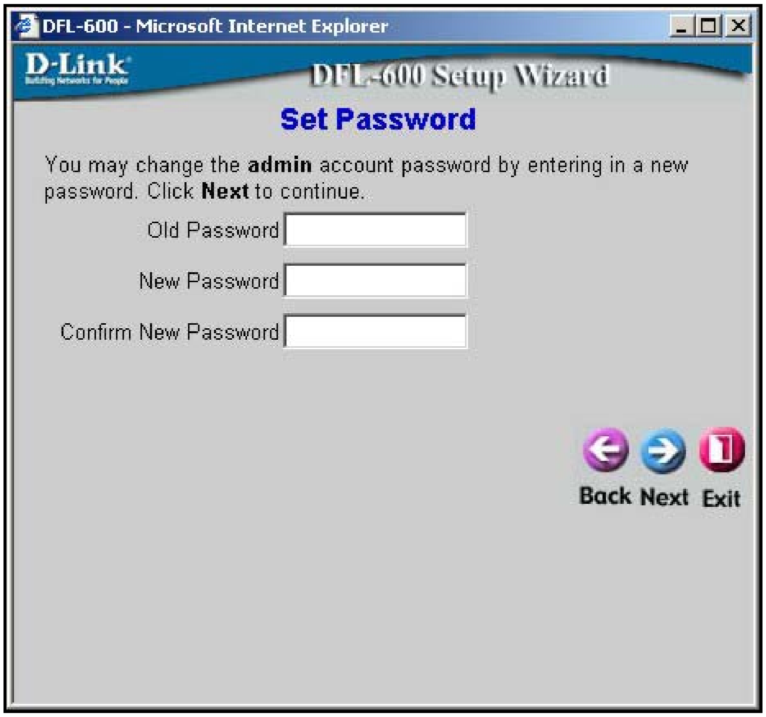
Welcome to the DFL-600 Setup Wizard. The Wizard will guide you through these three quick steps. Begin by clicking on **Next.**

Step 1. Set your new password

Step 2. Set Internet connection

Step 3. Restart

Click **Next** to continue.



Set Password

You may change the **admin** account password by entering in a new password. Click **Next** to continue.

Old Password

New Password

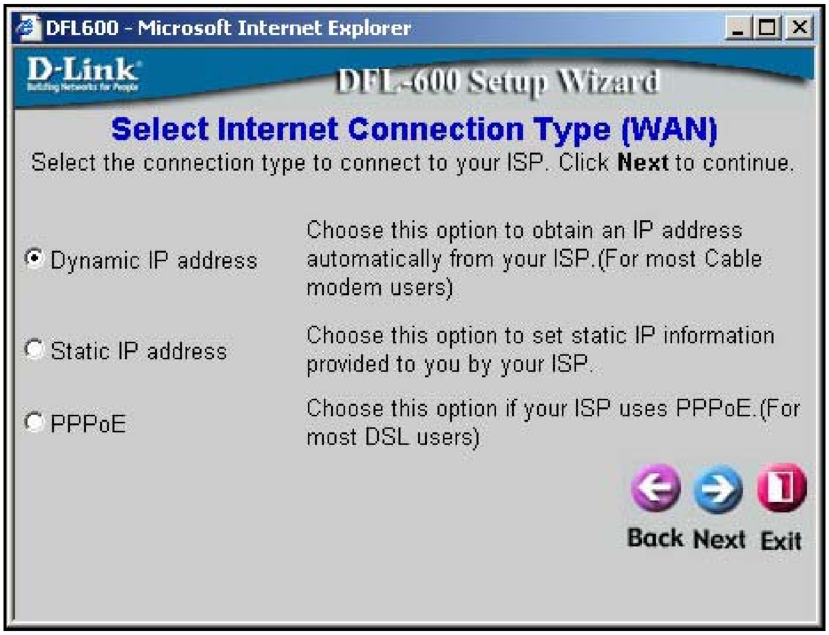
Confirm New Password

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.

Download from Www.Somanuals.com. All Manuals Search And Download.


DFL600 - Microsoft Internet Explorer
D-Link
Building Networks for People
DFL-600 Setup Wizard
Back
Next
Exit

Select Internet Connection Type (WAN)

Select the connection type to connect to your ISP. Click **Next** to continue.

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

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

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

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.

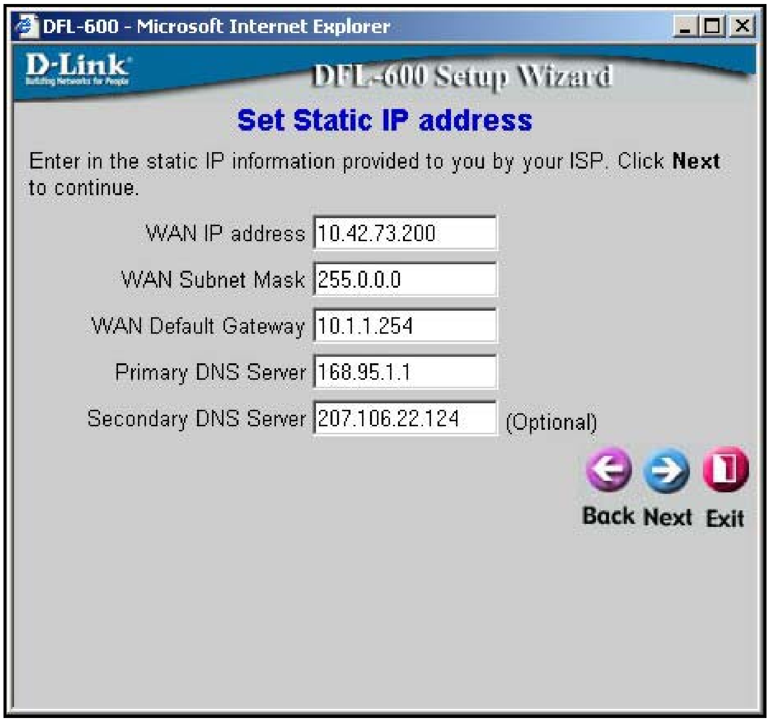
The **Static IP address** click-box is used to enter a permanent IP address that is assigned by your ISP. If your ISP assigns you a permanent IP address, choose this option.

Click **Next** to continue.

Download from Www.Somanuals.com. All Manuals Search And Download.

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:



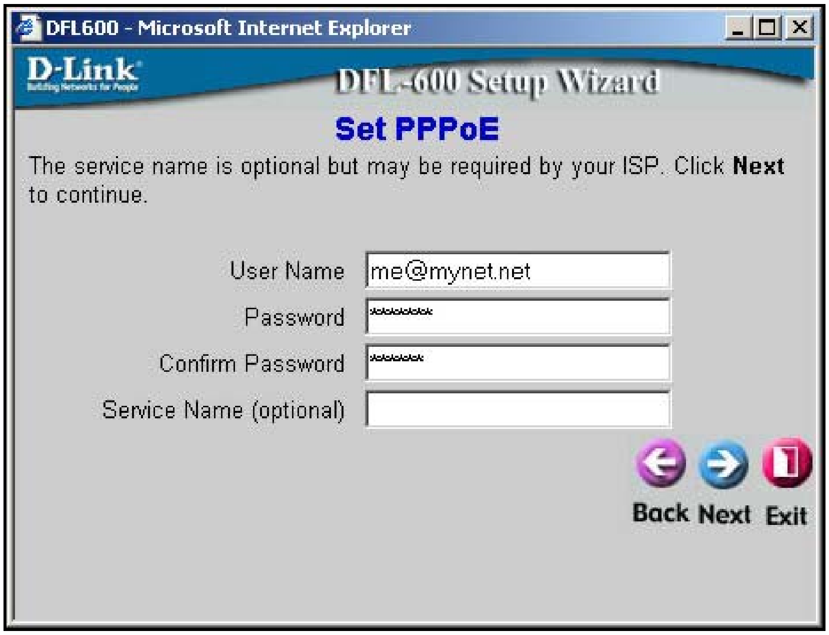
Set Static IP address

Enter in the static IP information provided to you by your ISP. Click **Next** to continue.

WAN IP address	10.42.73.200	
WAN Subnet Mask	255.0.0.0	
WAN Default Gateway	10.1.1.254	
Primary DNS Server	168.95.1.1	
Secondary DNS Server	207.106.22.124	(Optional)

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 for People
DFL-600 Setup Wizard

Set PPPoE

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

User Name: me@mynet.net

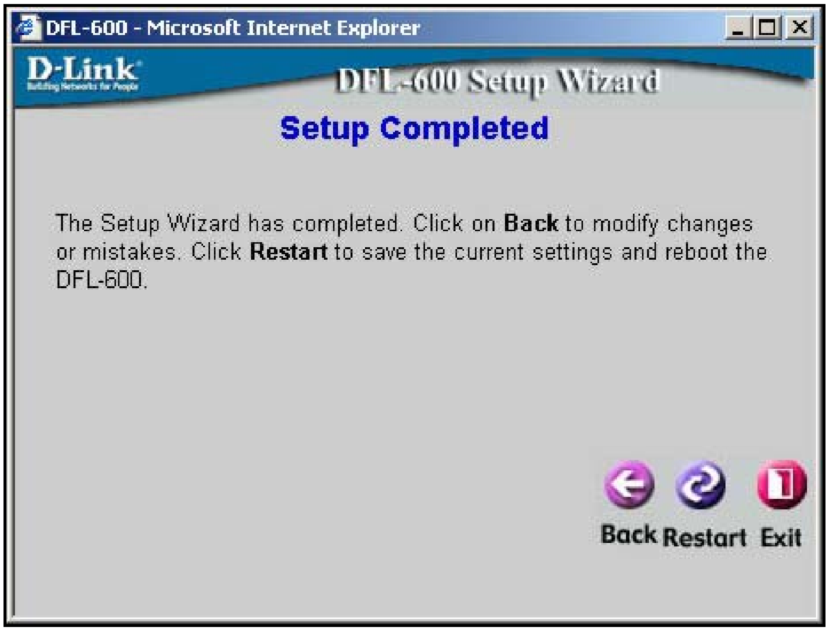
Password: *******

Confirm Password: ******

Service Name (optional):

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.


DFL-600 - Microsoft Internet Explorer
D-Link
Building Networks for People
DFL-600 Setup Wizard
Back
Restart
Exit

Setup Completed

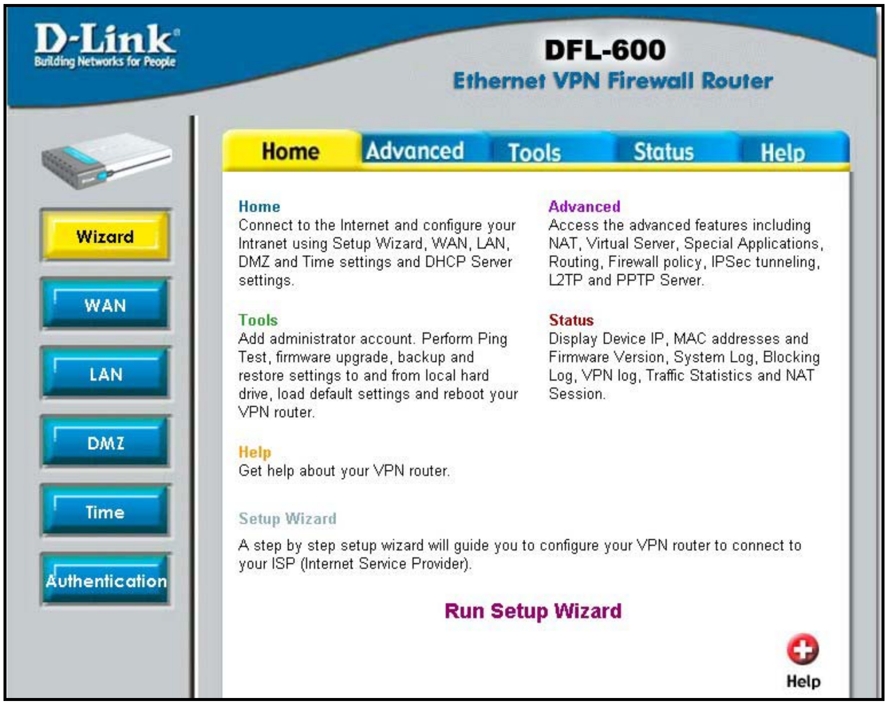
The Setup Wizard has completed. Click on **Back** to modify changes or mistakes. Click **Restart** to save the current settings and reboot the DFL-600.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Home

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



Home
Connect to the Internet and configure your Intranet using Setup Wizard, WAN, LAN, DMZ and Time settings and DHCP Server settings.

Advanced
Access the advanced features including NAT, Virtual Server, Special Applications, Routing, Firewall policy, IPSec tunneling, L2TP and PPTP Server.

Tools
Add administrator account. Perform Ping Test, firmware upgrade, backup and restore settings to and from local hard drive, load default settings and reboot your VPN router.

Status
Display Device IP, MAC addresses and Firmware Version, System Log, Blocking Log, VPN log, Traffic Statistics and NAT Session.

Help
Get help about your VPN router.

Setup Wizard

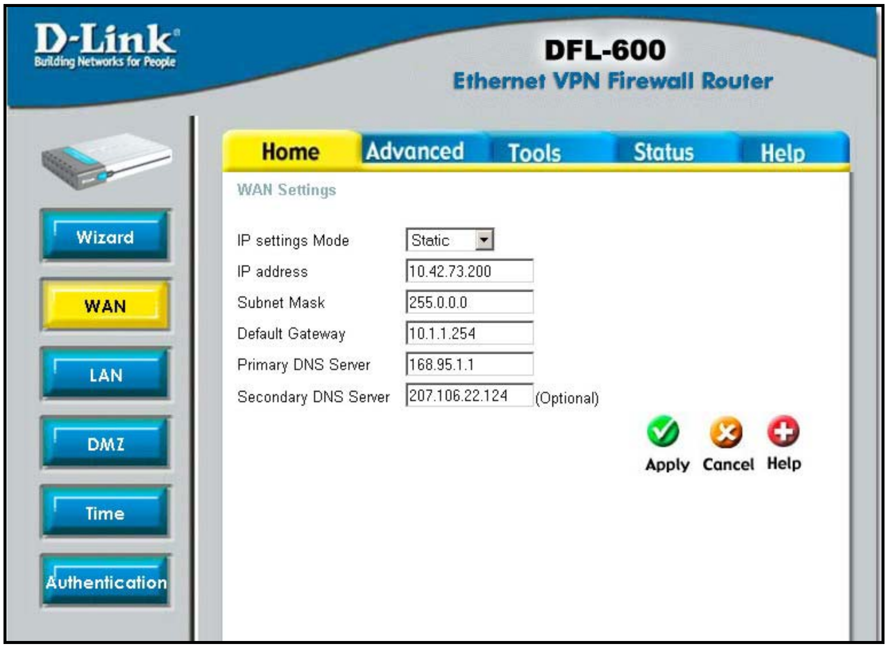
A step by step setup wizard will guide you to configure your VPN router to connect to your ISP (Internet Service Provider).

Run Setup Wizard

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.



WAN Settings

IP settings Mode	Static
IP address	10.42.73.200
Subnet Mask	255.0.0.0
Default Gateway	10.1.1.254
Primary DNS Server	168.95.1.1
Secondary DNS Server	207.106.22.124 (Optional)

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	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. **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. **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. **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.
IP Address	This is the current IP address used to identify your 'location' on the Internet. It is assigned by your ISP, or entered statically by you. IP addresses work in combination with a subnet mask, described below.
Subnet Mask	A subnet mask is a number, in the same form as an IP address, that is used to mathematically separate a range of IP addresses into a Network portion and a Node portion. The Node portion identifies a specific device on the Network – in this case, the DFL-600.

Default Gateway	This is the IP address of a device at your ISP's office where packets destined for the Internet – from your home network – are sent, before being forwarded to their final destination. For the DFL-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.

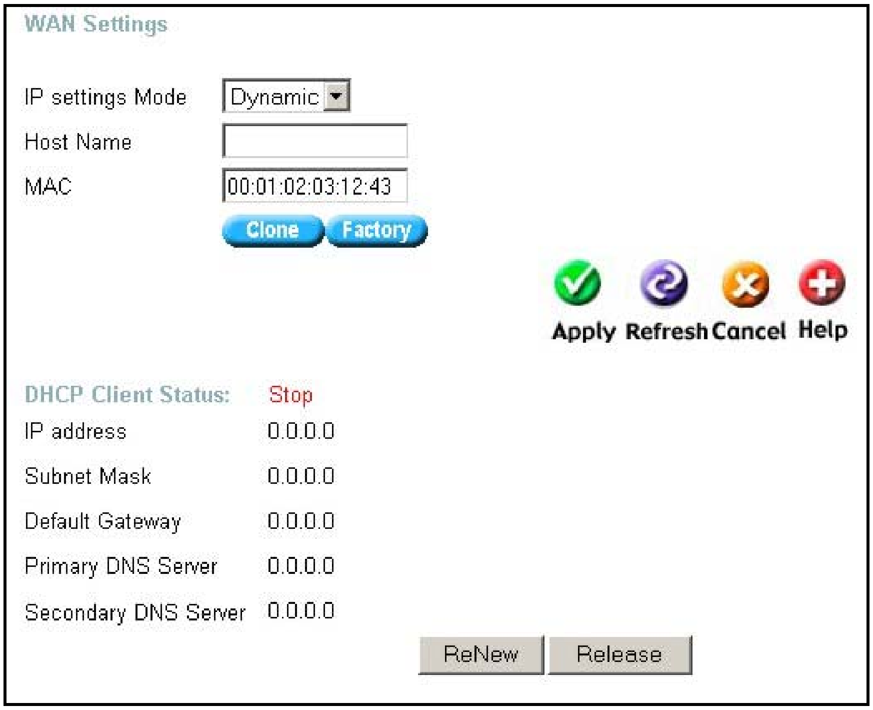
Dynamic IP Address – If your ISP uses the Dynamic Host Configuration Protocol (DHCP) to assign an IP address, subnet mask, default gateway and Domain Name Server (**DNS**) addresses, choose this option. Some ISPs require the use of an assigned Host Name for the device that will make the WAN connection.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

This is the type of IP address assignment protocol most commonly used by cable ISPs. In addition, many cable modems use the MAC address of the first computer to link to the modem as a way of identifying the user and the corresponding Internet account. The DFL-600 offers a MAC cloning feature where the DFL-600 will read the MAC address of the NIC card in the PC that the cable modem uses to identify the user. The DFL-600 will then use this

Download from Www.Somanuals.com. All Manuals Search And Download.

MAC address when connecting to the cable modem. Clicking on the **Clone** button will enable this function.

Remember to click the **Apply** button and then to save the changes using **Tools**, **System**, and the **Save** button.



WAN Settings

IP settings Mode: Dynamic

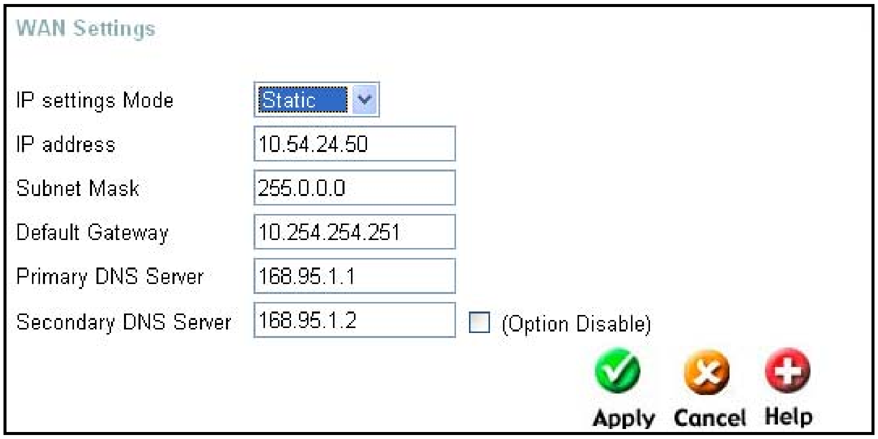
Host Name:

MAC: 00:01:02:03:12:43

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

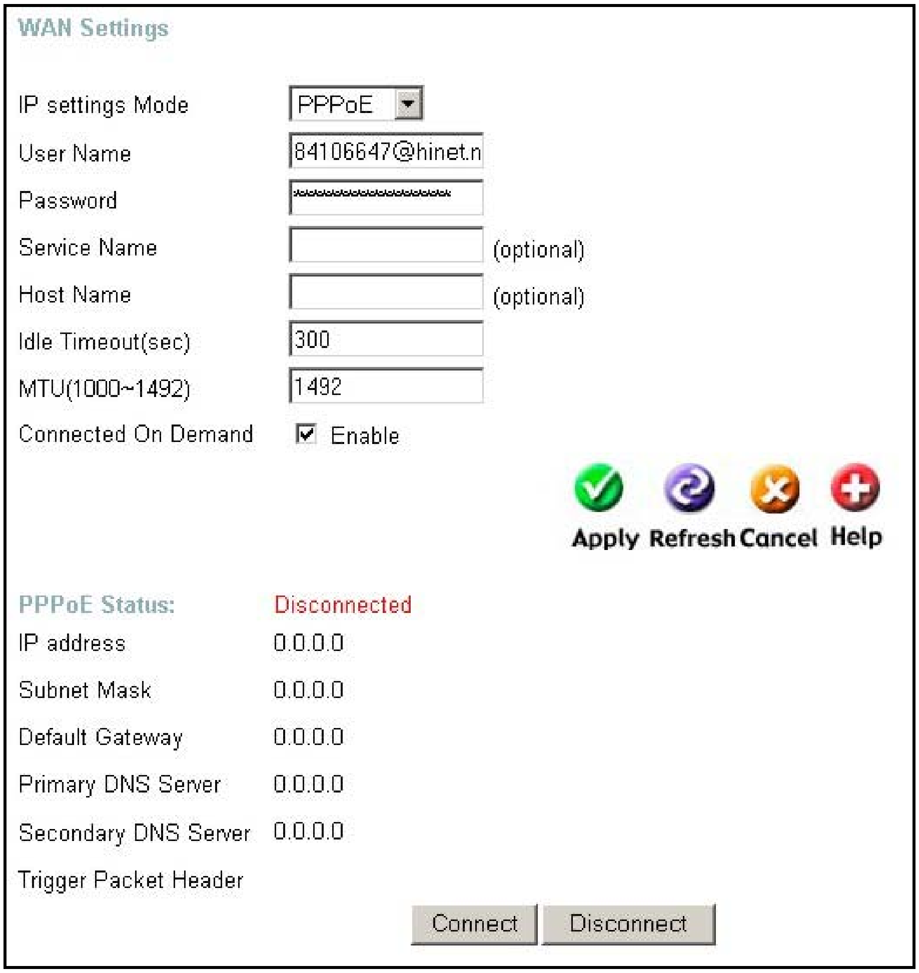
Static IP Address – If your ISP has assigned you an IP address that will never change, choose this option. When this option is chosen, the following fields appear to allow you to enter the network address information:



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)

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:



WAN Settings

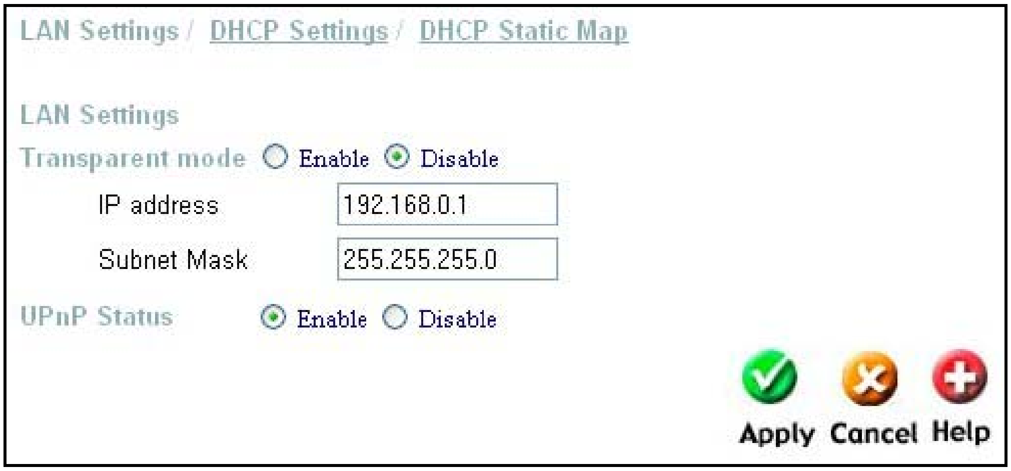
IP settings Mode	PPPoE	
User Name	84106647@hinet.n	
Password	********************	
Service Name		(optional)
Host Name		(optional)
Idle Timeout(sec)	300	
MTU(1000~1492)	1492	
Connected On Demand	☑ Enable	

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 / DHCP Static Map

LAN Settings

Transparent mode ○ Enable ● Disable

IP address 192.168.0.1

Subnet Mask 255.255.255.0

UPnP Status ● Enable ○ Disable

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. If you choose this option, you will have to reboot the PCs on the LAN side of the DFL-600 in order for them to get their new IP address settings (or you can enter the "C:\>ipconfig /renew" command in the Command Prompt window, without rebooting your computer).*

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.

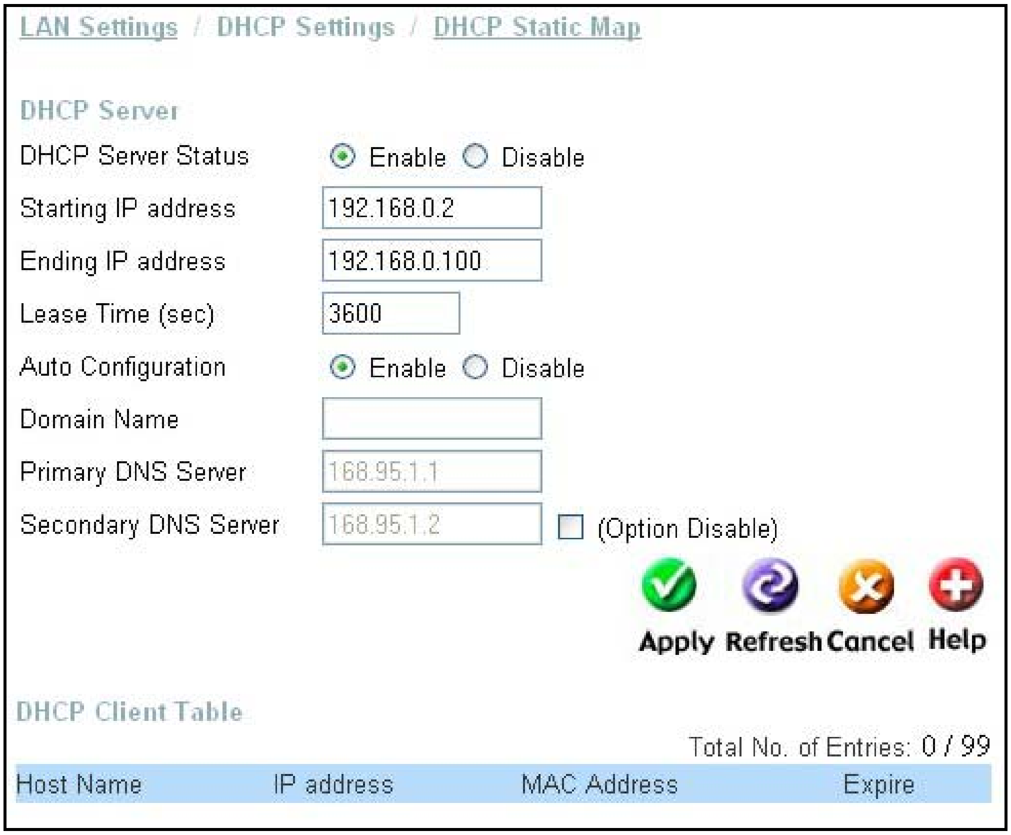
As an alternative, you could disable the DHCP server on the DFL-600 and manually update the IP address, subnet mask and default gateway information for each computer on the LAN side of the DFL-600.

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.



DHCP Server

DHCP Server Status	● Enable ○ Disable
Starting IP address	192.168.0.2
Ending IP address	192.168.0.100
Lease Time (sec)	3600
Auto Configuration	● Enable ○ Disable
Domain Name	
Primary DNS Server	168.95.1.1
Secondary DNS Server	168.95.1.2 □ (Option Disable)

DHCP Client Table

Total No. of Entries: 0 / 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 you 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.

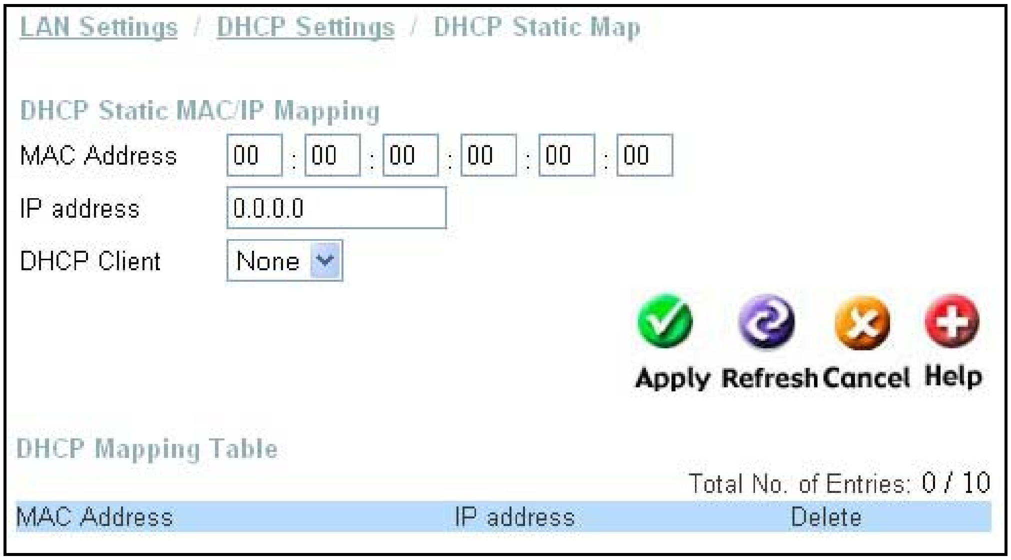
Download from Www.Somanuals.com. All Manuals Search And Download.

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.

DHCP Static Map

The DFL-600 allows you to identify PCs on your LAN by their MAC addresses, and then to specify what IP address (from the range of IP addresses established for your LAN) will be assigned to these PCs. In this way, you can always have a given PCs on your LAN assigned a given IP address.

Download from Www.Somanuals.com. All Manuals Search And Download.



LAN Settings / DHCP Settings / DHCP Static Map

DHCP Static MAC/IP Mapping

MAC Address 00 : 00 : 00 : 00 : 00 : 00

IP address 0.0.0.0

DHCP Client None

DHCP Mapping Table

Total No. of Entries: 0 / 10

MAC Address	IP address	Delete

MAC Address	This is the MAC address of the PC you want to assign the IP address specified below using DHCP.
IP Address	This is the IP address you want to assign the PC identified by its MAC address above, using DHCP.
DHCP Client	This identifies the PC as either a DHCP client or not. This allows you to check to see if the specified MAC address has already been assigned an IP address using DHCP.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

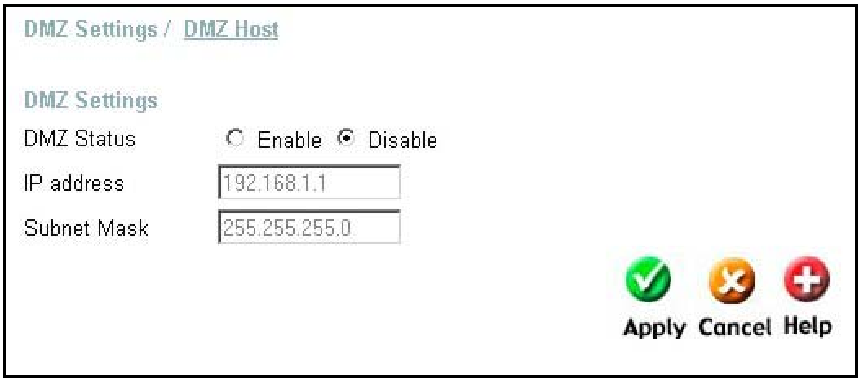
For example, if you want to use video conferencing and still use NAT, you can use the DMZ port and DMZ IP address. In this case, you must have a PC or server through which video conferencing will take place, and that computer is assigned the DMZ IP address.

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).

Download from Www.Somanuals.com. All Manuals Search And Download.

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.


DMZ Settings / DMZ Host

DMZ Settings

DMZ Status ○ Enable ● Disable

IP address 192.168.1.1

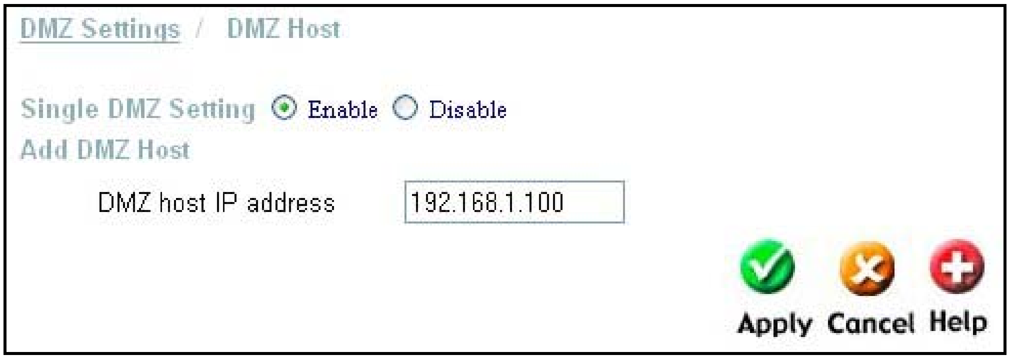
Subnet Mask 255.255.255.0

IP Address	This is the IP address assigned to the DMZ port, and will be assigned to a PC that you connect to this port. You can assign any IP address to the DFL-600's DMZ port that is within the range 192.168.1.1 to 192.168.1.254.
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

Single DMZ Setting ● Enable ○ Disable

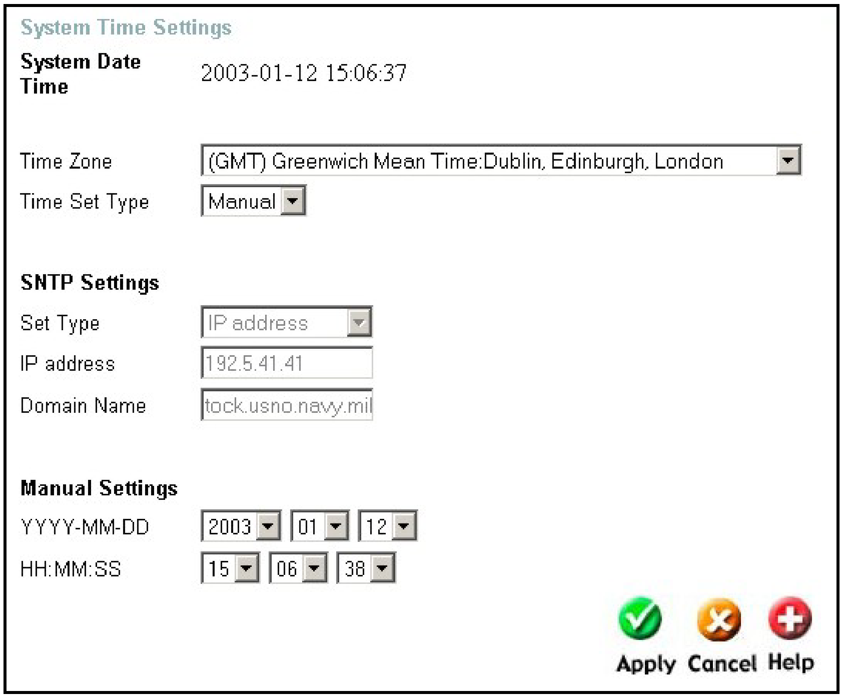
Add DMZ Host

DMZ host IP address: 192.168.1.100

DMZ host 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.

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 2003-01-12 15:06:37

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 12

HH:MM:SS 15 06 38

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.

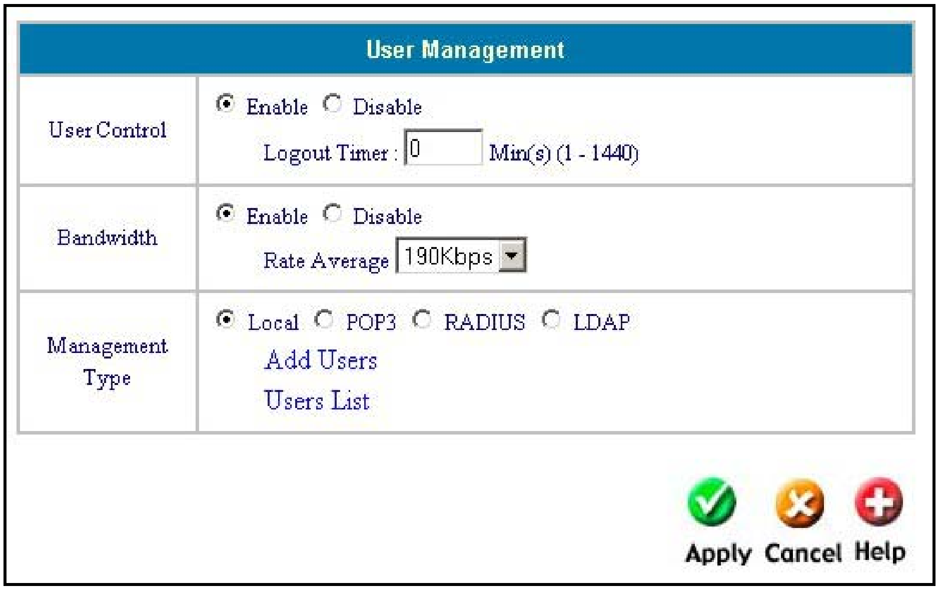
Authentication

The Authentication button opens the User Management page, as shown below. This page allows you to control how users on your LAN are authorized and to manage the bandwidth available to users on your LAN.

You can choose from the LDAP, POP3, RADIUS, Local, or 802.1X authentication protocols. In addition, you can enable or disable the user authentication without changing the configuration. This is useful when you are troubleshooting Internet access problems for PCs on your LAN.

Download from Www.Somanuals.com. All Manuals Search And Download.

Clicking the Enable click box, opposite the User Control table entry, will open the rest of the User Management page, including the Bandwidth control and Management Type table entries.

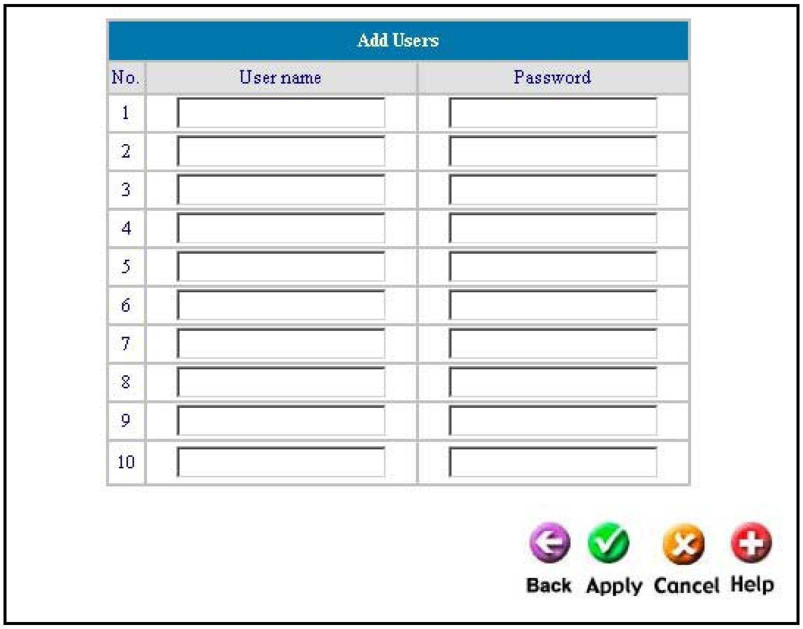


User Management	
User Control	● Enable ○ Disable Logout Timer : 0 Min(s) (1 - 1440)
Bandwidth	● Enable ○ Disable Rate Average 190Kbps
Management Type	● Local ○ POP3 ○ RADIUS ○ LDAP Add Users Users List

User Control	This allows you to enable or disable the authentication of users on the LAN side of the DFL-600, without changing the configuration settings. This is useful when you need to troubleshoot Internet access problems for PCs on your LAN.
Logout Timer	You can enter a maximum amount of time that users are allowed to be "logged in". When a user is logged in for a period of time longer than that specified here, they must log in again. Entering a '0' disables the logout timer.
Bandwidth	This allows you to enable or disable the bandwidth control feature of your DFL-600. Use the drop-down menu to set the maximum data rate that the DFL-600 will allow between PCs on your LAN and the WAN (the Internet).
Management Type	This allows you to choose and configure the protocol that the DFL-600 will use to authenticate users. You can choose between the **LDAP, POP3, RADIUS, Local**, or **802.1X** authentication protocols. The Local protocol means that the DFL-600 itself will provide user authentication, based on Usernames and Passwords that are entered by clicking the **Add Users** link. You can view the list of users by clicking the **Users List** link. The configuration of the other authentication protocols is described below.

Download from Www.Somanuals.com. All Manuals Search And Download.

Clicking the **Add Users** link will open the following page:



Add Users

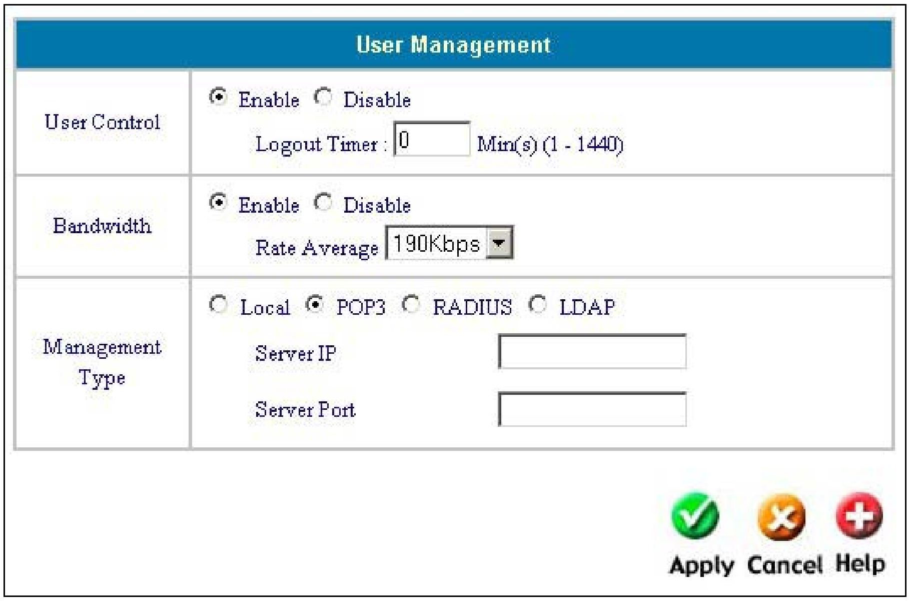
No.	User name	Password
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

Add Users	This allows you to add User names and Passwords for users on your LAN. In the **Local** mode, the DFL-600 authenticates users based upon the User name and Password entered here.
User name	Enter a **User name** here.
Password	Enter a **Password** corresponding to the User name entered above.

POP3

The Post Office Protocol, version 3 (POP3) is used to access and retrieve e-mail from a mailbox on a server that is usually located at your ISP’s facility. Choosing POP3 will allow the DFL-600 to connect PCs on your LAN to the POP3 e-mail server on the WAN to view and retrieve e-mail.

Clicking the **POP3** click box will open the following page:



User Management

User Control	● Enable ○ Disable Logout Timer : 0 Min(s) (1 - 1440)
Bandwidth	● Enable ○ Disable Rate Average 190Kbps
Management Type	○ Local ● POP3 ○ RADIUS ○ LDAP Server IP Server Port

POP3	The Post Office Protocol, version 3. This is used to view and retrieve e-mail from a POP3 server on the WAN.
Server IP	Enter the IP address of your POP3 server here. Your ISP should provide you with this address.
Server Port	This is the TCP port number that the POP3 server will use to communicate with PCs on your LAN. TCP port 110 is the 'well known' or default port used for the POP3 protocol.

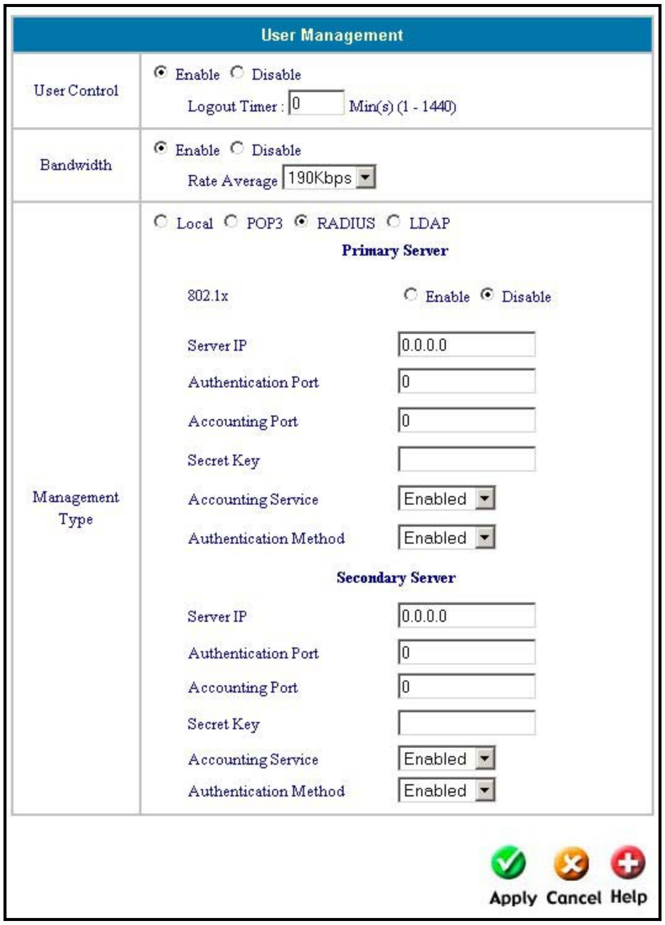
RADIUS

The Remote Access Dial-in User Service (RADIUS) is one of the most common protocols used to carry authorization, authentication, and configuration information between a RADIUS server on the WAN and PCs on your LAN. Choosing RADIUS will allow the DFL-600 to connect PCs on your LAN to a RADIUS server on the WAN. If RADIUS user authentication is enabled on the DFL-600, PCs on your LAN will require entering a Username and Password into the Windows Logon dialog box before they can access the Internet.

Download from Www.Somanuals.com. All Manuals Search And Download.

If you have some PCs (or other network devices) that do not require RADIUS user authentication to access the WAN (Internet), you can enable 802.1x, and then enter the IP Address and IP (subnet) Mask of these devices under the Edit link (which will appear when you enable 802.1x). PCs and network devices that have their IP Address and IP (subnet) Mask entered on the **802.1x Device Configuration** page will be allowed to access the WAN (Internet) by the DFL-600 without any RADIUS user authentication, effectively bypassing the RADIUS user authentication step.

Clicking the **RADIUS** click box will open the following page:



User Management

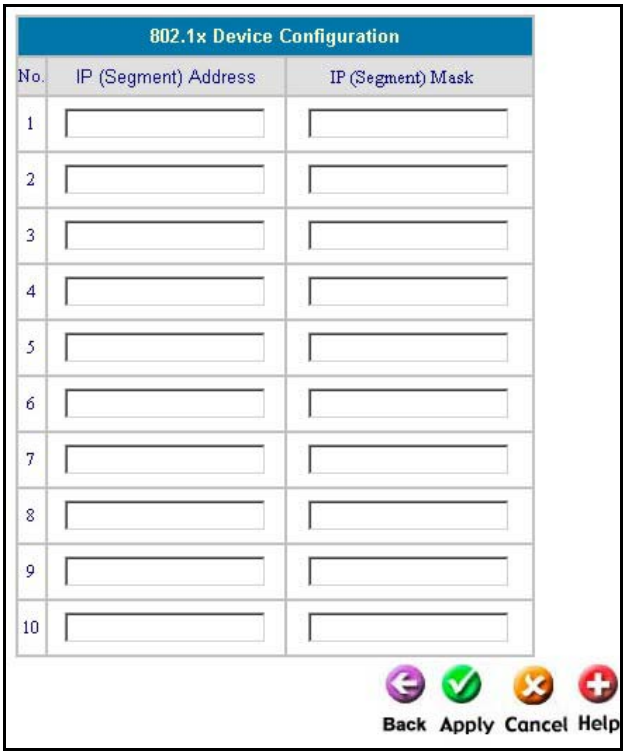
User Control	● Enable ○ Disable Logout Timer : 0 Min(s) (1 - 1440)
Bandwidth	● Enable ○ Disable Rate Average 190Kbps
Management Type	○ Local ○ POP3 ● RADIUS ○ LDAP **Primary Server** 802.1x ○ Enable ● Disable Server IP 0.0.0.0 Authentication Port 0 Accounting Port 0 Secret Key Accounting Service Enabled Authentication Method Enabled **Secondary Server** Server IP 0.0.0.0 Authentication Port 0 Accounting Port 0 Secret Key Accounting Service Enabled Authentication Method Enabled

RADIUS	The Remote Access Dial-in User Service (RADIUS) is one of the most common protocols used to carry authorization, authentication, and configuration information between a RADIUS server on the WAN and PCs on your LAN. Choosing RADIUS will allow the DFL-600 to connect PCs on your LAN to a RADIUS server on the WAN.
802.1X	802.1x is a standard for passing the Extensible Authentication Protocol (EAP) packets over a LAN. You should enable this if there are any 802.1x devices between the DFL-600 and the RADIUS server on the WAN. Clicking on the Edit link (which appears when you enable 802.1x) will open the **802.1x Device Configuration** page, as shown below. If you have PCs on your LAN that do not require RADIUS user authentication to access the Internet (or other networks through your ISP), you can use **Enable** 802.1x, and then click the **Edit** link. This will allow you to enter the IP Address and IP (subnet) Mask of PCs on your LAN that need to bypass the RADIUS user authentication. PCs (and network devices) whose IP Addresses and IP (subnet) Masks are entered on the **802.1x Device Configuration** page will be allowed to access the Internet without RADIUS user authentication.
Server IP	Enter the IP address of the RADIUS server on the WAN that you will use to authenticate users on your LAN. Your ISP should provide you with this address.
Authentication Port	Enter the TCP/UDP port number that the RADIUS server will use to connect to PCs on your LAN. The default port number for authentication is 1812.
Accounting Port	Enter the TCP/UDP port number that the

Download from Www.Somanuals.com. All Manuals Search And Download.

	RADIUS server will use to connect to PCs on your LAN for the RADIUS accounting function. The default port number for accounting is 1813.
Secret Key	Enter the shared key used between PCs on your LAN and the RADIUS server.
Accounting Service	Use the drop-down menu to enable or disable the RADIUS accounting service.
Authentication Method	Use the drop-down menu to enable or disable the RADIUS accounting service.

Clicking the 802.1x **Enable** click-box, and then **Edit** link will open the following page:



802.1x Device Configuration

No.	IP (Segment) Address	IP (Segment) Mask
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		

802.1x is a standard for passing the Extensible Authentication Protocol (EAP) packets over a LAN. You should enable this if there are any 802.1x devices between the DFL-600 and the RADIUS server on the WAN.

Download from Www.Somanuals.com. All Manuals Search And Download.

Clicking on the Edit link (which appears when you enable 802.1x) will open the **802.1x Device Configuration** page, as shown below.

If you have PCs on your LAN that do not require RADIUS user authentication to access the Internet (or other networks through your ISP), you can use **Enable** 802.1x, and then click the **Edit** link. This will allow you to enter the IP Address and IP (subnet) Mask of PCs on your LAN that need to bypass the RADIUS user authentication. PCs (and network devices) whose IP Addresses and IP (subnet) Masks are entered on the **802.1x Device Configuration** page will be allowed to access the Internet without RADIUS user authentication

Download from Www.Somanuals.com. All Manuals Search And Download.

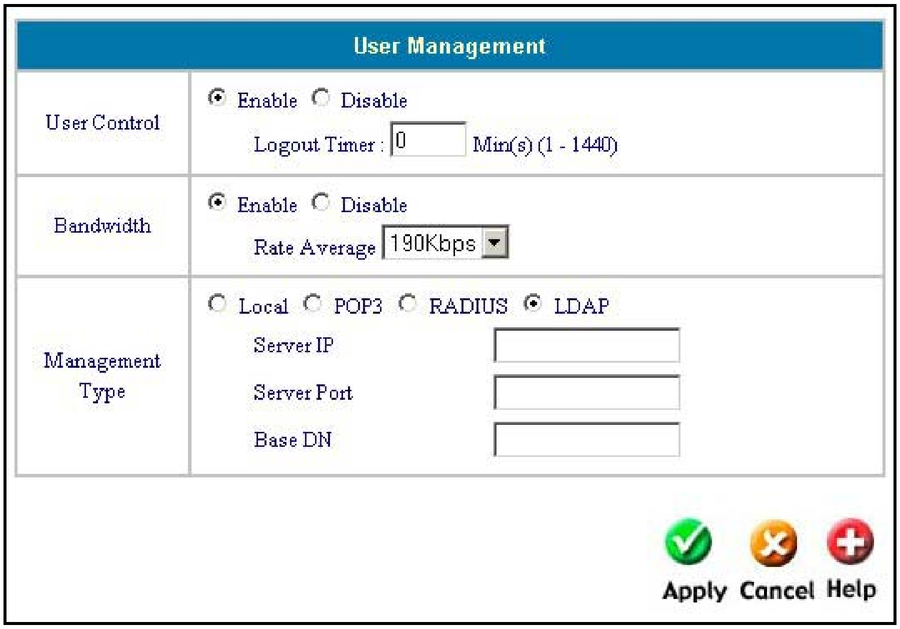
802.1X	802.1x is a standard for passing the Extensible Authentication Protocol (EAP) over a LAN. You should enable this only if there are 802.1x devices between the DFL-600 and the RADIUS server on the WAN. Clicking on the Edit link (which appears when you enable 802.1x) will open the **802.1x Device Configuration** page, as shown below. Use this table to enter the IP Address and IP Mask The DFL-600 supports only 802.1X pass through. This means that the DFL-600 will forward 802.1X packets from a RADIUS server on the WAN (Internet) to PCs on your LAN. If you enable 802.1X and do not enter the IP Address and IP Mask of a PC on your LAN in the 802.1x Device Configuration menu, that PC will not be allowed to access the Internet without being authorized by a RADIUS server. PCs on your LAN that have their IP Address and IP Mask entered into the 802.1x Device Configuration table, will be allowed to access the Internet without being authorized by a RADIUS server.
IP (Segment) Address	Enter the IP address of an 802.1x device between the DFL-600 and the RADIUS server on the WAN.
IP (Segment) Mask	Enter the subnet mask corresponding to the 802.1x device's IP address you entered above.

LDAP

LDAP (Lightweight Directory Access Protocol) serves as an *Internet phonebook*. When you are using e-mail programs, LDAP lets you lookup people's names and find their e-mail addresses, phone numbers, and office location. Of course, this assumes that you work inside a company or university where the net administrators have setup such a server for your use.

Download from Www.Somanuals.com. All Manuals Search And Download.

Clicking the **LDAP** click box will open the following page:



User Management

User Control	● Enable ○ Disable Logout Timer : 0 Min(s) (1 - 1440)
Bandwidth	● Enable ○ Disable Rate Average 190Kbps
Management Type	○ Local ○ POP3 ○ RADIUS ● LDAP Server IP Server Port Base DN

LDAP	
Server IP	Enter the IP address of your LDAP server here. Your ISP should provide you with this address.
Server Port	This is the TCP port number that the LDAP server will use to communicate with PCs on your LAN. Port 389 is the 'well known' or default port used for LDAP, while Secure LDAP uses port 636.
Base DN	This is the Distinguished Name used for LDAP.

Download from Www.Somanuals.com. All Manuals Search And Download.

Advanced Settings

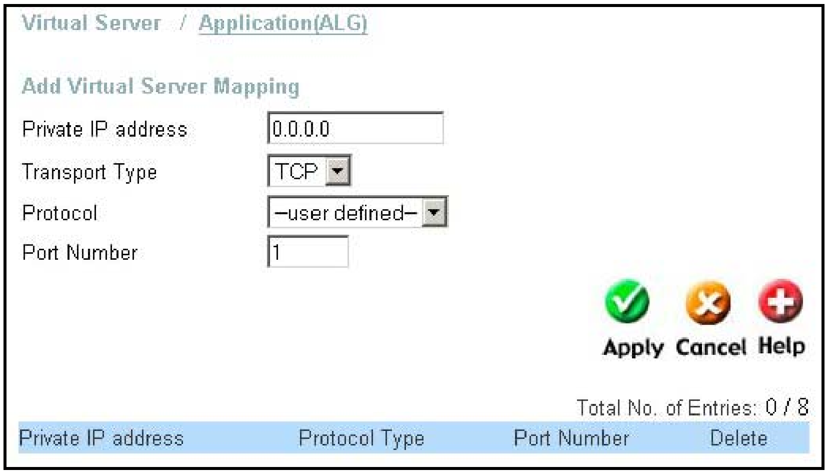
NAT

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.



Add Virtual Server Mapping

Private IP address	0.0.0.0
Transport Type	TCP
Protocol	–user defined–
Port Number	1

Total No. of Entries: 0 / 8

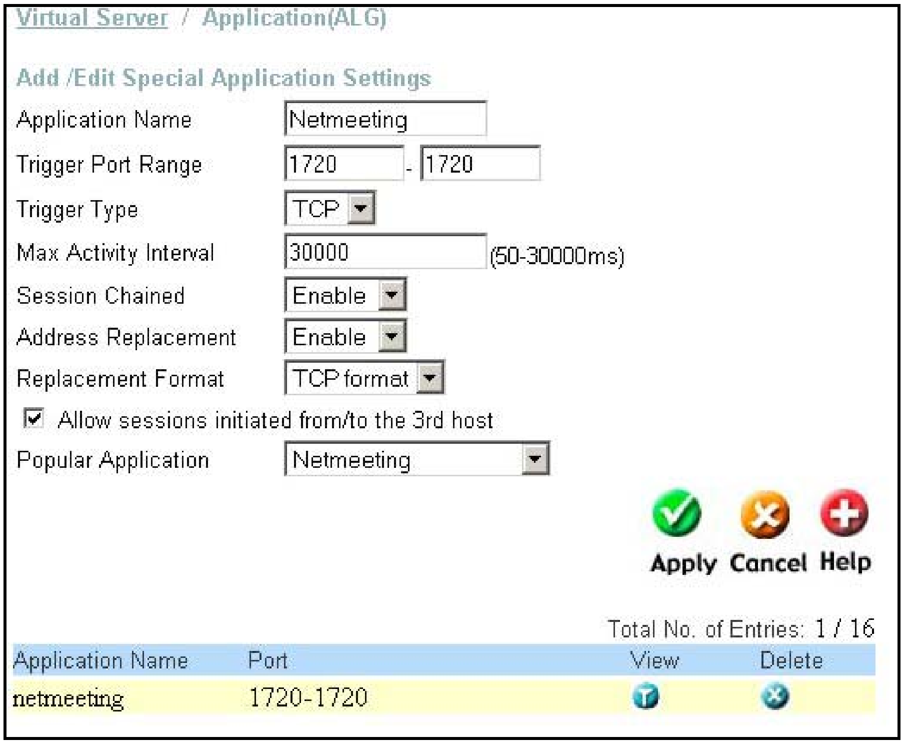
Private IP address	Protocol Type	Port Number	Delete

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

Application Gateway (ALG)

Some applications (programs running on a PC on your LAN) 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	Netmeeting
Trigger Port Range	1720 - 1720
Trigger Type	TCP
Max Activity Interval	30000 (50-30000ms)
Session Chained	Enable
Address Replacement	Enable
Replacement Format	TCP format

☑ Allow sessions initiated from/to the 3rd host

Popular Application: Netmeeting

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

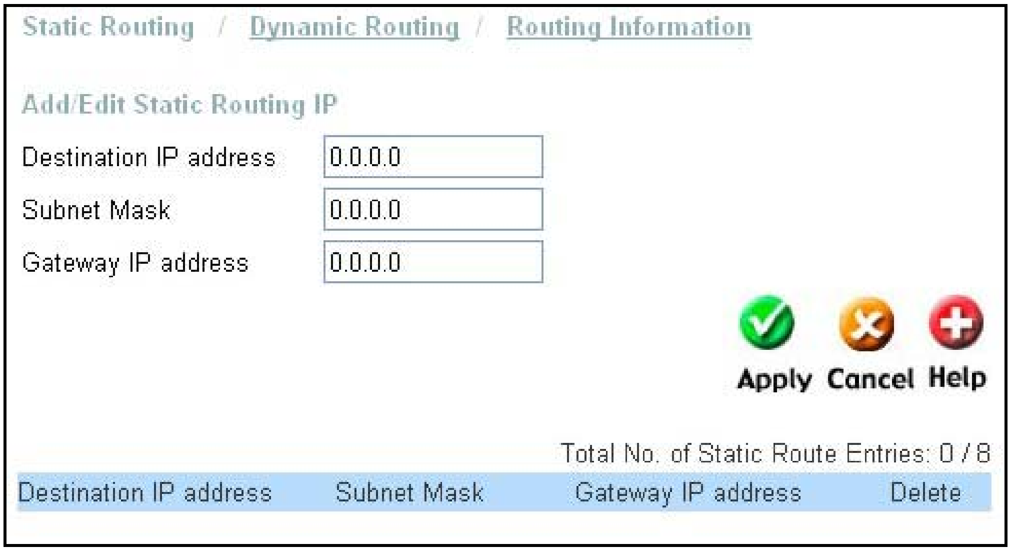
	single port, or a range of ports. If only a single port is used, enter the same port number in both the starting and ending port number fields.
Trigger Type	This is the protocol (TCP or UDP) that the application uses to make the connection.
Max Activity Interval	This is the maximum interval, in milliseconds, 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

Download from Www.Somanuals.com. All Manuals Search And Download.

	firmware and can be selected here from the drop-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.

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.



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

Total No. of Static Route Entries: 0 / 8

Destination IP address	Subnet Mask	Gateway IP address	Delete

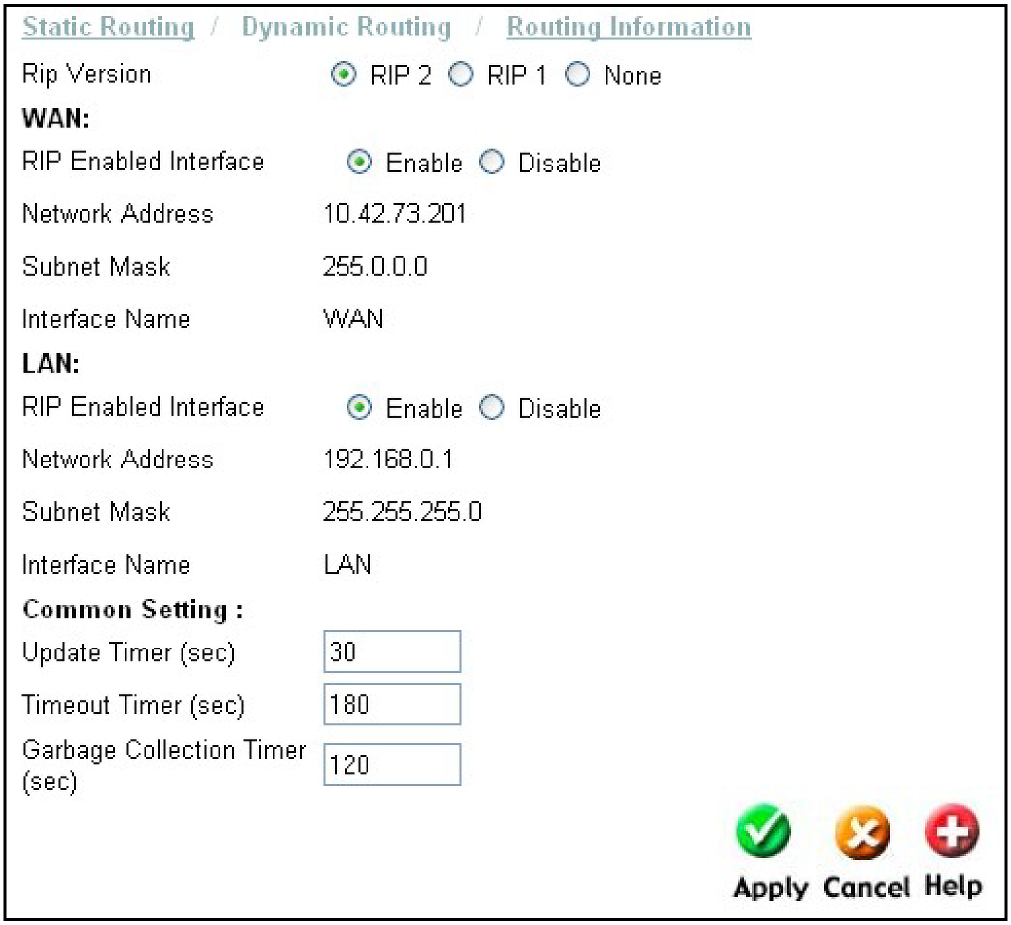
Download from Www.Somanuals.com. All Manuals Search And Download.

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.

Dynamic Routing

Your DFL-600 can automatically discover routes to destinations on both your LAN and the WAN (Internet). You can choose either **RIP1, RIP2** or **None**. RIP2 (Routing Information Protocol version 2) adds support for variable-length subnet masks, and is generally the best choice. Choosing **None** will disable the routing function of your router, as will choosing **Disabled** for the WAN or LAN RIP interface.

Download from Www.Somanuals.com. All Manuals Search And Download.



Rip Version ● RIP 2 ○ RIP 1 ○ None

WAN:

RIP Enabled Interface ● Enable ○ Disable

Network Address 10.42.73.201

Subnet Mask 255.0.0.0

Interface Name WAN

LAN:

RIP Enabled Interface ● Enable ○ Disable

Network Address 192.168.0.1

Subnet Mask 255.255.255.0

Interface Name LAN

Common Setting :

Update Timer (sec) 30

Timeout Timer (sec) 180

Garbage Collection Timer (sec) 120

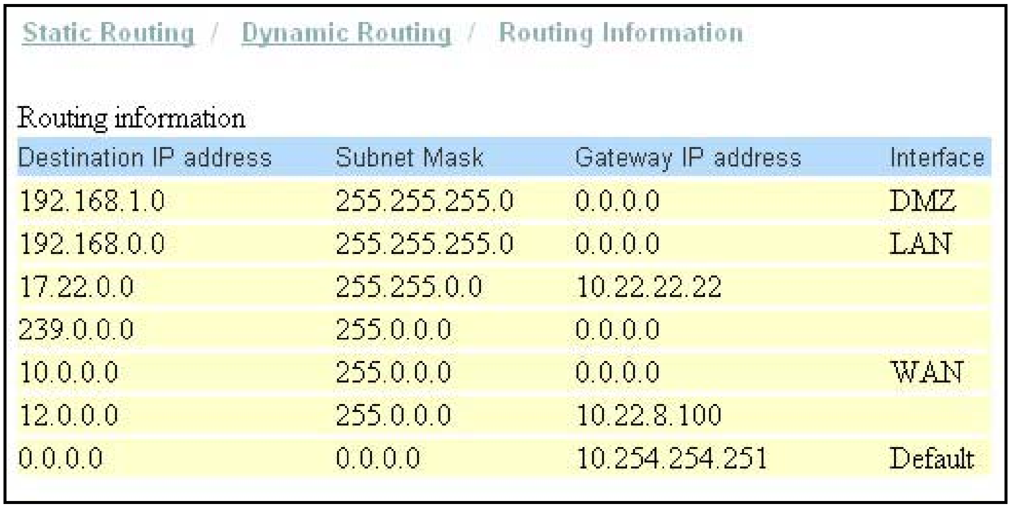
Rip Version	Your DFL-600 can automatically discover routes to destinations on both your LAN and the WAN (Internet). You can choose either **RIP1, RIP2** or **None**. RIP2 (Routing Information Protocol version 2) adds support for variable-length subnet masks, and is generally the best choice. Choosing **None** will disable the routing function of your router, as will choosing **Disabled** for the WAN or LAN RIP interface.
RIP Enabled Interface	These two click boxes allow you to enable or disable RIP for either the LAN or WAN interface. Choosing **Disabled** for the WAN or

	LAN RIP interface will disable the routing function of your router.
Network Address	This is the IP address of either the LAN or WAN side of your DFL-600.
Subnet Mask	This is the subnet mask corresponding to the Network Address above.
Interface Name	This is the name of the interface corresponding to the Network Address above.
Multicast Support	You can enable or disable multicast support. It is recommended that you enable this feature.
Update Timer	This allows you to specify how often the DFL-600 will update its routing table. The default is 30 seconds.
Timeout Timer	This allows you to specify how long a route discovered by the DFL-600 will remain in its memory without being used. The default is 180 seconds.
Garbage Collection Timer	This allows you to specify the period of time between the collection of garbage routes. The default is 120 seconds.

Routing Information

Your DFL-600 can automatically discover routes to destinations on both your LAN and the WAN (Internet), and you can also enter routing information statically. To display the **Routing Information** table, click on the **Routing Information** link. This information is displayed in the Routing Information table, as shown below.

Download from Www.Somanuals.com. All Manuals Search And Download.



Routing information

Destination IP address	Subnet Mask	Gateway IP address	Interface
192.168.1.0	255.255.255.0	0.0.0.0	DMZ
192.168.0.0	255.255.255.0	0.0.0.0	LAN
17.22.0.0	255.255.0.0	10.22.22.22	
239.0.0.0	255.0.0.0	0.0.0.0	
10.0.0.0	255.0.0.0	0.0.0.0	WAN
12.0.0.0	255.0.0.0	10.22.8.100	
0.0.0.0	0.0.0.0	10.254.254.251	Default

In the case shown above, the DFL-600's WAN port was connected to a 10.0.0.0 network – with a subnet mask of 255.0.0.0. The LAN ports used the default 192.168.0.0 network addresses, and the DMZ port used the default 192.168.1.0 network addresses – both with a subnet mask of 255.255.255.0.

The 0.0.0.0 IP address signifies the Broadcast address – the address within the DFL-600 where all packets that have an unknown destination address are forwarded. The DFL-600 then relates the 0.0.0.0 IP address to the WAN's gateway address of 10.254.254.251. This route is labeled as the **Default** route, and leads to the Internet.

Download from Www.Somanuals.com. All Manuals Search And Download.

Some Examples

Your DFL-600 allows you to make policy rules and then group these rules into a policy that will limit the types of access PCs on your LAN can have to the WAN (Internet). In addition, you can create a Schedule that will determine at what times and days of the week these policies are enforced. Finally, the DFL-600 offers a Global Policy Status page that allows you to enable or disable the filters that control what type of access to the WAN (Internet) PCs on your LAN can have, and what type of access to Virtual Servers and Application (ALGs) on your LAN can be granted to PCs on the WAN (Internet).

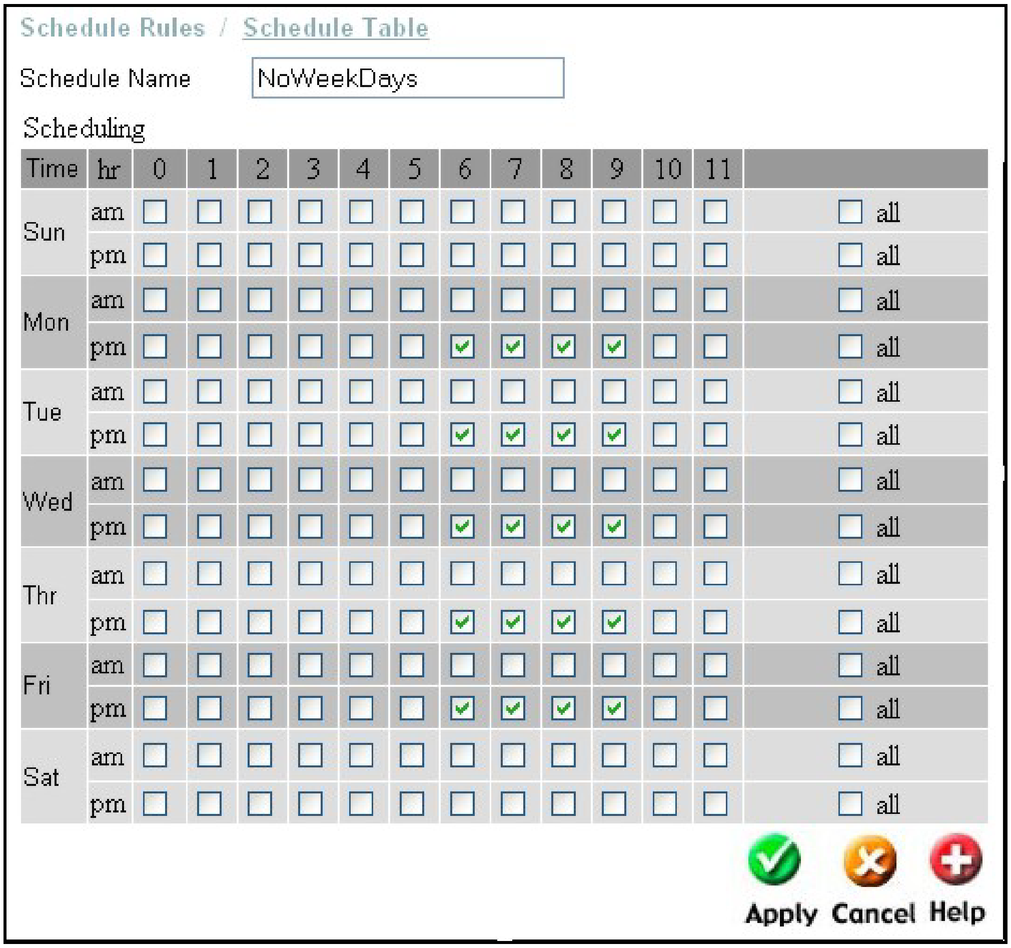
The DFL-600 offers many preset options for making these policies, and rather than describing them individually, a series of examples may be most informative.

Example 1 – Limiting Web-page Access

In this example, you will deny any PC on your LAN from accessing web-pages on the WAN (Internet) between the hours of 6 pm and 9 pm, Monday through Friday.

Setting the Schedule

Let's say that you are concerned that your children will access web-pages on the Internet when they should be studying or doing their homework. In this case, the schedule would be established first. To do this, click on the Schedule button to open the Schedule Rules page, as shown below.



Schedule Rules / Schedule Table

Schedule Name: NoWeekDays

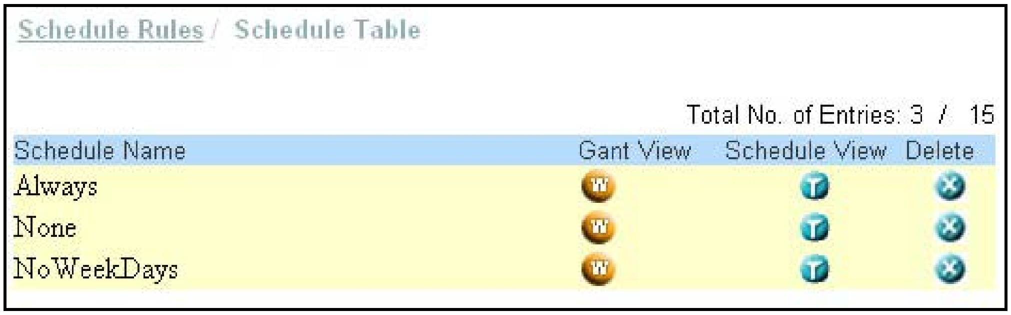
Scheduling

Time	hr	0	1	2	3	4	5	6	7	8	9	10	11	
Sun	am	□	□	□	□	□	□	□	□	□	□	□	□	□ all
	pm	□	□	□	□	□	□	□	□	□	□	□	□	□ all
Mon	am	□	□	□	□	□	□	□	□	□	□	□	□	□ all
	pm	□	□	□	□	□	□	☑	☑	☑	☑	□	□	□ all
Tue	am	□	□	□	□	□	□	□	□	□	□	□	□	□ all
	pm	□	□	□	□	□	□	☑	☑	☑	☑	□	□	□ all
Wed	am	□	□	□	□	□	□	□	□	□	□	□	□	□ all
	pm	□	□	□	□	□	□	☑	☑	☑	☑	□	□	□ all
Thr	am	□	□	□	□	□	□	□	□	□	□	□	□	□ all
	pm	□	□	□	□	□	□	☑	☑	☑	☑	□	□	□ all
Fri	am	□	□	□	□	□	□	□	□	□	□	□	□	□ all
	pm	□	□	□	□	□	□	☑	☑	☑	☑	□	□	□ all
Sat	am	□	□	□	□	□	□	□	□	□	□	□	□	□ all
	pm	□	□	□	□	□	□	□	□	□	□	□	□	□ all

A schedule called **NoWeekDays** has been entered with the hours between 6 pm and 9 pm checked for the weekdays Monday through Friday. Click on the **Apply** button to enter this schedule into the Schedule Table.

You can enter up to 15 Schedules, but two default schedules are automatically maintained by the DFL-600 – **Always** and **None**. You can make changes to the **None** Schedule, but the **Always** Schedule is intended for policies that should always be enforced.

To check the entered schedules, click the **Schedule Table** link. This will open the **Schedule Table**, as shown below.



Schedule Rules / Schedule Table

Total No. of Entries: 3 / 15

Schedule Name	Gant View	Schedule View	Delete
Always	W	T	✕
None	W	T	✕
NoWeekDays	W	T	✕

You can change the times and days entered for a Schedule by clicking on the link below the **Schedule View** heading. This will open the **Schedule Rules** page for the corresponding **Schedule Name**, and allow you to make changes.

Setting the Policy Rules

Now you need to configure the DFL-600 to block PCs on your LAN from accessing Web-pages on the WAN (Internet). To do this, click on the **Policy** button to open the **Policy Rules** page, as shown below.

Enter a name for this rule in the Rule Name field. This name is used to reference the **Policy Rule**. For this example, we will use **BlockWeb** for the policy rule name.

In order to block PCs on your LAN from downloading web-pages from the WAN (Internet), you need to select the HTTP (Hyper Text Transfer Protocol) from the **Protocol** drop-down menu. HTTP is the protocol that the World Wide Web uses to transfer web pages from the Internet to a PC on your LAN. The HTTP protocol uses TCP port 80 to make connections to PCs, but the necessary parameters for a **Policy Rule** are already entered when you select **http(80)** from the Protocol drop-down menu.

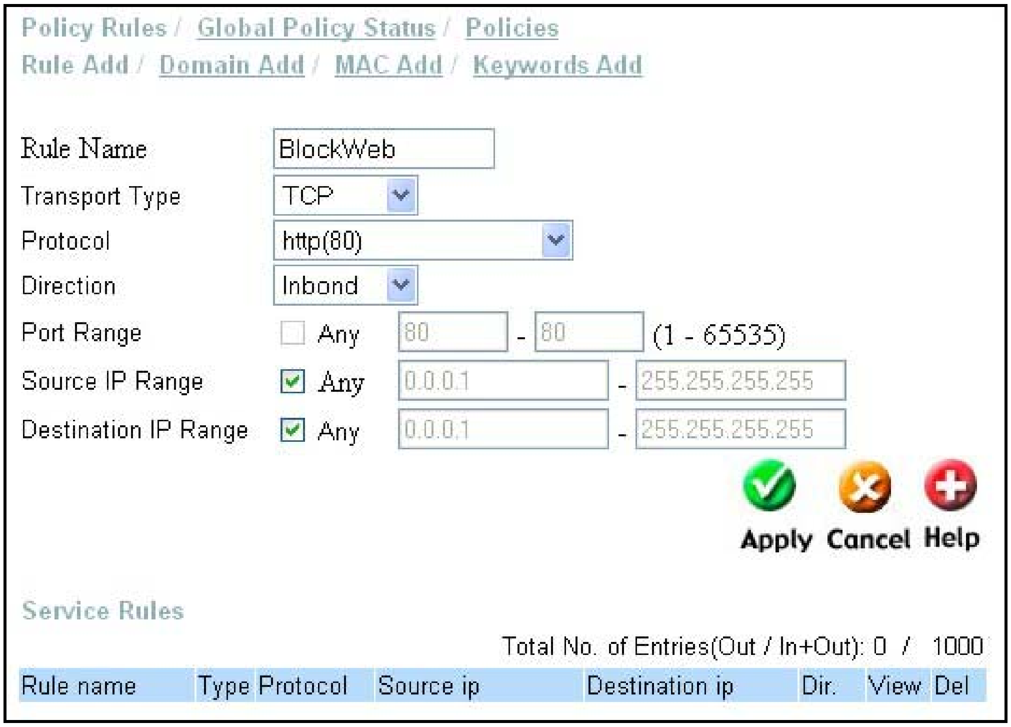
Most of the commonly used protocols on the Internet are already entered in the **Protocol** drop-down menu.

Next you need to specify the IP addresses of the possible sources of PCs on your LAN that this Policy Rule will apply to. You can specify any IP address range that may include all of the PCs on your LAN, or limit the IP address

Download from Www.Somanuals.com. All Manuals Search And Download.

range to PCs that you want the Policy Rule to apply to, and leave PCs with IP addresses outside the range free to access web-pages on the WAN (Internet).

For simplicity in this example, we are going to specify **Any** in both the **Source IP Range** and **Destination IP Range** fields. This will mean that any PC on your LAN will be denied access to web-pages on the WAN (Internet) regardless of that PC’s IP address.


Policy Rules / Global Policy Status / Policies
Rule Add / Domain Add / MAC Add / Keywords Add
Apply
Cancel
Help

Rule Name	BlockWeb		
Transport Type	TCP		
Protocol	http(80)		
Direction	Inbond		
Port Range	□ Any	80 - 80	(1 - 65535)
Source IP Range	☑ Any	0.0.0.1 - 255.255.255.255	
Destination IP Range	☑ Any	0.0.0.1 - 255.255.255.255	

Service Rules

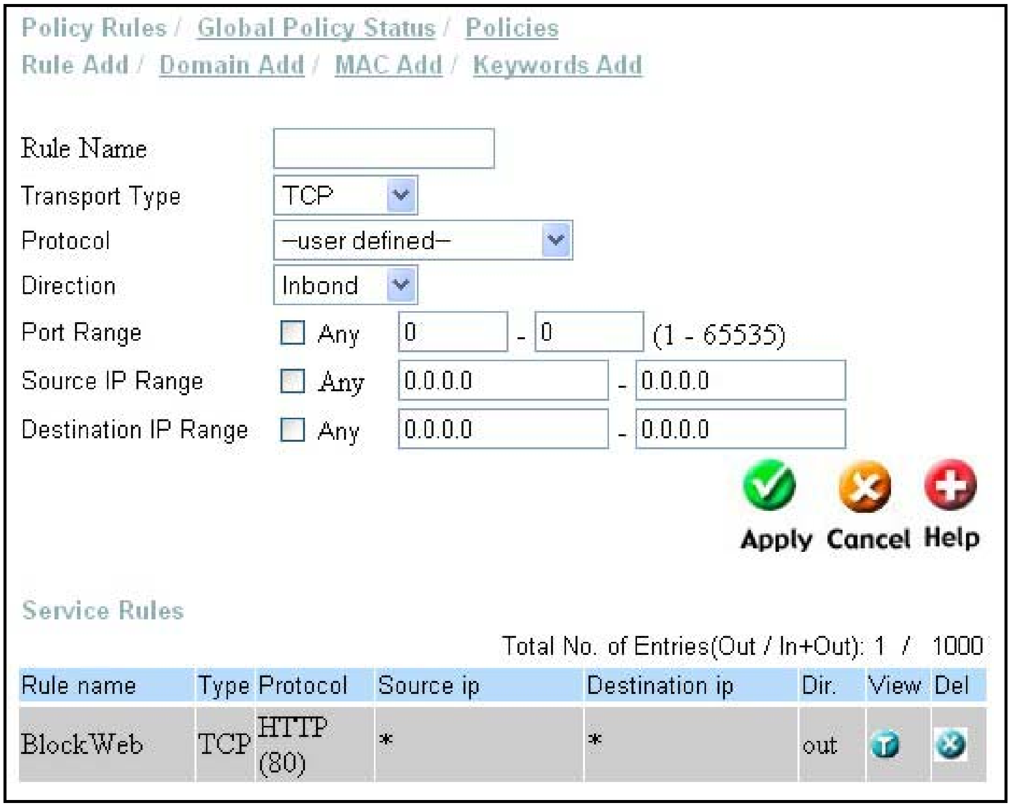
Total No. of Entries(Out / In+Out): 0 / 1000

Rule name	Type	Protocol	Source ip	Destination ip	Dir.	View	Del

Adding the Policy Rule to a Policy Group

After clicking the **Apply** button to add the **BlockWeb Policy Rule** to the **Service Rules** table, the page appears as shown below.

Download from Www.Somanuals.com. All Manuals Search And Download.



Policy Rules / Global Policy Status / Policies
Rule Add / Domain Add / MAC Add / Keywords Add

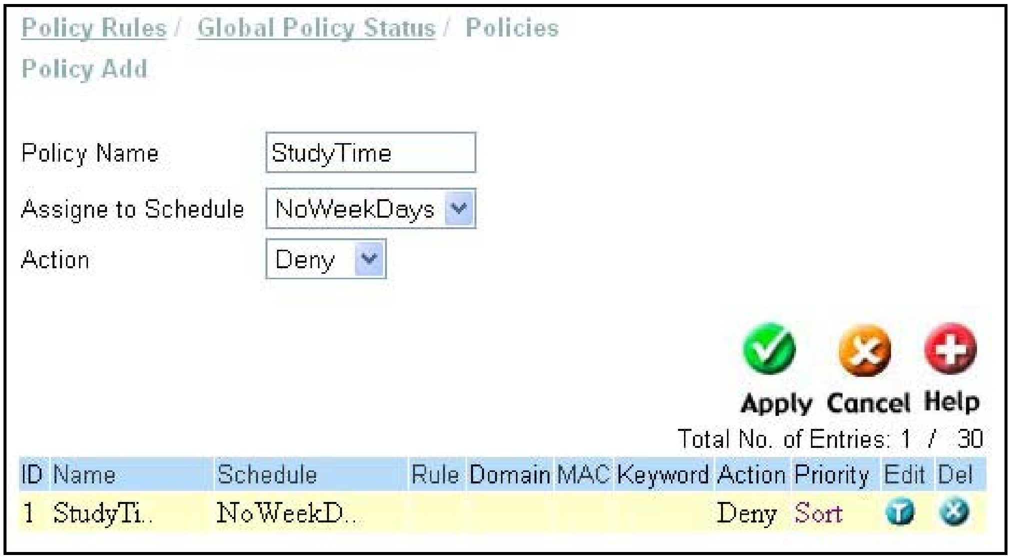
Rule Name			
Transport Type	TCP		
Protocol	–user defined–		
Direction	Inbond		
Port Range	□ Any	0 - 0	(1 - 65535)
Source IP Range	□ Any	0.0.0.0 - 0.0.0.0	
Destination IP Range	□ Any	0.0.0.0 - 0.0.0.0	

Service Rules

Total No. of Entries(Out / In+Out): 1 / 1000

Rule name	Type	Protocol	Source ip	Destination ip	Dir.	View	Del
BlockWeb	TCP	HTTP (80)	*	*	out		

Now that the **Policy Rule – Block Web –** is configured, we want to add this **Policy Rule** to a **Policy** group. Click on the **Policies** link to open the **Policy Add** page, as shown below.



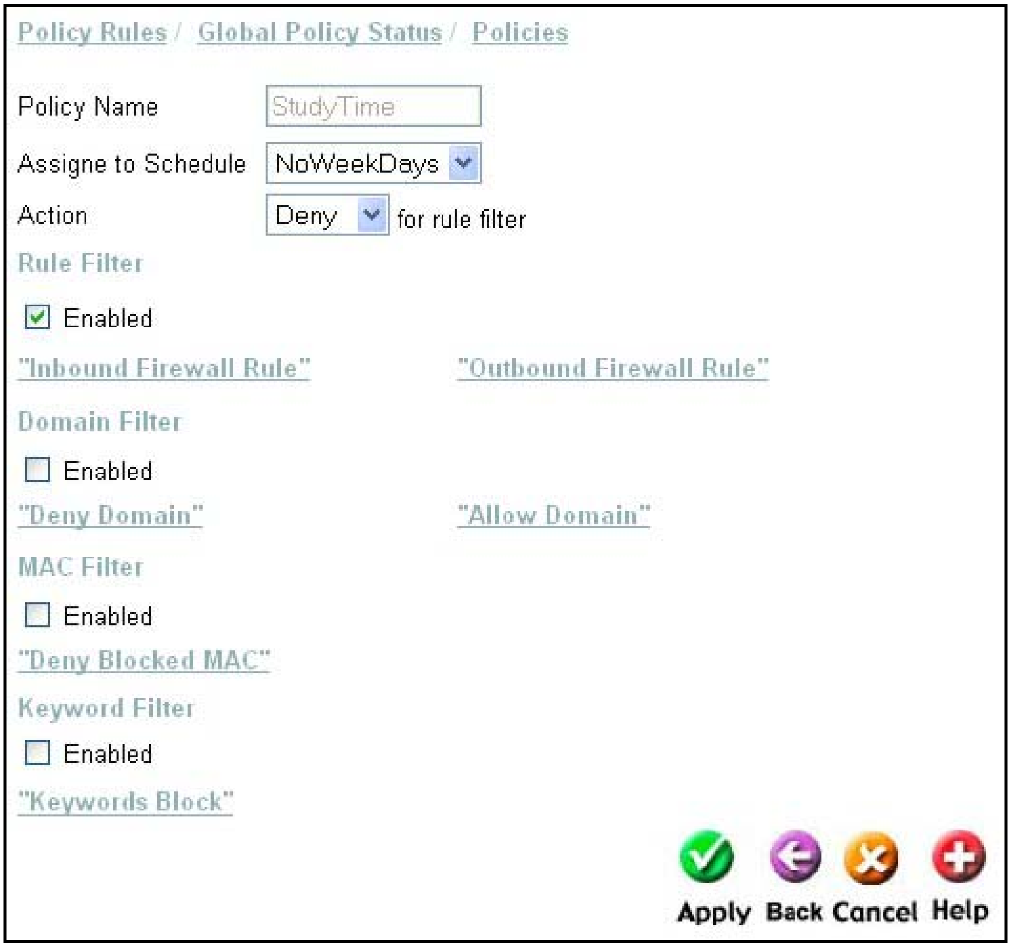
Policy Name	StudyTime
Assigne to Schedule	NoWeekDays
Action	Deny

Total No. of Entries: 1 / 30

ID	Name	Schedule	Rule	Domain	MAC	Keyword	Action	Priority	Edit	Del
1	StudyTi..	NoWeekD..					Deny	Sort		

Enter a name for the Policy group in the **Policy Name** field. This name will be used to reference this Policy group. In this case, we have named this Policy group **StudyTime**. The schedule we created previously will appear in the **Assign to Schedule** drop-down menu and is selected as the times and days of the weed this Policy will be enforced. We want to deny access to PCs on our LAN, so in the **Action** drop-down menu, we select **Deny**.

Clicking the Apply button will enter the Policy into the Policy group table, as shown above. Clicking on the icon under the Edit heading will open the following page.


Policy Rules / Global Policy Status / Policies

Policy Name StudyTime

Assigne to Schedule NoWeekDays

Action Deny for rule filter

Rule Filter

☑ Enabled

"Inbound Firewall Rule" "Outbound Firewall Rule"

Domain Filter

□ Enabled

"Deny Domain" "Allow Domain"

MAC Filter

□ Enabled

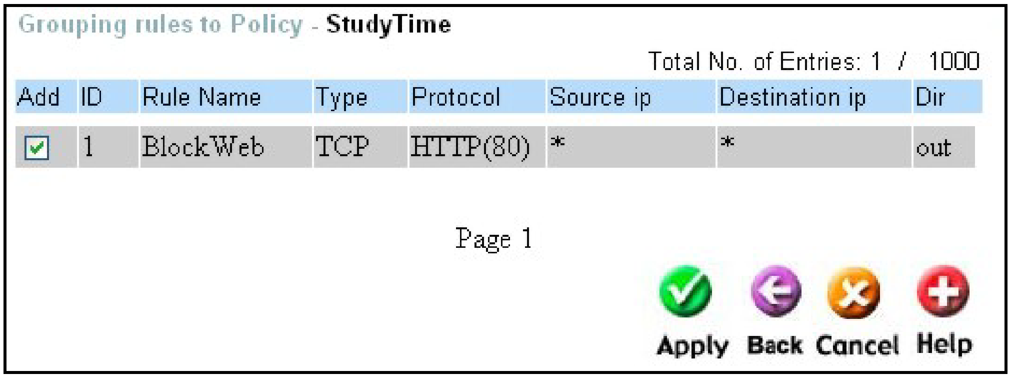
"Deny Blocked MAC"

Keyword Filter

□ Enabled

"Keywords Block"

Under the **Rule Filter** heading, click **Enabled**, and then click the **"Outbound Firewall Rule"** link. This will open a page that contains all of the **Policy Rules** that apply to **Outbound** packets, as shown below.


Grouping rules to Policy - StudyTime

Total No. of Entries: 1 / 1000

Add	ID	Rule Name	Type	Protocol	Source ip	Destination ip	Dir
☑	1	BlockWeb	TCP	HTTP(80)	*	*	out

Page 1

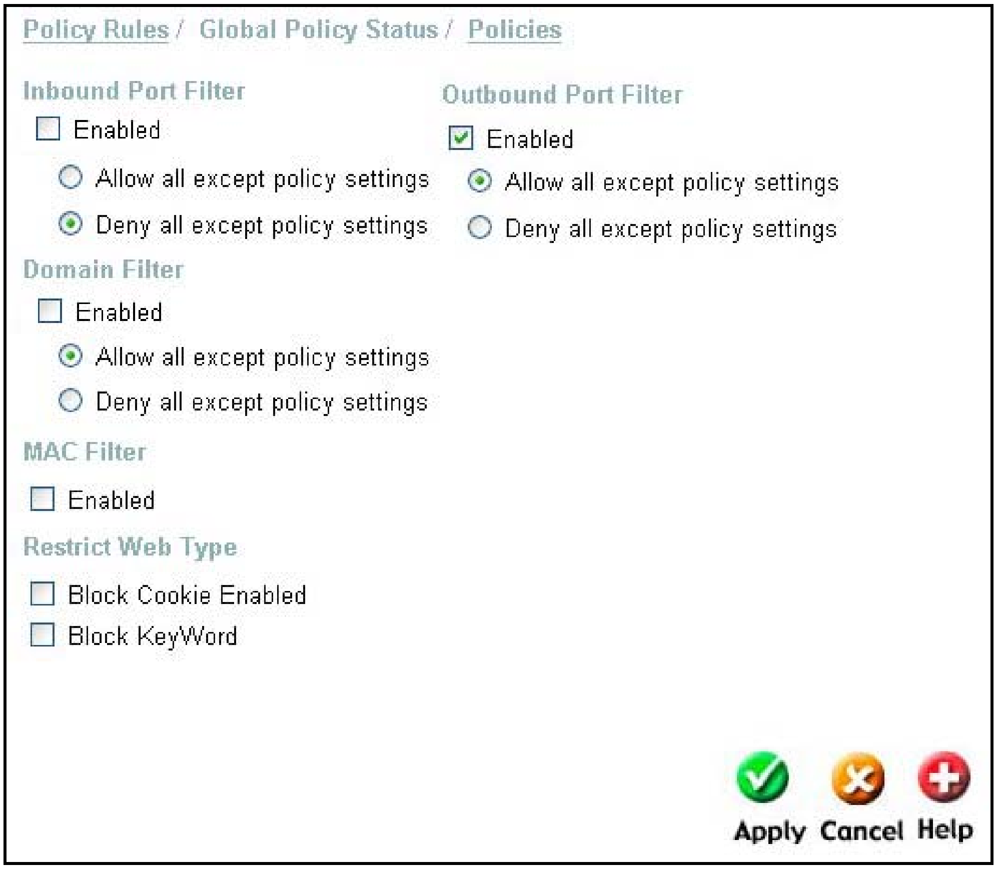
Click the box under the **Add** heading to add the **BlockWeb** Policy Rule to the **StudyTime** Policy group. Click the **Apply** button to make the entry current.

Click the Back button to return to the **Policy Add** page.

Setting the Policy Global Status

Now we need to configure the **Global Policy Status**. Click the **Global Policy Status** link – from the **Policy Add** page – to open the following page.

Download from Www.Somanuals.com. All Manuals Search And Download.


Policy Rules / Global Policy Status / Policies

Inbound Port Filter

☐ Enabled

○ Allow all except policy settings

● Deny all except policy settings

Domain Filter

☐ Enabled

● Allow all except policy settings

○ Deny all except policy settings

MAC Filter

☐ Enabled

Restrict Web Type

☐ Block Cookie Enabled

☐ Block KeyWord

Outbound Port Filter

☑ Enabled

● Allow all except policy settings

○ Deny all except policy settings

For the **BlockWeb** Policy Rule and the **StudyTime** Policy group, we need to set the **Outbound Port Filter** to **Enabled** – by clicking the **Enabled** click-box – and to select the **Allow all except policy settings** option. When **Allow all except policy settings** is selected, the DFL-600 will drop (filter) packets that meet the criteria established in the Policy Rules (in this case, HTTP packets). All other packets will be forwarded to their destination. If we had selected **Deny all except policy settings**, then the DFL-600 would forward only HTTP packets. All other packet types would be dropped (filtered).

This Policy configuration will block HTTP packets (using TCP port 80 – the default port number for the HTTP protocol) from being sent from PCs on your LAN to the WAN (Internet) between the hours of 6 pm and 9 pm and the weeddays Monday through Friday. This will effectively block access to the Internet from PCs on your LAN during these times.

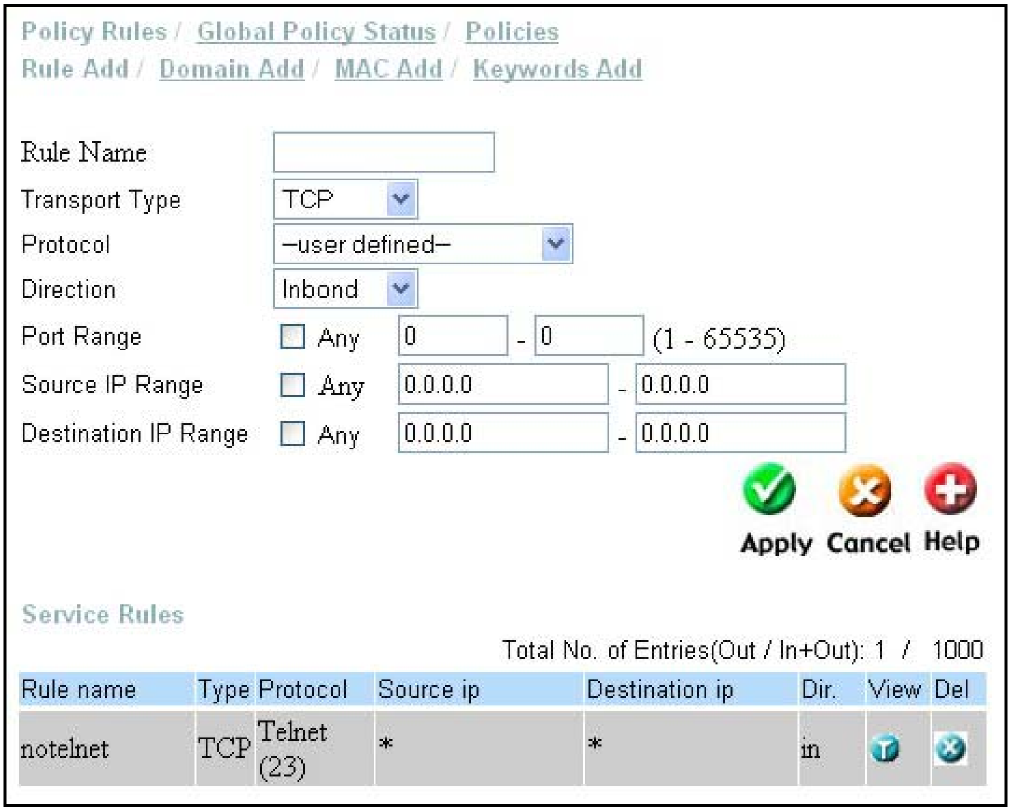
Remember to save the Policy configuration into the DFL-600's non-volatile RAM using the **Save** button (under the **Tools** tab, click the **System** button to see the **Save** options). This will ensure that the DFL-600 will retain the Policy configurations when it is restarted or if the AC power is interupted.

Example 2 – Limiting Access to Internet Domains

Policy Rules

The DFL-600 allows you to specify rules that it will use to limit access (filter packets) to and from PCs on your LAN. A policy rule on the DFL-600 establishes what information packets must contain before an action is taken by the router. The action taken when a packet is read by the DFL-600 is specified on the subsequent web pages, described below. To configure a policy rule, click on the **Policy** button to open the **Policy Rules** page, as shown below.

Download from Www.Somanuals.com. All Manuals Search And Download.



Policy Rules / Global Policy Status / Policies
Rule Add / Domain Add / MAC Add / Keywords Add

Rule Name		
Transport Type	TCP	
Protocol	–user defined–	
Direction	Inbond	
Port Range	□ Any	0 - 0 (1 - 65535)
Source IP Range	□ Any	0.0.0.0 - 0.0.0.0
Destination IP Range	□ Any	0.0.0.0 - 0.0.0.0

Service Rules

Total No. of Entries(Out / In+Out): 1 / 1000

Rule name	Type	Protocol	Source ip	Destination ip	Dir.	View	Del
notelnet	TCP	Telnet (23)	*	*	in		

Enter a name for the policy rule you want to configure in the **Rule Name** field. This name will appear in the **Service Rules** table, along with all of the parameters you specify for the rule, and is used to identify and reference the rule on subsequent web pages, as described below.

In the case shown above, a rule called **notelnet** has been entered to block telnet packets from coming in from the WAN to the LAN. The rule was constructed using the **Protocol** drop-down menu, and then selecting the **telnet(23)** entry to specify the TELNET protocol, TCP transport type, and TCP port number 23. Most of the commonly used protocols on the Internet are listed in the **Protocol** drop-down menu. Their transport types and port numbers are automatically entered, when you select one of these protocols. If you need to configure a policy rule for a protocol that is not listed, you can manually enter the **Transport Type,** and **Port Range** in the appropriate fields. For this type of policy rule, the **Protocol** is listed as **–user defined-**.

The next step is to specify if you want the policy rule to apply to **Inbound** or **Outbound** packets. Inbound here means from the WAN to your LAN, while Outbound means from your LAN to the WAN. The **Direction** drop-down menu allows you to choose which direction the DFL-600 will filter packets that meet the criteria of the policy rule.

Please Note: at the time of the writing of this manual, the **Inbound** direction specification for **Policy Rules** only applies to the **Application (ALGs)** and **Virtual Servers** that have been set up on the **NAT** page.

If, for example, you want to prevent the TELNET protocol from being used to access PCs on your LAN from the Internet (WAN), your would specify **Inbound**. If you want to prevent PCs on your LAN from using TELNET to access PCs on the Internet (WAN), you would specify **Outbound**. Entering two policy rules for inbound and outbound packets will totally eliminate a given protocol from being used to across the DFL-600.

You can specify a range of TCP or UDP ports using the **Port Range** field. Selecting **Any** will prevent any port from being used.

In addition, you can specify a range of IP addresses – as either a source or a destination – that the policy rule will be applied to.

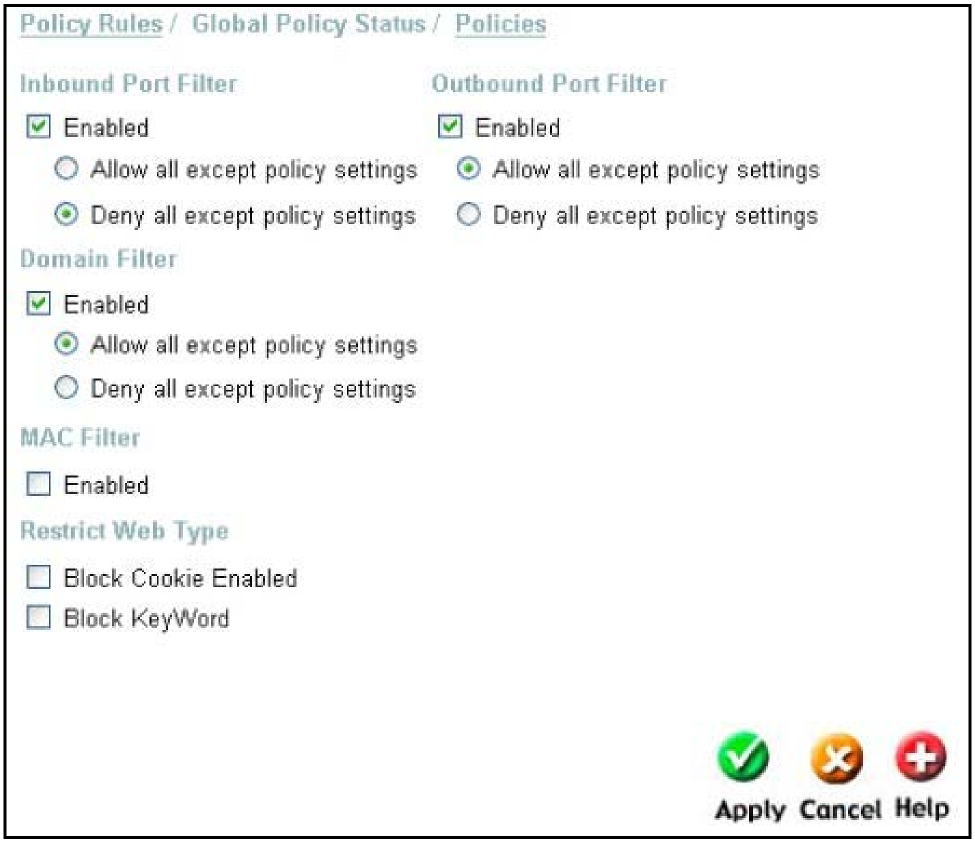
Once you have configured the policy rule and clicked on the **Apply** button, the rule will be entered into the **Service Rules** table. If you need to change the policy rule, click on the icon in the **View** field of the **Service Rules** table. This will allow you to view and modify the rule's configuration. To delete a policy rule, click on the icon in the **Del** field.

Global Policy Status

Once you have configured the Policy Rules, you need to determine how the DFL-600 will apply these rules to the packets that cross between your LAN and the Internet (WAN). The Global Policy Status page enables you to specify this.

"Default" on this page means "if no packets that meet the criteria established in the policy rules, then ..." either "allow all" or "deny all". On the Global

Policy Status page, "**Default allow all**" means that the DFL-600 will allow all packets except those that meet the criteria established in the policy rules. "**Default deny all**" means that the DFL-600 will deny (filter) all packets except those that meet the criteria established in the policy rules.



Policy Rules / Global Policy Status / Policies

Inbound Port Filter

☑ Enabled

○ Allow all except policy settings

● Deny all except policy settings

Outbound Port Filter

☑ Enabled

● Allow all except policy settings

○ Deny all except policy settings

Domain Filter

☑ Enabled

● Allow all except policy settings

○ Deny all except policy settings

MAC Filter

☐ Enabled

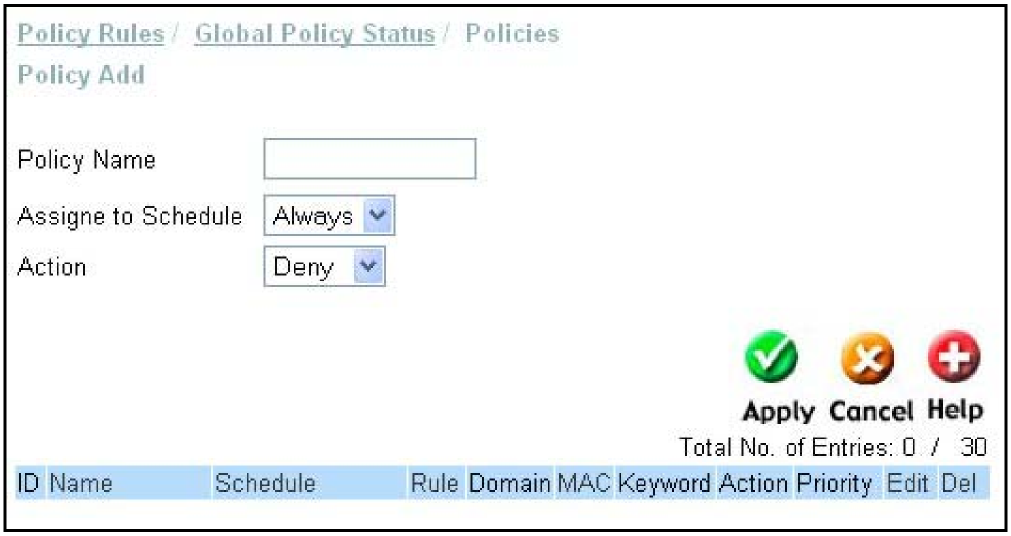
Restrict Web Type

☐ Block Cookie Enabled

☐ Block KeyWord

Policies – Policy Add

Once you have defined what type of packets you want the DFL-600 to look for, you need to assign those rules to a policy. Clicking on the **Policies** link will open the **Policy Add** page, as shown below.



Policy Name

Assigne to Schedule: Always

Action: Deny

Total No. of Entries: 0 / 30

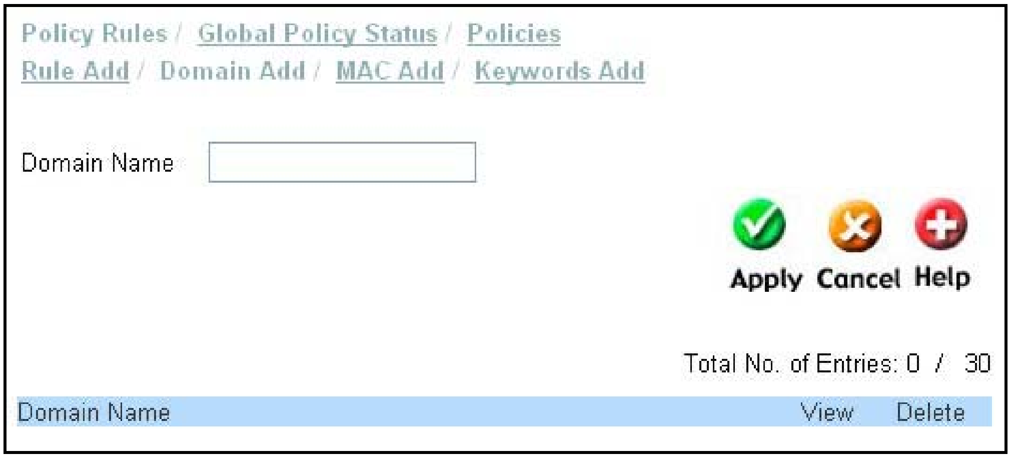
ID	Name	Schedule	Rule	Domain	MAC	Keyword	Action	Priority	Edit	Del

Enter a name for the new group of policy rules in the Policy Name field. This name is used to reference the group of policy rules. You can also assign this group of policy rules to a schedule (which is either **Always** or a schedule you can create below). Finally, you can choose to **Allow** or **Deny** access.

Blocking Internet Domains

The DFL-600 will allow you to make a list of Domain names for which packets will be filtered.

Clicking on the **Domain Add** link on the **Policy Rules** page will open the following page.

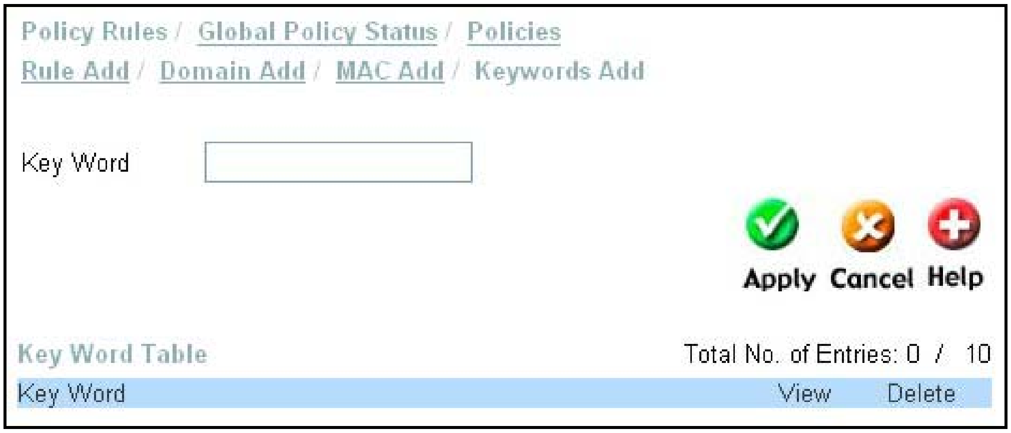

Policy Rules / Global Policy Status / Policies
Rule Add / Domain Add / MAC Add / Keywords Add
Domain Name
Apply
Cancel
Help
Total No. of Entries: 0 / 30
Domain Name
View
Delete

Enter a domain name you want to limit access to in the **Domain Name** field. Click the **Apply** button to add this domain name to the list.

Blocking Keywords

The DFL-600 will allow you to make a list of keywords for which packets will be filtered

Clicking on the **Keywords Add** link on the **Policy Rules** page will open the following page.

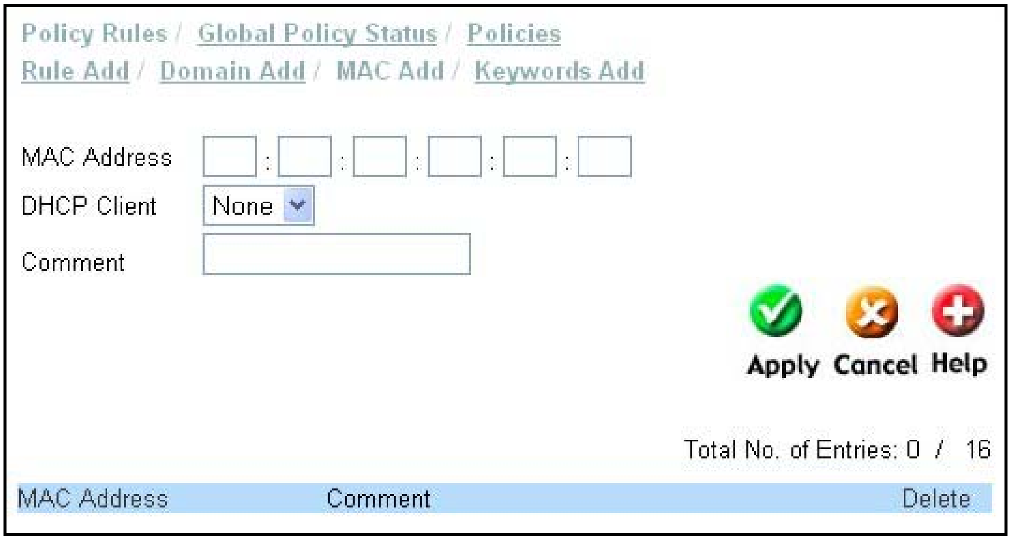

Policy Rules / Global Policy Status / Policies
Rule Add / Domain Add / MAC Add / Keywords Add
Key Word
Apply
Cancel
Help
Key Word Table
Total No. of Entries: 0 / 10
Key Word
View
Delete

Enter a key word you want the DFL-600 to examine packets for in the **Key Word** field. Click the **Apply** button to enter this key word into the list.

Blocking MAC Addresses

The DFL-600 will allow you to make a list of MAC addresses for which packets will be filtered. MAC (Media Access Control) addresses are the physical addresses that are assigned to networking devices by their respective manufacturers. These addresses are 12 hexadecimal digits long and are in the form 01-23-45-67-89-AB – where the numerals 0-9 and the letters A-F are used.

Clicking on the **MAC Add** link on the **Policy Rules** page will open the following page.


Policy Rules / Global Policy Status / Policies
Rule Add / Domain Add / MAC Add / Keywords Add
Apply
Cancel
Help

MAC Address ___ : ___ : ___ : ___ : ___ : ___

DHCP Client None

Comment

Total No. of Entries: 0 / 16

MAC Address	Comment	Delete

Enter a **MAC Address** that you want the DFL-600 to scan for and filter packets that have that MAC address as their destination address. Click the **Apply** button to enter the MAC address into the table.

Download from Www.Somanuals.com. All Manuals Search And Download.

IPSec Settings

IPSec (IP Secure) is a group of IP extensions developed by the Internet Engineering Task Force (IETF) to provide security services that are compatible with the existing IP standard. IPSec provides authentication, integrity, access control, and confidentially. The data and information exchanged between two ends of an IPSec connection can be encrypted and verified. Virtual Private Network (VPN) Tunnels can be created to allow encrypted and secured communication across networks or the Internet.

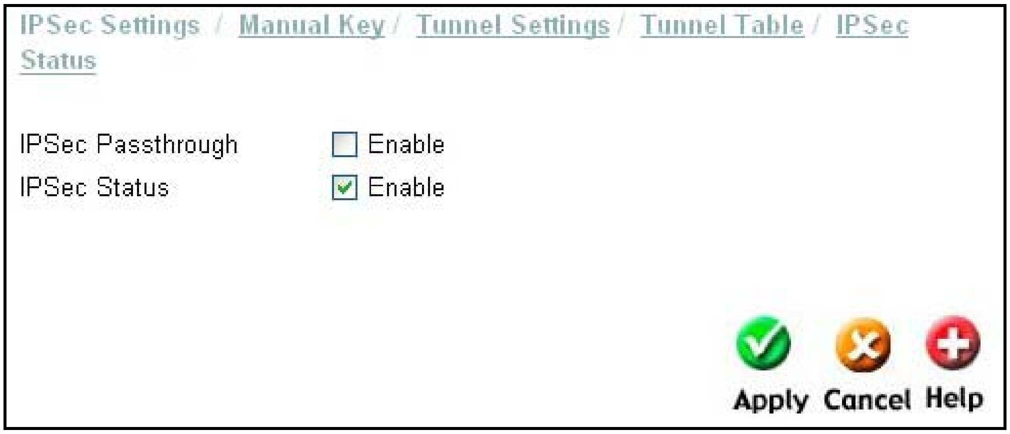
The two protocols provided by IPSec are Authentication Header (AH) and Encapsulated Security Payload (ESP).

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 security level. 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.

The DFL-600 can be configured to either establish and maintain an IPSec connection with a remote workstation, or to simply allow the IPSec packets to pass through it. The **IPSec Passthrough** mode allows the IPSec packets to be forwarded to a PC on the LAN side of the DFL-600. This PC should then have the appropriate software running on it to establish and maintain the IPSec connection.

To enable **IPSec Passthrough**, click on the **VPN-IPSec** button to open the **IPSec Settings** page, as shown below.

Download from Www.Somanuals.com. All Manuals Search And Download.


IPSec Settings / Manual Key / Tunnel Settings / Tunnel Table / IPSec Status
Apply
Cancel
Help

IPSec Passthrough □ Enable

IPSec Status ☑ Enable

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.

Manual Key Settings

There are two methods for exchanging the encryption/decryption keys required by IPSec – Manual Key entry and Internet Key Exchange (IKE). The difference between Manual Key and IKE is how the encryption keys and SPI are determined. For a Manual Key VPN, the encryption key, authentication key (if required) and SPIs are predetermined by a Network Administrator when configuring the connection.

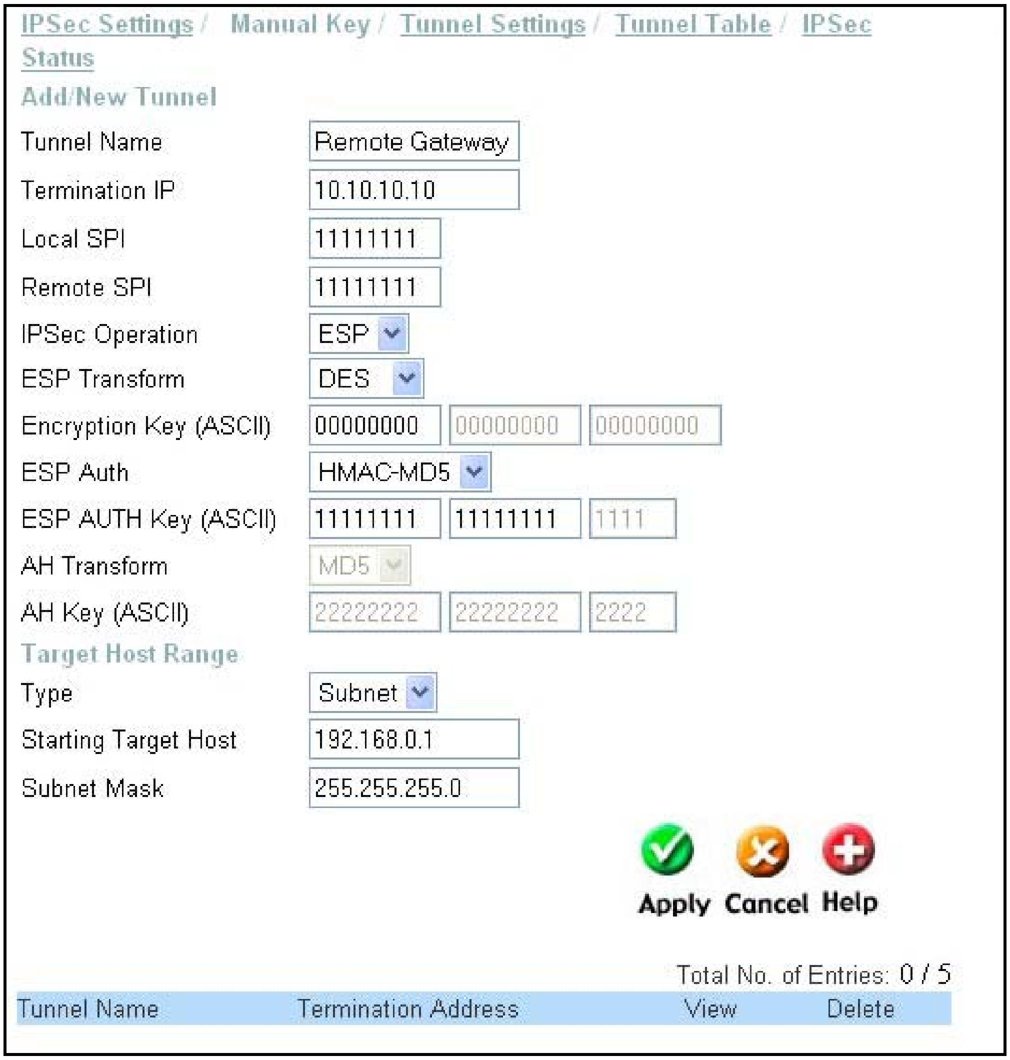
The differences between Manual Key and IKE can be summarized as:

- Manual Key VPN requires the encryption key, authentication key (if required), and SPIs to be predetermined by a network administrator when the IPSec connection is configured.
- For an IKE VPN, the keys and SPIs are negotiated between VPN gateways. The two VPN gateways can then use these keys and

SPIs to maintain the IPSec connection.

An IKE VPN is generally considered more secure than a Manual Key VPN because IKE can generate new keys and SPIs randomly during the negotiation phase.

To configure a Manual Key VPN, click the **Manual Key** link to open the page shown below.


IPSec Settings / Manual Key / Tunnel Settings / Tunnel Table / IPSec Status
Apply
Cancel
Help

Add/New Tunnel

Tunnel Name	Remote Gateway		
Termination IP	10.10.10.10		
Local SPI	11111111		
Remote SPI	11111111		
IPSec Operation	ESP		
ESP Transform	DES		
Encryption Key (ASCII)	00000000	00000000	00000000
ESP Auth	HMAC-MD5		
ESP AUTH Key (ASCII)	11111111	11111111	1111
AH Transform	MD5		
AH Key (ASCII)	22222222	22222222	2222

Target Host Range

Type	Subnet
Starting Target Host	192.168.0.1
Subnet Mask	255.255.255.0

Total No. of Entries: 0 / 5

Tunnel Name	Termination Address	View	Delete

Download from Www.Somanuals.com. All Manuals Search And Download.

Add/New Tunnel	The following fields will identify the Manual Key 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.
Local SPI	Refers to the SPI of your DFL-600 when establishing a VPN tunnel.
Remote SPI	Refers to the SPI of the remote peer toward which the VPN tunnel will be established.
IPSec Operation	This drop-down menu allows you to select the kind of encryption that will be applied to packets that are sent between the two endpoints of a VPN tunnel. **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). **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.

Download from Www.Somanuals.com. All Manuals Search And Download.

ESP Transform	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. You can choose between **Null** – no encryption, **DES** – using DES encryption, and **3DES** – using triple DES encryption. You must select the exact same ESP transform (encryption algorithm) on both ends of a VPN tunnel.
Encryption Key (ASCII)	Enter the predetermined alphanumeric Encryption key. The length of the key will vary depending upon the choice of ESP transform made in the drop-down menu above. You must select the exact same Encryption key on both ends of a VPN tunnel.
ESP Auth	This drop-down menu allows you to select the authentication method that will be used when **ESP** is selected in the **IPSec Operation** drop-down menu above. You can choose between **Null** – no authorization, **MD5** – using MD5 message digest authentication, and **SHA** – using the SHA authentication method. You must select the exact same ESP authentication method on both ends of a VPN tunnel.
ESP Auth Key (ASCII)	Enter the predetermined alphanumeric ESP Authentication key. The length of the key will vary depending upon the choice of ESP Authentication in the drop-down menu above. You must select the exact same ESP

Download from Www.Somanuals.com. All Manuals Search And Download.

	Authentication key on both ends of a VPN tunnel.
AH Transform	This drop-down menu allows you to select the authentication method that will be used when **AH** is selected in the **IPSec Operation** drop-down menu above. You can choose between **MD5** – using MD5 message digest authentication, and **SHA** – using the SHA authentication method. You must select the exact same AH authentication method on both ends of a VPN tunnel.
AH Auth Key (ASCII)	Enter the predetermined alphanumeric AH Authorization key. The length of the key will vary depending upon the choice of AH Transform in the drop-down menu above. You must select the exact same AH Authorization key on both ends of a VPN tunnel
Type	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.
Starting Target Host	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 192.168.2.1 to 192.168.2.254 will be allowed to access the VPN. Note that the IP addresses192.168.2.0 and 192.168.2.255 are reserved for use on the remote network.

Subnet Mask	Enter the subnet mask corresponding to the IP address range entered above.

Tunnel Settings – IPSec

There are two methods for exchanging the encryption/decryption keys required by IPSec – Manual Key entry and Internet Key Exchange (IKE). The difference between Manual Key and IKE is how the encryption keys and SPI are determined. The **Tunnel Settings** page on the DFL-600 allows you to configure IKE for an IPSec VPN tunnel.

The differences between Manual Key and IKE can be summarized as:

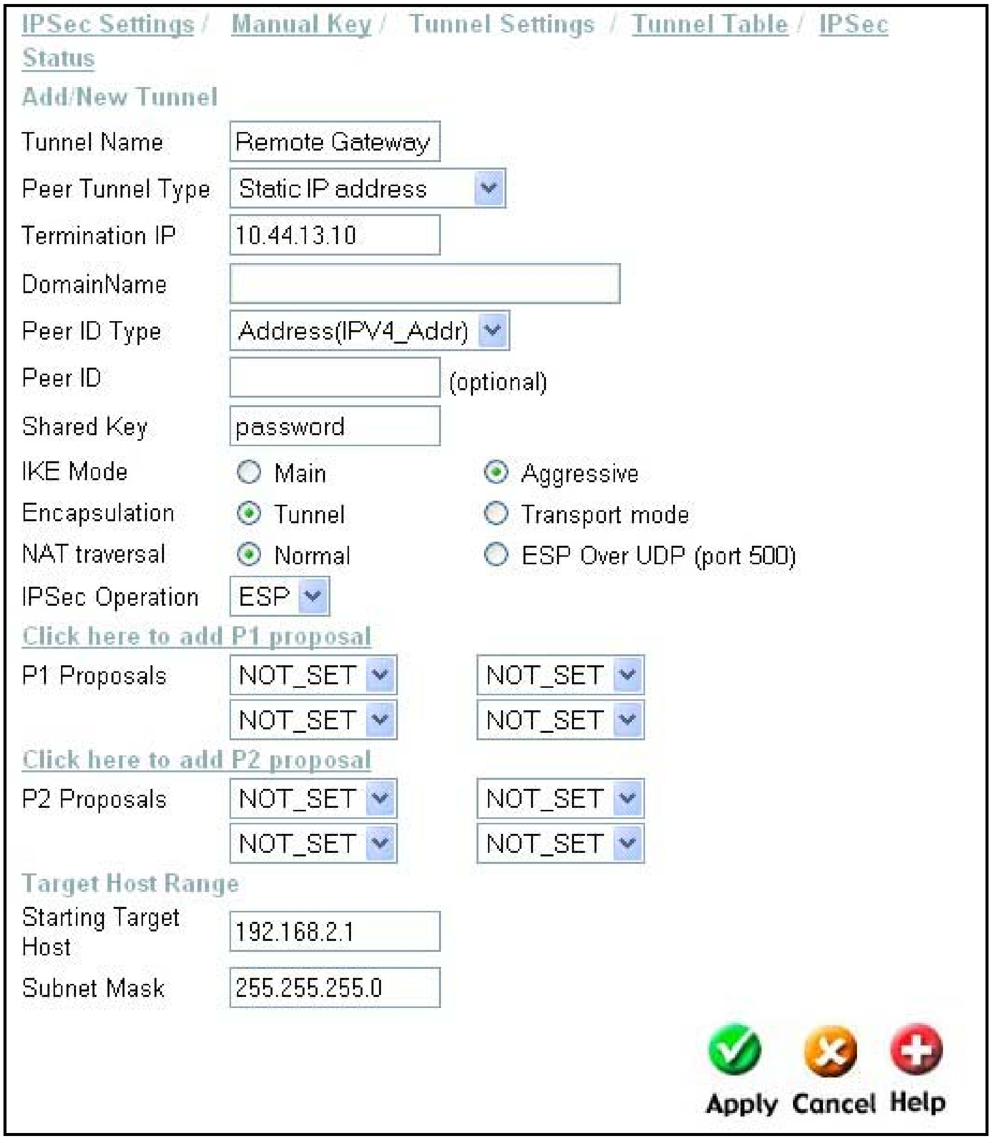
- For an IKE VPN, the keys and SPIs are negotiated between VPN gateways. The two VPN gateways can then use these keys and SPIs to maintain the IPSec connection.
- Manual Key VPN requires the encryption key, authentication key (if required), and SPIs to be predetermined by a network administrator when the IPSec connection is configured.

An IKE VPN is generally considered more secure than a Manual Key VPN because IKE can generate new keys and SPIs randomly during the negotiation phase.

To configure an IPSec VPN using IKE, click the **Tunnel Settings** link to open the page shown below.

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

Download from Www.Somanuals.com. All Manuals Search And Download.


IPSec Settings / Manual Key / Tunnel Settings / Tunnel Table / IPSec Status

Add/New Tunnel

Tunnel Name: Remote Gateway

Peer Tunnel Type: Static IP address

Termination IP: 10.44.13.10

DomainName:

Peer ID Type: Address(IPV4_Addr)

Peer ID: (optional)

Shared Key: password

IKE Mode: ○ Main ● Aggressive

Encapsulation: ● Tunnel ○ Transport mode

NAT traversal: ● Normal ○ ESP Over UDP (port 500)

IPSec Operation: ESP

Click here to add P1 proposal

P1 Proposals: NOT_SET NOT_SET NOT_SET NOT_SET

Click here to add P2 proposal

P2 Proposals: NOT_SET NOT_SET NOT_SET NOT_SET

Target Host Range

Starting Target Host: 192.168.2.1

Subnet Mask: 255.255.255.0

Add/New Tunnel	The following fields will identify the VPN tunnel on the DFL-600.
Tunnel Name	Enter a name by which this IPSec VPN tunnel configuration can be referrenced.
Peer Tunnel Type	You can choose the type of remote peer that

Download from Www.Somanuals.com. All Manuals Search And Download.

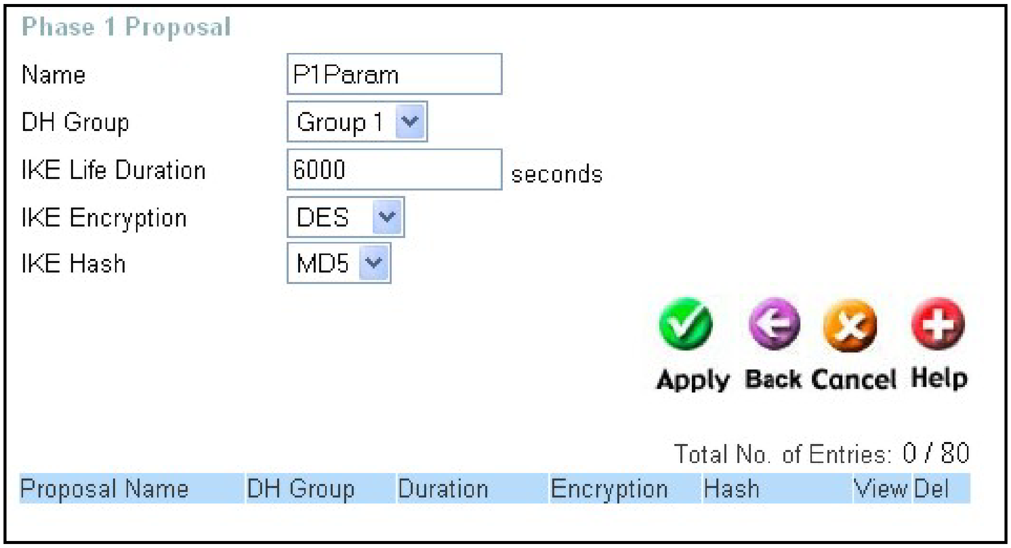
	this VPN tunnel will connect with using this drop-down menu. **Static IP address** allows you to specify the IP address of the remote end of the VPN tunnel – assuming that this IP address does not change (is statically assigned by the remote peer's ISP). **Domain Name** allows you to specify the domain name of the remote end of the VPN tunnel. This requires that the designated DNS server for the DFL-600 be able to resolve the specified domain name into an IP address. **Dynamic IP address** allows you to specify that the remote end of the VPN tunnel is assigned an IP address using DHCP. Please note that if the remote end of an IPSec VPN tunnel uses a dynamically assigned IP address, this end must have a statically assigned IP address. That is, both ends of an IPSec VPN tunnel cannot have a dynamically assigned IP address.
Termination IP	The IP address of the remote gateway. If you choose **Static IP address** in the drop-down menu above, you must enter the IP address of the remote end of the IPSec VPN tunnel here.
Domain Name	The domain name of the remote gateway. If you choose **Domain Name** in the drop-down menu above, you must enter the domain name of the remote end of the IPSec VPN tunnel here.
Peer ID Type	This drop-down menu allows you to specify the type of authorization key **Address(IPV4_Addr) –** This allows you to specify that the IP address of the remote end of the IPSec VPN tunnel will be used to identify and authenticate the remote host.

Download from Www.Somanuals.com. All Manuals Search And Download.

	Sting(FQDN) – This allows you to specify that the "fully-qualified domain name" of the remote end of the IPSec VPN tunnel will be used to identify and authenticate the remote host. **Email(UFQDN) –** This allows you to specify that the E-mail address of the remote end of the IPSec VPN tunnel will be used to identify and authenticate the remote host.
Peer ID	This allows you to enter the IP address, "fully-qualified domain name," or E-mail address of the remote end of the IPSec VPN tunnel.
Shared Key	The shared secret key that must be supplied by the remote end of the IPSec VPN tunnel. The shared key and the IP address, FQDN, or E-mail address will be used together to uniquely identify a remote host (or a set of hosts sharing a common identity).
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. Click on this link to open the **Phase 1 Proposal** configuration page, as shown below.
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. Click on this link to open the **Phase 2 Proposal** configuration page, as shown below.
Target Host Range	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.
Starting Target Host	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 192.168.2.1 to 192.168.2.254 will be allowed to access the VPN. Note that the IP addresses192.168.2.0 and 192.168.2.255 are reserved for use on the remote network.
Subnet Mask	Enter the subnet mask corresponding to the IP address range entered above.

Phase 1 Proposal



Phase 1 Proposal

Name	P1Param
DH Group	Group 1
IKE Life Duration	6000 seconds
IKE Encryption	DES
IKE Hash	MD5

Total No. of Entries: 0 / 80

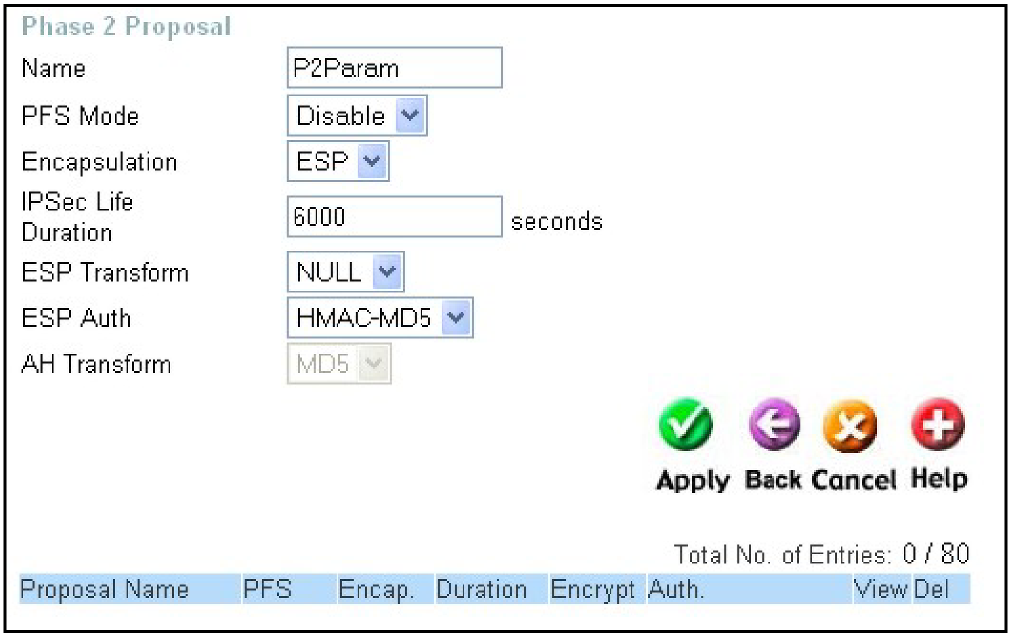
Proposal Name	DH Group	Duration	Encryption	Hash	View	Del

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


Phase 2 Proposal

Name	P2Param	
PFS Mode	Disable	
Encapsulation	ESP	
IPSec Life Duration	6000	seconds
ESP Transform	NULL	
ESP Auth	HMAC-MD5	
AH Transform	MD5	

Total No. of Entries: 0 / 80

Proposal Name	PFS	Encap.	Duration	Encrypt	Auth.	View	Del

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

Download from Www.Somanuals.com. All Manuals Search And Download.

	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	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. **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). **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.
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.

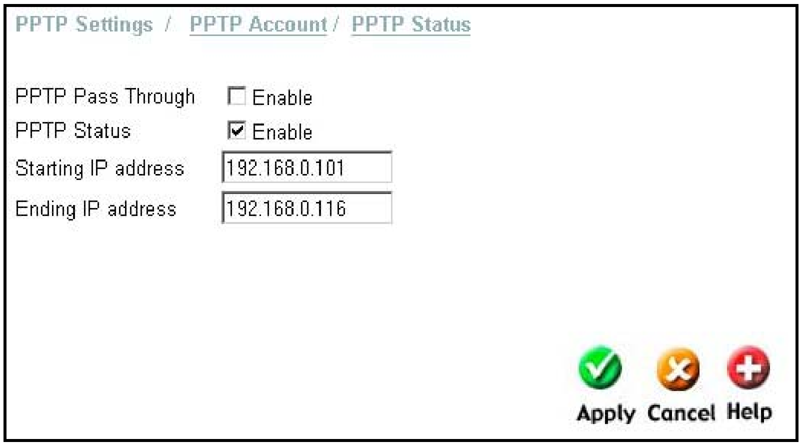
Download from Www.Somanuals.com. All Manuals Search And Download.

ESP Transform	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. You can choose between **Null** – no encryption, **DES** – using DES encryption, and **3DES** – using triple DES encryption. You must select the exact same ESP transform (encryption algorithm) on both ends of a VPN tunnel.
ESP Auth	This drop-down menu allows you to select the authentication method that will be used when **ESP** is selected in the **IPSec Operation** drop-down menu above. You can choose between **Null** – no authorization, **MD5** – using MD5 message digest authentication, and **SHA** – using the SHA authentication method. You must select the exact same ESP authentication method on both ends of a VPN tunnel.
AH Transform	This drop-down menu allows you to select the authentication method that will be used when **AH** is selected in the **IPSec Operation** drop-down menu above. You can choose between **MD5** – using MD5 message digest authentication, and **SHA** – using the SHA authentication method. You must select the exact same AH authentication method on both ends of a VPN tunnel.

Download from Www.Somanuals.com. All Manuals Search And Download.

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 Pass Through □ Enable

PPTP Status ☑ Enable

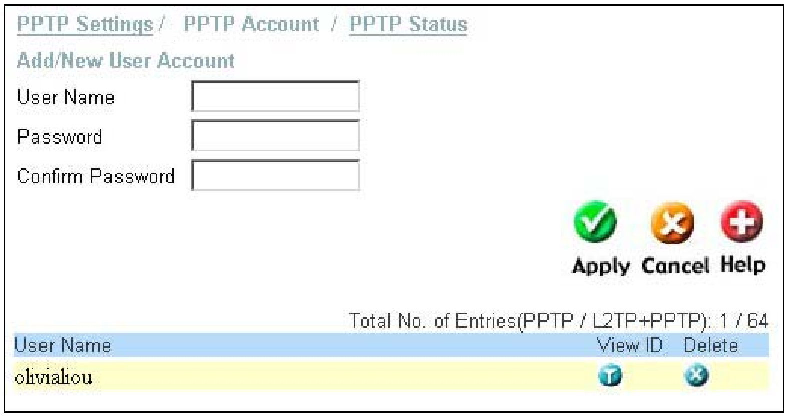
Starting IP address 192.168.0.101

Ending IP address 192.168.0.116

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 clients 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 clients 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.



User Name

Password

Confirm Password

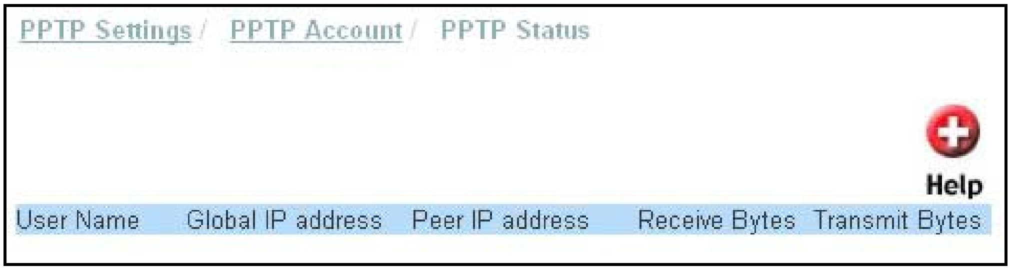
Total No. of Entries(PPTP / L2TP+PPTP): 1 / 64

User Name	View ID	Delete
olivialiou		

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

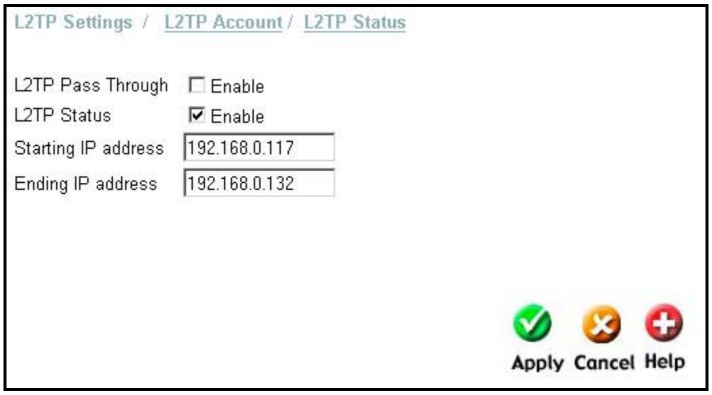
Click on the **PPTP Status** link to display the current status of a PPTP tunnel on the DFL-600, as shown below.



User Name	Global IP address	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 Pass Through □ Enable

L2TP Status ☑ Enable

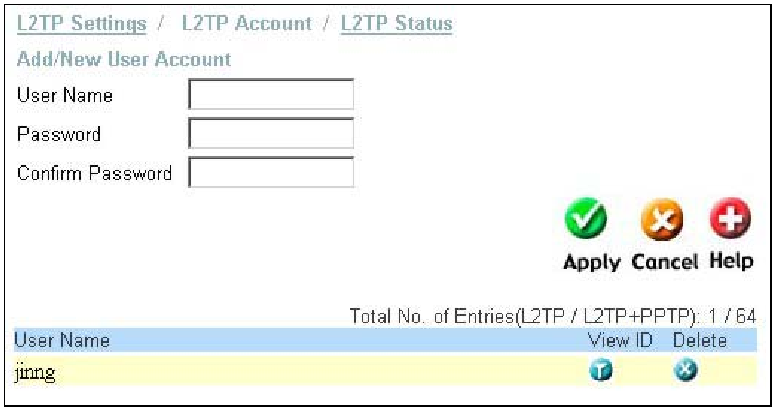
Starting IP address 192.168.0.117

Ending IP address 192.168.0.132

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.



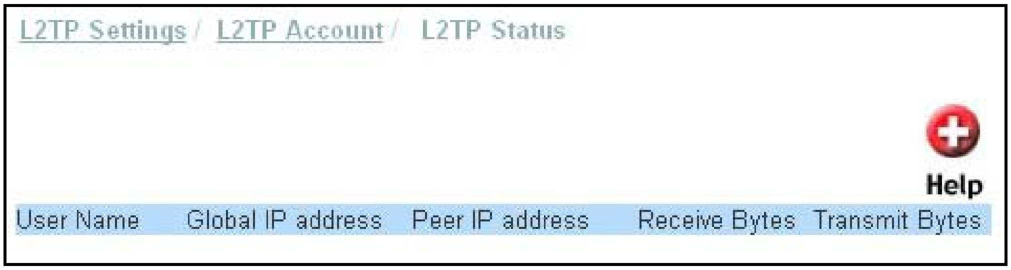
Total No. of Entries(L2TP / L2TP+PPTP): 1 / 64

User Name	View ID	Delete
jinng		

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.



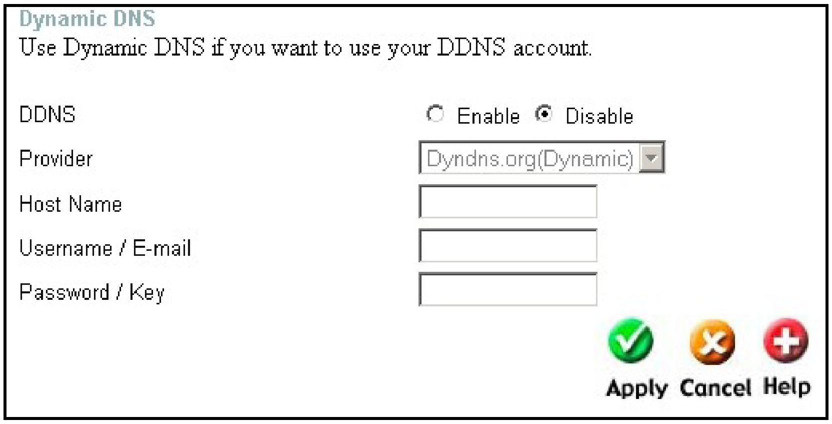
User Name	Global IP address	Peer IP address	Receive Bytes	Transmit Bytes

Download from Www.Somanuals.com. All Manuals Search And Download.

DDNS

The DFL-600 can be configured to use Dynamic DNS (DDNS). If you choose to use DDNS you must fist setup a user account with either Dynamic DNS Network Services (www.dyndns.org) or PeanutHull(China) – a service available in China. Please visit their respective websites for more information.

Clicking on the **DDNS** button from the **Advanced** page will open the following page.



Dynamic DNS

Use Dynamic DNS if you want to use your DDNS account.

DDNS	○ Enable ● Disable
Provider	Dyndns.org(Dynamic)
Host Name	
Username / E-mail	
Password / Key	

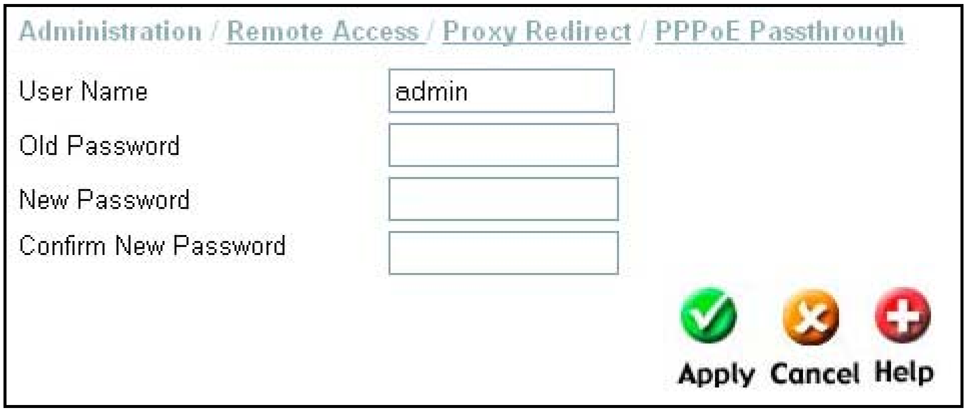
DDNS	This allows you to enable or disable DDNS on the DFL-600
Provider	Select either Dyndns.org or PeanutHull(China)
Host Name	Enter the appropriate host name here.
Username/E-mail	Enter the appropriate Username here.
Password/Key	Enter the appropriate Password or Key here.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.



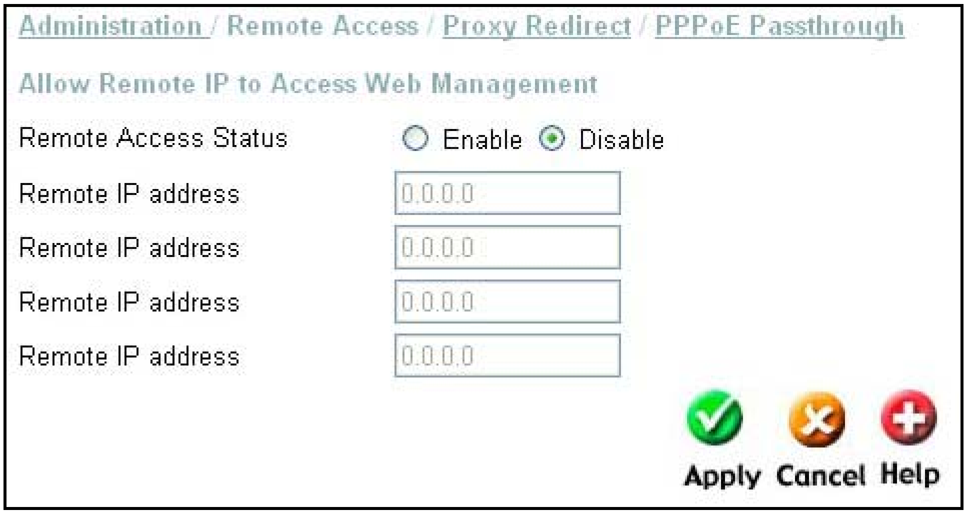
Administration / Remote Access / Proxy Redirect / PPPoE Passthrough

User Name	admin
Old Password	
New Password	
Confirm New Password	

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 no IP address on the WAN side of the DFL-600 (no computer from the Internet) will be allowed to access the DFL-600's configuration utility.



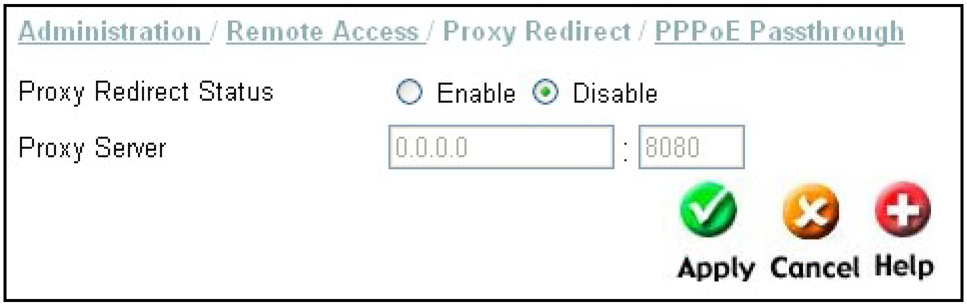
Administration / Remote Access / Proxy Redirect / PPPoE Passthrough

Allow Remote IP to Access Web Management

Remote Access Status	○ Enable ● Disable
Remote IP address	0.0.0.0
Remote IP address	0.0.0.0
Remote IP address	0.0.0.0
Remote IP address	0.0.0.0

Proxy Redirect

The DFL-600 allows you to specify a proxy server for your LAN. Enter the IP address and the port number in the fields provided.

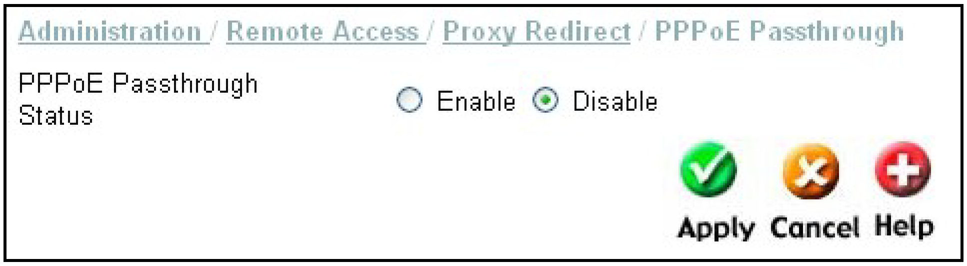


Administration / Remote Access / Proxy Redirect / PPPoE Passthrough

Proxy Redirect Status	○ Enable ● Disable
Proxy Server	0.0.0.0 : 8080

PPPoE Passthrough

The DFL-600 allows you to pass PPPoE authentication and connection packets to a PC on your LAN that will then make the connection using appropriate software to give the server at your ISP the appropriate username and password, if necessary.



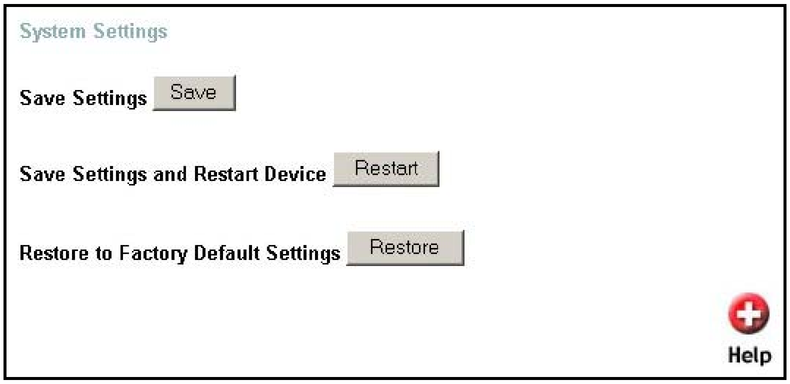
Administration / Remote Access / Proxy Redirect / PPPoE Passthrough

PPPoE Passthrough Status ○ Enable ● Disable

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.


System Settings

Save Settings

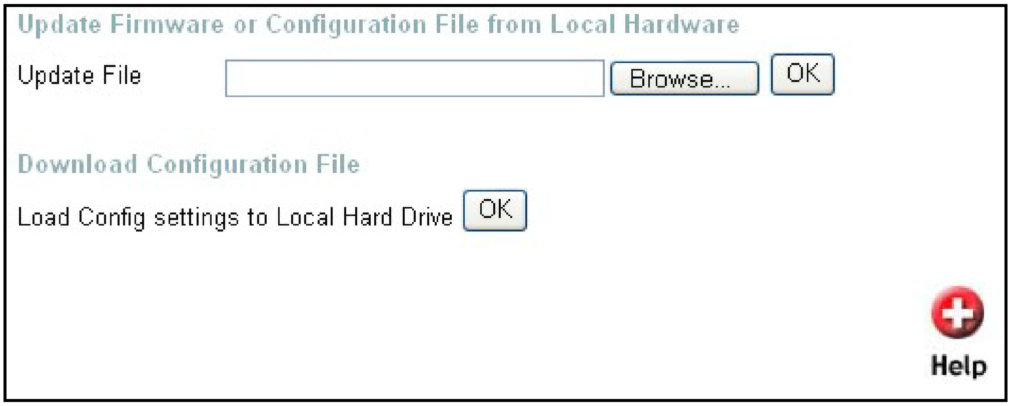
Save Settings and Restart Device

Restore to Factory Default Settings

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 Firmware or Configuration File from Local Hardware

Update File

Download Configuration File

Load Config settings to Local Hard Drive

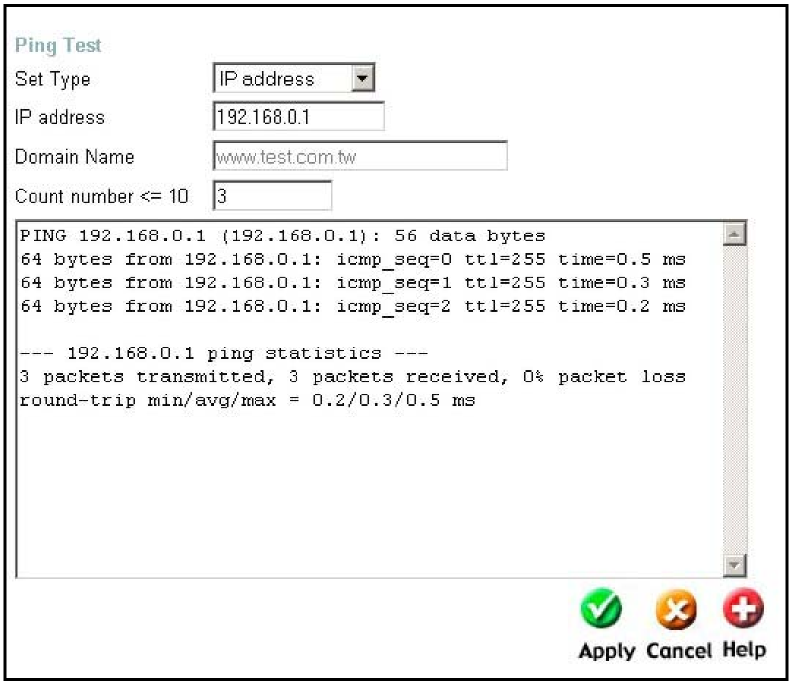
Update File	Enter the full DOS path and filename to the new firmware file on your local hard drive. For example, if the file is in the root directory of your C drive, enter **C:\newfile.had** and click the **OK** button to begin the file transfer.
Browse	If you are unsure about the location of the new 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.

Download from Www.Somanuals.com. All Manuals Search And Download.



Ping Test

Set Type: IP address

IP address: 192.168.0.1

Domain Name: www.test.com.tw

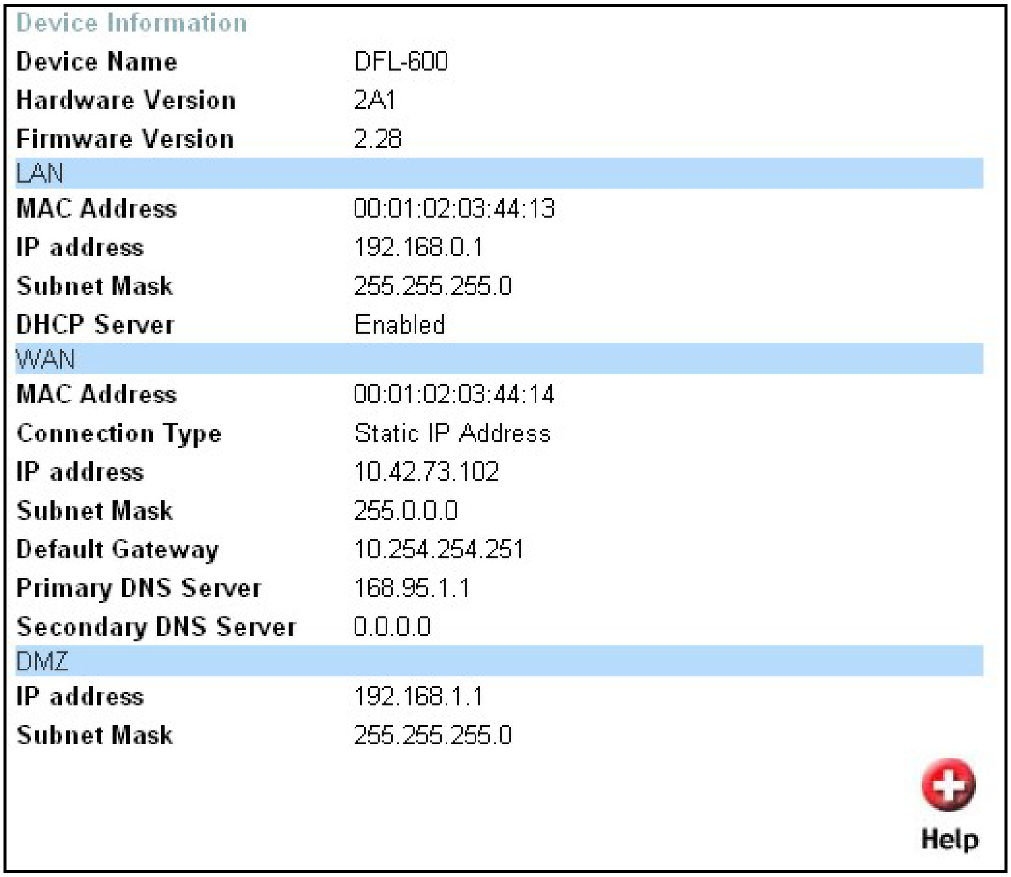
Count number <= 10: 3

```
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
```

Download from Www.Somanuals.com. All Manuals Search And Download.

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	2.28
LAN	
MAC Address	00:01:02:03:44:13
IP address	192.168.0.1
Subnet Mask	255.255.255.0
DHCP Server	Enabled
WAN	
MAC Address	00:01:02:03:44:14
Connection Type	Static IP Address
IP address	10.42.73.102
Subnet Mask	255.0.0.0
Default Gateway	10.254.254.251
Primary DNS Server	168.95.1.1
Secondary DNS Server	0.0.0.0
DMZ	
IP address	192.168.1.1
Subnet Mask	255.255.255.0

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.

Download from Www.Somanuals.com. All Manuals Search And Download.

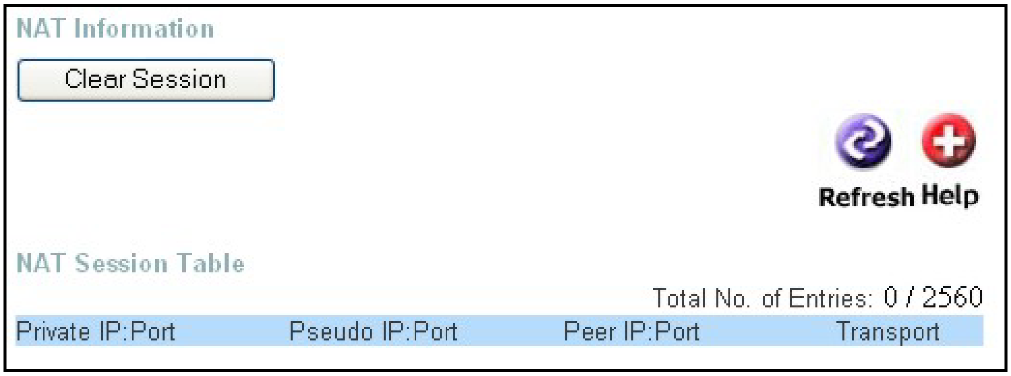
Subnet Mask	This is the subnet mask corresponding to the IP address above – that is currently in use by the DFL-600 on the LAN.
DHCP Server	Displays whether the DFL-600 is currently configured as a DHCP server on the LAN.

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:



NAT Information

NAT Session Table

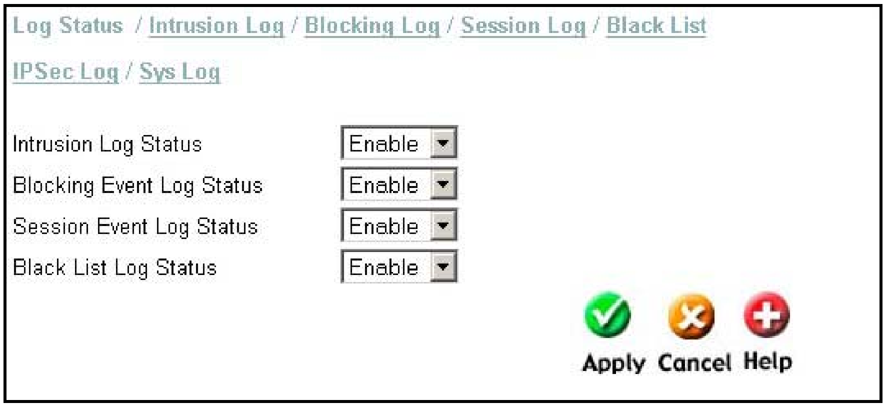
Total No. of Entries: 0 / 2560

Private IP:Port	Pseudo IP:Port	Peer IP:Port	Transport

Private IP: Port	This is the IP address and port number of a computer or device on your LAN that has an active NAT session.
Pseudo IP: Port	This is the IP address and port number that the DFL-600 used to establish the LAN side of the NAT connection
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
Transport	This is the transport protocol in use by the corresponding session.

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: Enable

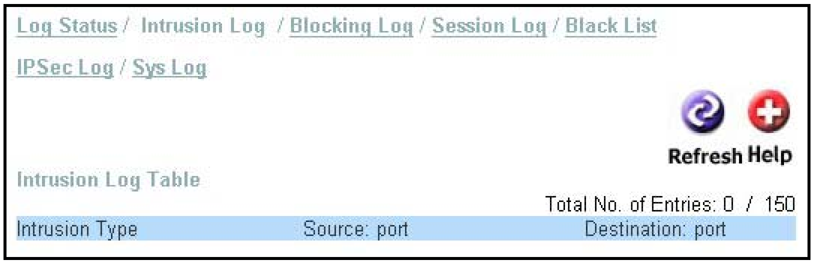
Blocking Event Log Status: Enable

Session Event Log Status: Enable

Black List Log Status: Enable

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

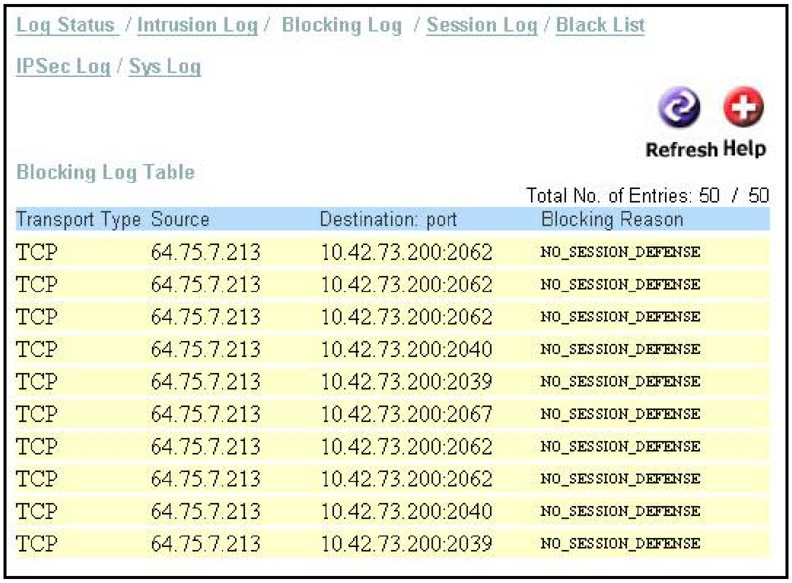
Total No. of Entries: 0 / 150

Intrusion Type	Source: port	Destination: port

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

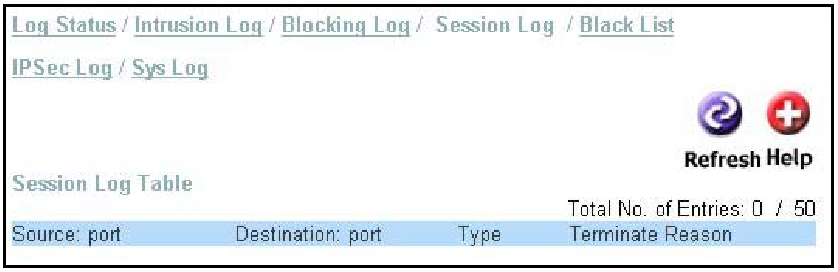
Transport Type	Source	Destination: port	Blocking Reason
TCP	64.75.7.213	10.42.73.200:2062	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2062	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2062	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2040	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2039	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2067	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2062	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2062	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2040	NO_SESSION_DEFENSE
TCP	64.75.7.213	10.42.73.200:2039	NO_SESSION_DEFENSE

Transport Type **Source**	The protocol used to make the connection attempt is displayed here.
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:

Download from Www.Somanuals.com. All Manuals Search And Download.


Log Status / Intrusion Log / Blocking Log / Session Log / Black List
IPSec Log / Sys Log
Refresh
Help

Session Log Table

Total No. of Entries: 0 / 50

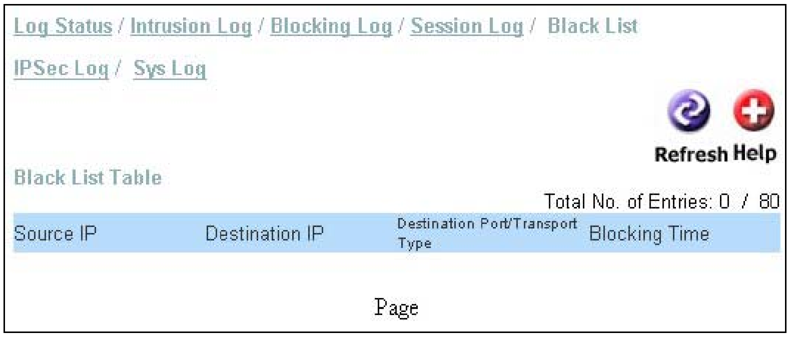
Source: port	Destination: port	Type	Terminate Reason

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.


Log Status / Intrusion Log / Blocking Log / Session Log / Black List
IPSec Log / Sys Log
Refresh
Help

Black List Table

Total No. of Entries: 0 / 80

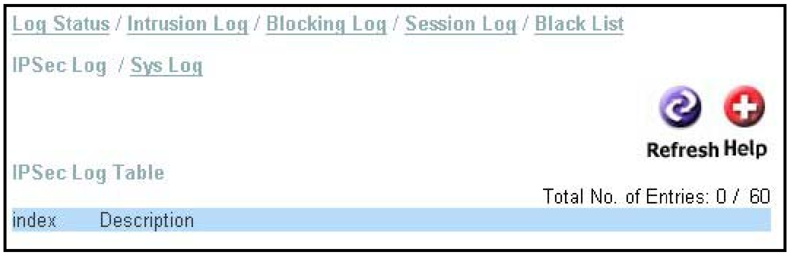
Source IP	Destination IP	Destination Port/Transport Type	Blocking Time

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:


Log Status / Intrusion Log / Blocking Log / Session Log / Black List
IPSec Log / Sys Log
Refresh
Help

IPSec Log Table

Total No. of Entries: 0 / 60

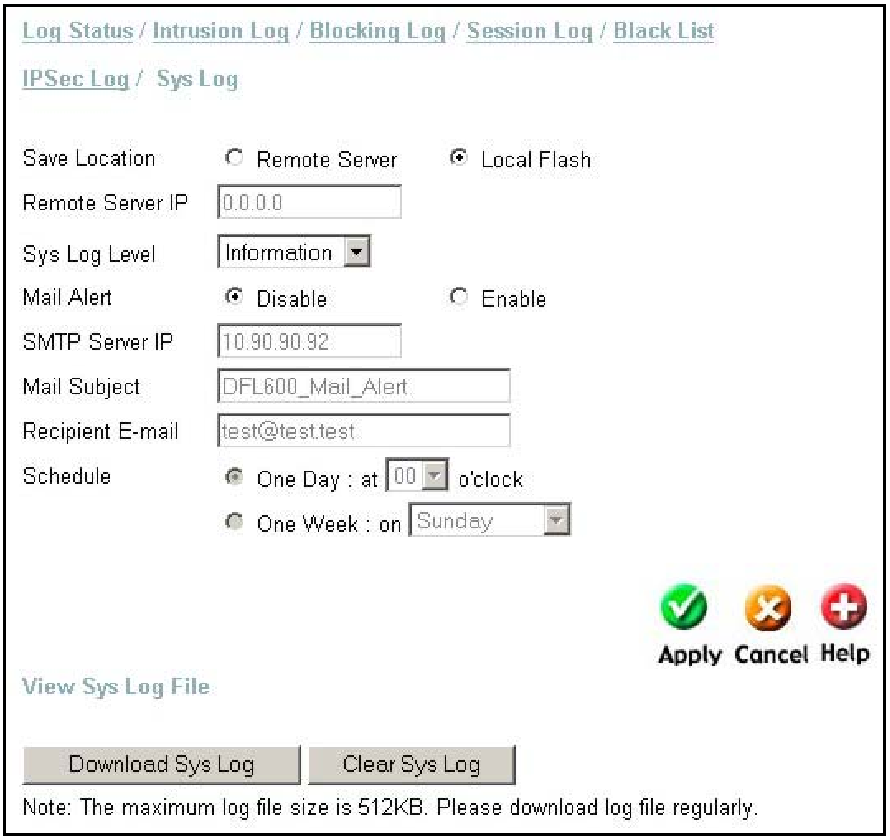
index	Description

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

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.



Log Status / Intrusion Log / Blocking Log / Session Log / Black List
IPSec Log / Sys Log

Save Location ○ Remote Server ● Local Flash

Remote Server IP 0.0.0.0

Sys Log Level Information

Mail Alert ● Disable ○ Enable

SMTP Server IP 10.90.90.92

Mail Subject DFL600_Mail_Alert

Recipient E-mail test@test.test

Schedule ● One Day : at 00 o'clock

○ One Week : on Sunday

Note: The maximum log file size is 512KB. Please download log file regularly.

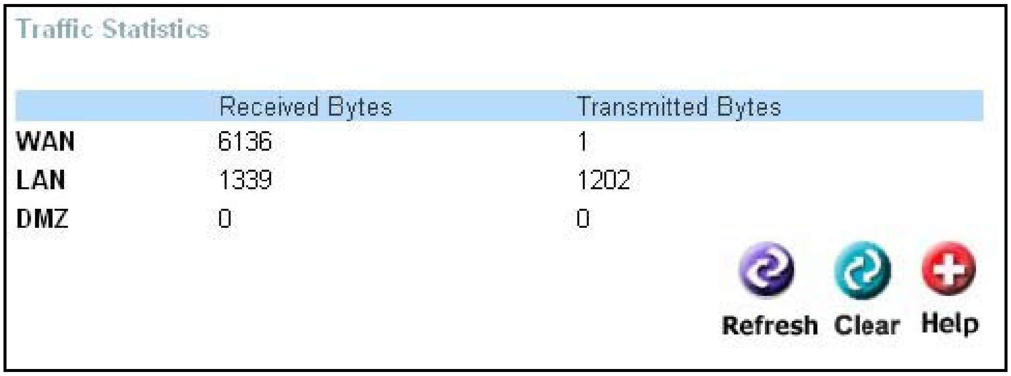
Save Location	Choose either the **Remote Server** or the **Local Flash** option.

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.
Mail Alert	This allows you to send syslog messages to an e-mail address you specify below.
SMTP Server IP	This is the IP address of your Simple Mail Transfer Protocol (SMTP) server.
Mail Subject	This is the subject line that will appear when a syslog message e-mail is sent.
Recipient E-mail	This is the e-mail address the syslog message e-mail will be sent to.
Schedule	You can select between sending a syslog message e-mail once per day or once per week.

Download from Www.Somanuals.com. All Manuals Search And Download.

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.



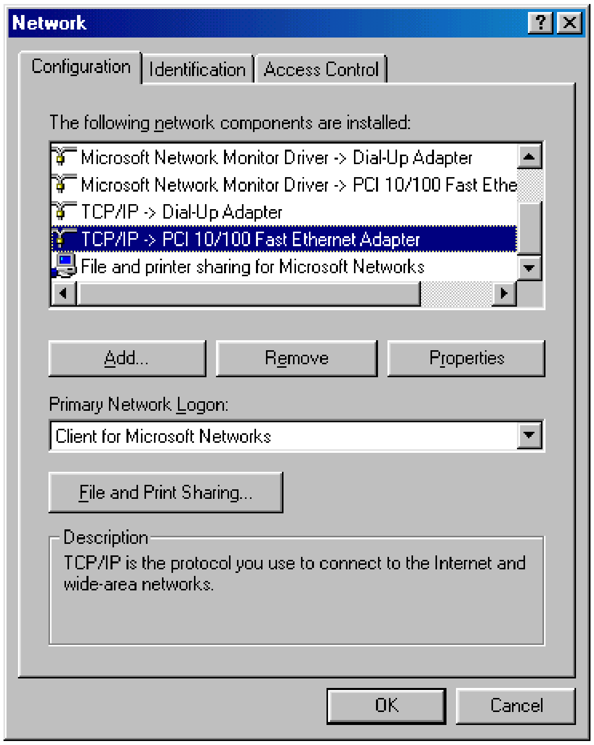
Traffic Statistics

	Received Bytes	Transmitted Bytes
WAN	6136	1
LAN	1339	1202
DMZ	0	0

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/adapter. If there is no TCP/IP line listed, you will need to install TCP/IP now.



The following network components are installed:

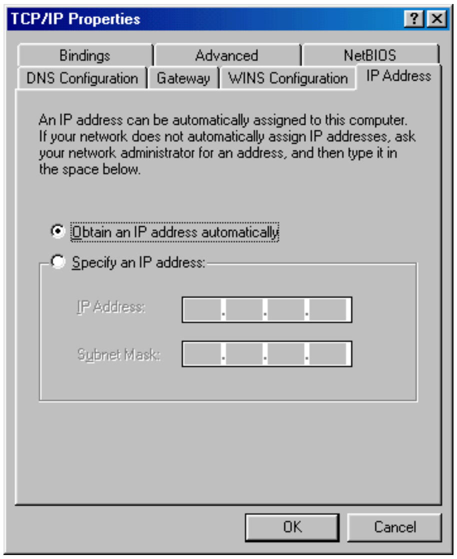
- Microsoft Network Monitor Driver -> Dial-Up Adapter
- Microsoft Network Monitor Driver -> PCI 10/100 Fast Ethe
- TCP/IP -> Dial-Up Adapter
- TCP/IP -> PCI 10/100 Fast Ethernet Adapter
- File and printer sharing for Microsoft Networks

Primary Network Logon: Client for Microsoft Networks

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

Download from Www.Somanuals.com. All Manuals Search And Download.

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



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

● Obtain an IP address automatically

○ Specify an IP address:

IP Address: . . .

Subnet Mask: . . .

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

CONFIRM YOUR PC'

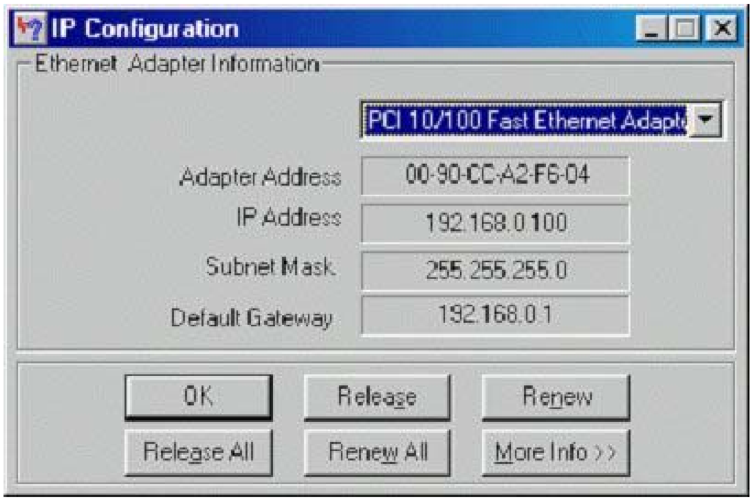
There are two tools which are great for finding out a computer's IP configuration: MAC address and default gateway.

- **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.

Download from Www.Somanuals.com. All Manuals Search And Download.



IP Configuration

Ethernet Adapter Information

PCI 10/100 Fast Ethernet Adapt

Adapter Address: 00-90-CC-A2-F6-04

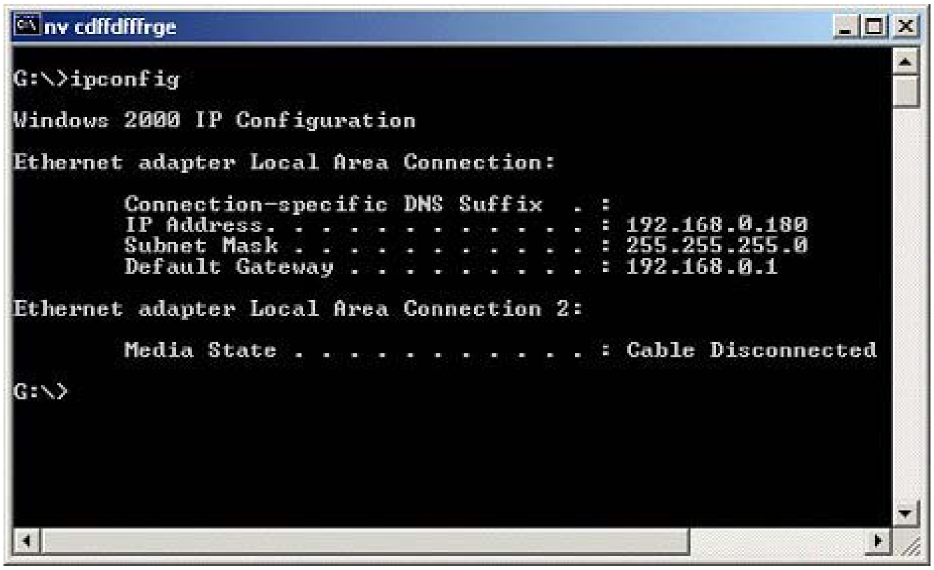
IP Address: 192.168.0.100

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.1

- 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.



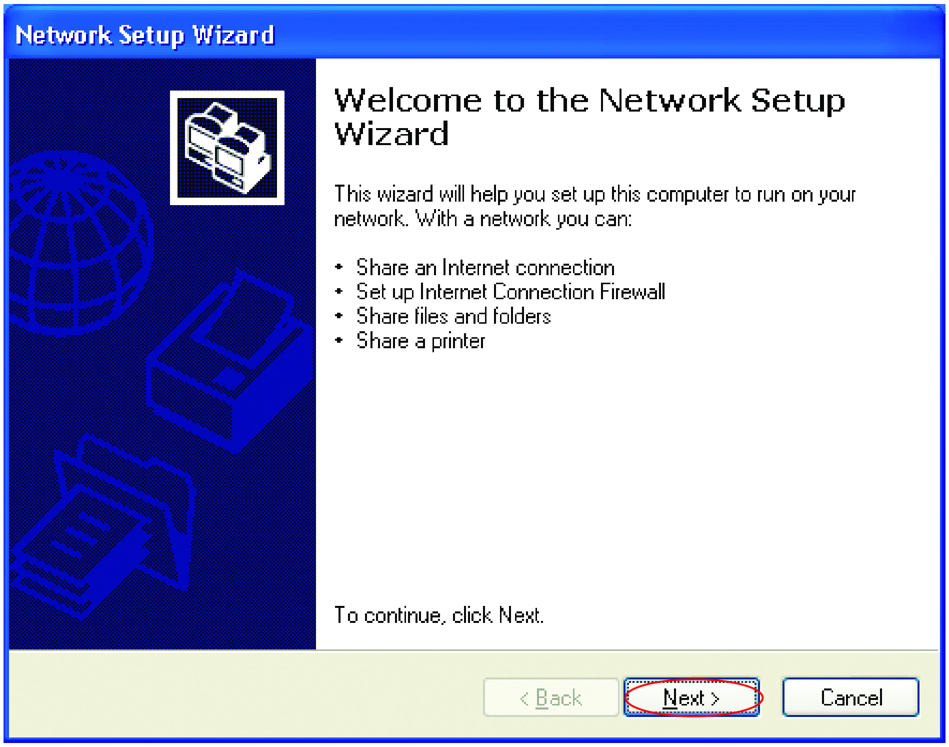
```
G:\>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.180
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.0.1

Ethernet adapter Local Area Connection 2:

        Media State . . . . . . . . . . . : Cable Disconnected

G:\>
```

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



Network Setup Wizard

Welcome to the Network Setup Wizard

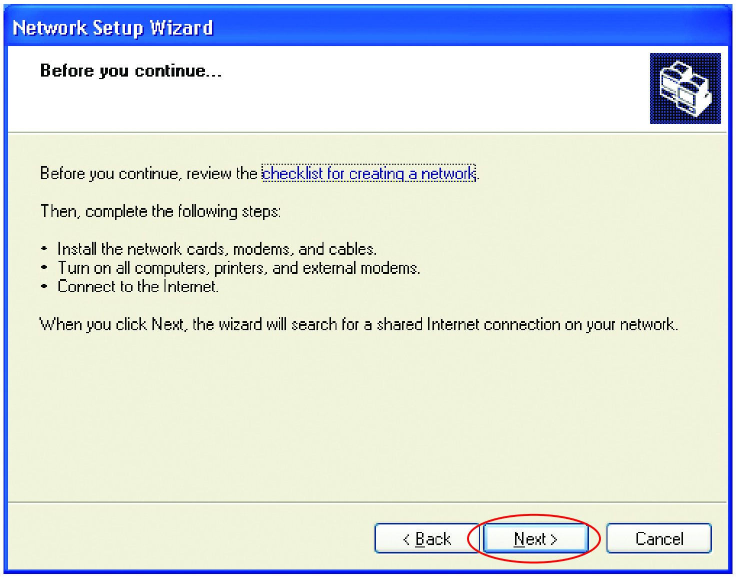
This wizard will help you set up this computer to run on your network. With a network you can:

- Share an Internet connection
- Set up Internet Connection Firewall
- Share files and folders
- Share a printer

To continue, click Next.

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

Please follow all the instructions in this window:



Before you continue...

Before you continue, review the checklist for creating a network.

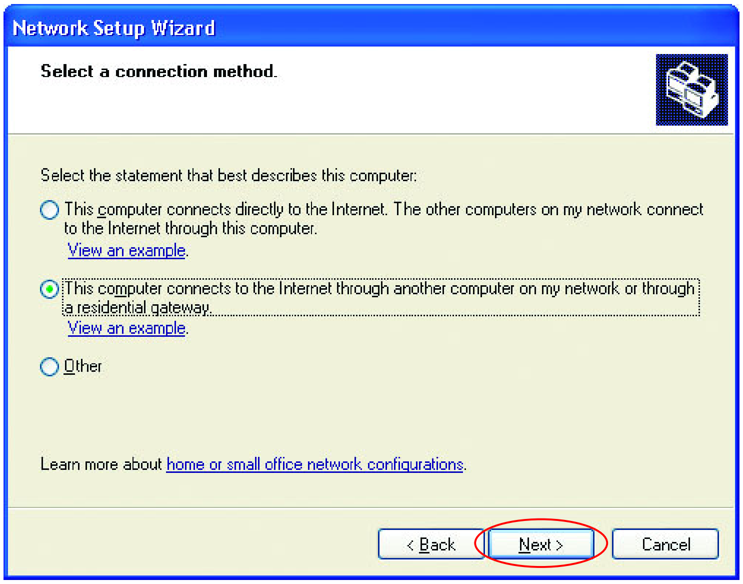
Then, complete the following steps:

- Install the network cards, modems, and cables.
- Turn on all computers, printers, and external modems.
- Connect to the Internet.

When you click Next, the wizard will search for a shared Internet connection on your network.

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.



Network Setup Wizard

Select a connection method.

Select the statement that best describes this computer:

○ This computer connects directly to the Internet. The other computers on my network connect to the Internet through this computer.
View an example.

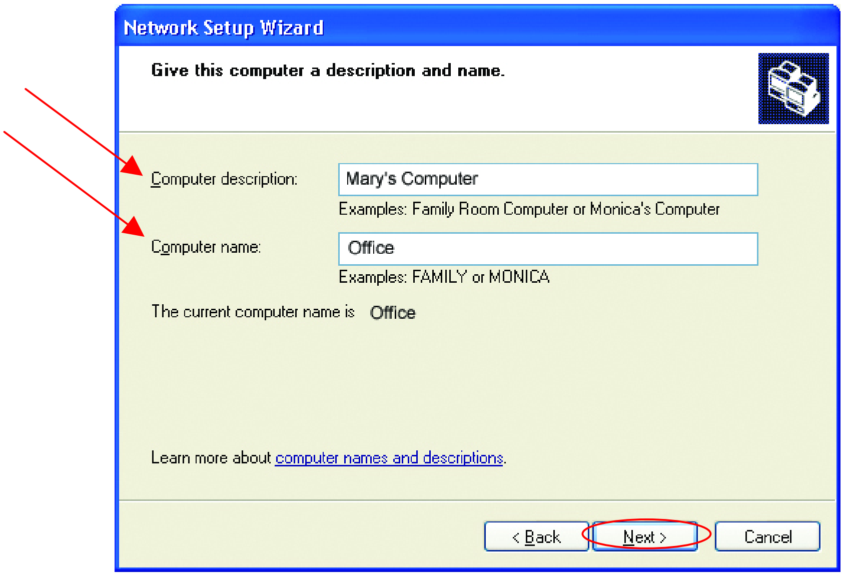
● This computer connects to the Internet through another computer on my network or through a residential gateway.
View an example.

○ Other

Learn more about home or small office network configurations.

Click **Next**

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



Network Setup Wizard

Give this computer a description and name.

Computer description: Mary's Computer
Examples: Family Room Computer or Monica's Computer

Computer name: Office
Examples: FAMILY or MONICA

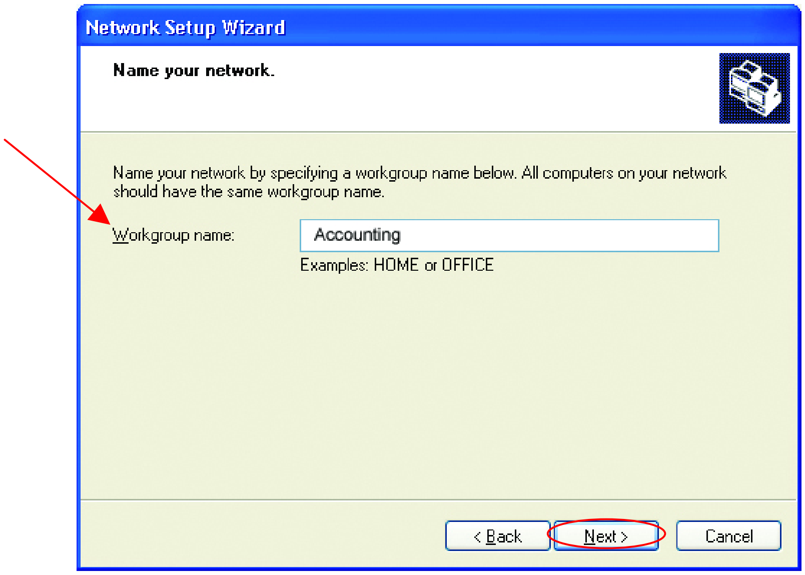
The current computer name is Office

Learn more about computer names and descriptions.

Click **Next**

Download from Www.Somanuals.com. All Manuals Search And Download.

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



Name your network by specifying a workgroup name below. All computers on your network should have the same workgroup name.

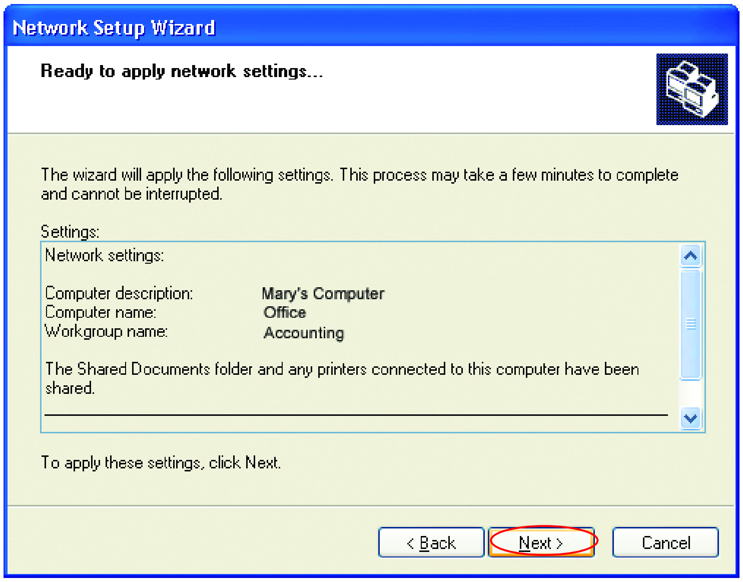
Workgroup name: Accounting

Examples: HOME or OFFICE

Click **Next**

Please wait while the wizard applies the changes.

Download from Www.Somanuals.com. All Manuals Search And Download.



Ready to apply network settings...

The wizard will apply the following settings. This process may take a few minutes to complete and cannot be interrupted.

Settings:

Network settings:

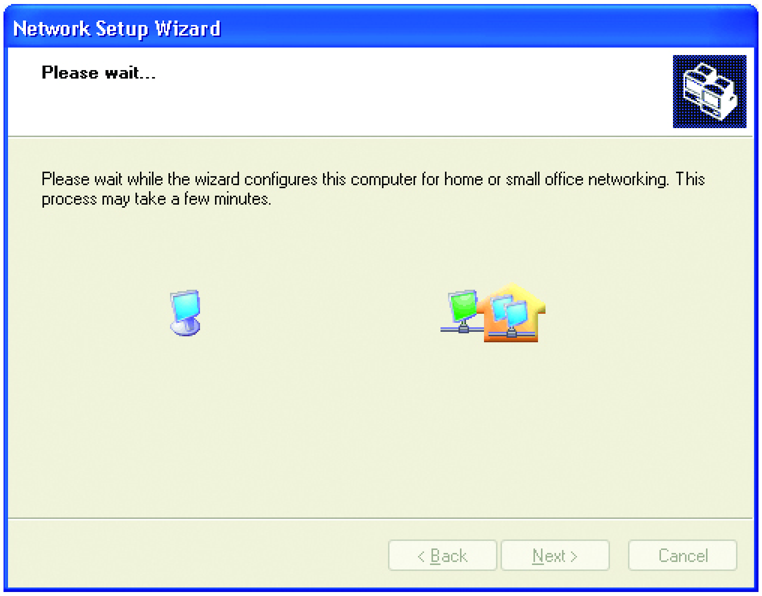
Computer description:	Mary's Computer
Computer name:	Office
Workgroup name:	Accounting

The Shared Documents folder and any printers connected to this computer have been shared.

To apply these settings, click Next.

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

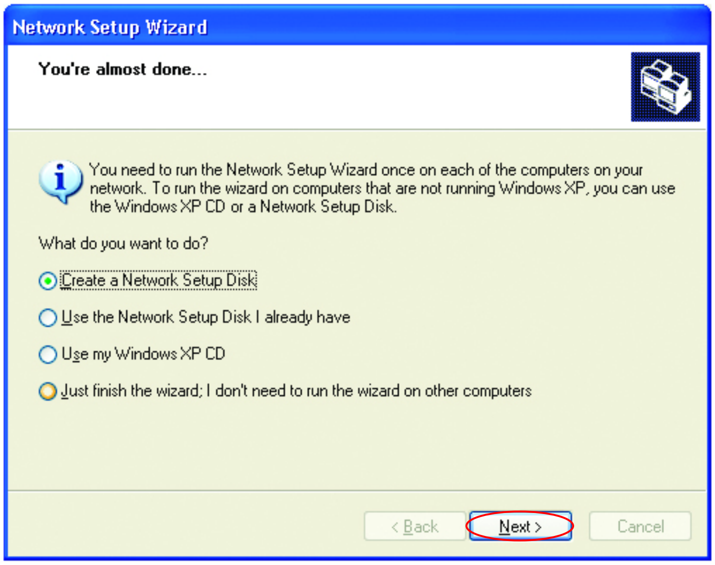
Please wait while the wizard configures the computer.
This may take a few minutes.



Please wait...

Please wait while the wizard configures this computer for home or small office networking. This process 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**.



Network Setup Wizard

You're almost done...

You need to run the Network Setup Wizard once on each of the computers on your network. To run the wizard on computers that are not running Windows XP, you can use the Windows XP CD or a Network Setup Disk.

What do you want to do?

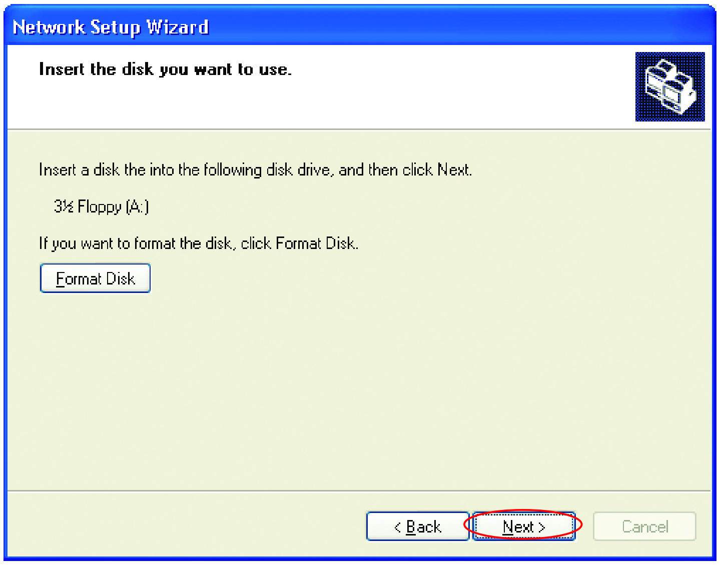
● Create a Network Setup Disk

○ Use the Network Setup Disk I already have

○ Use my Windows XP CD

○ Just finish the wizard; I don't need to run the wizard on other computers

Insert a disk into the Floppy Disk Drive, in this case drive "A:"



Network Setup Wizard

Insert the disk you want to use.

Insert a disk the into the following disk drive, and then click Next.

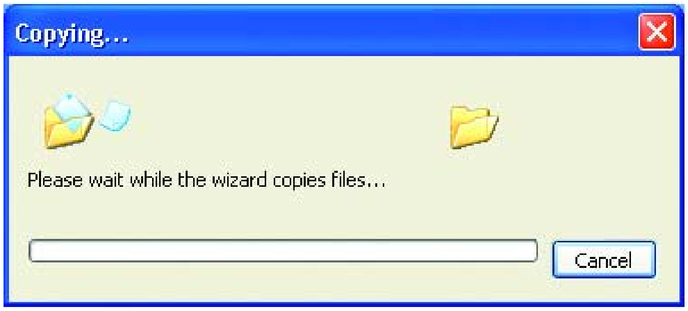
3½ Floppy (A:)

If you want to format the disk, click Format Disk.

Download from Www.Somanuals.com. All Manuals Search And Download.

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

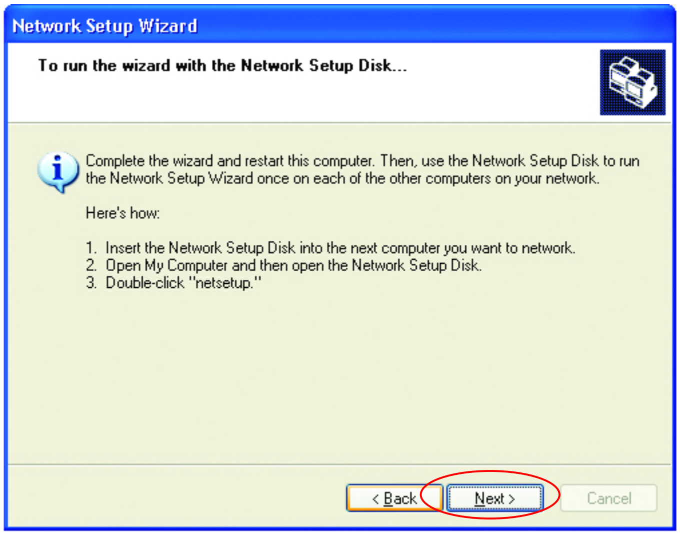
Please wait while the wizard copies the files.



Please wait while the wizard copies 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**



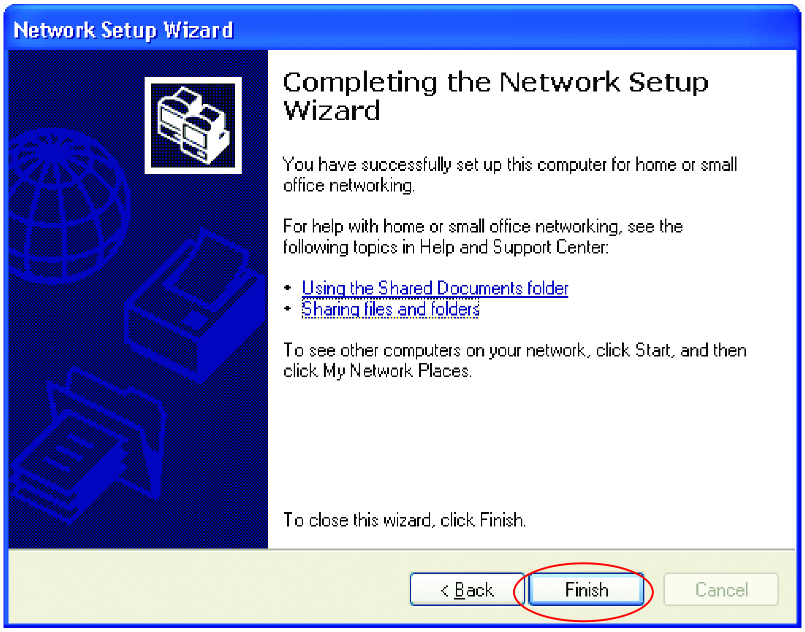
To run the wizard with the Network Setup Disk...

Complete the wizard and restart this computer. Then, use the Network Setup Disk to run the Network Setup Wizard once on each of the other computers on your network.

Here's how:

1. Insert the Network Setup Disk into the next computer you want to network.
2. Open My Computer and then open the Network Setup Disk.
3. Double-click "netsetup."

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



Completing the Network Setup Wizard

You have successfully set up this computer for home or small office networking.

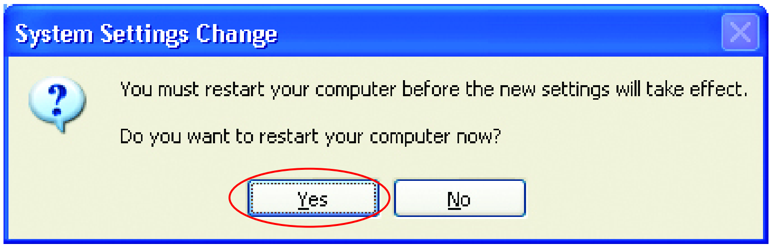
For help with home or small office networking, see the following topics in Help and Support Center:

- Using the Shared Documents folder
- Sharing files and folders

To see other computers on your network, click Start, and then click My Network Places.

To close this wizard, click Finish.

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



You must restart your computer before the new settings will take effect.

Do you want to restart your computer now?

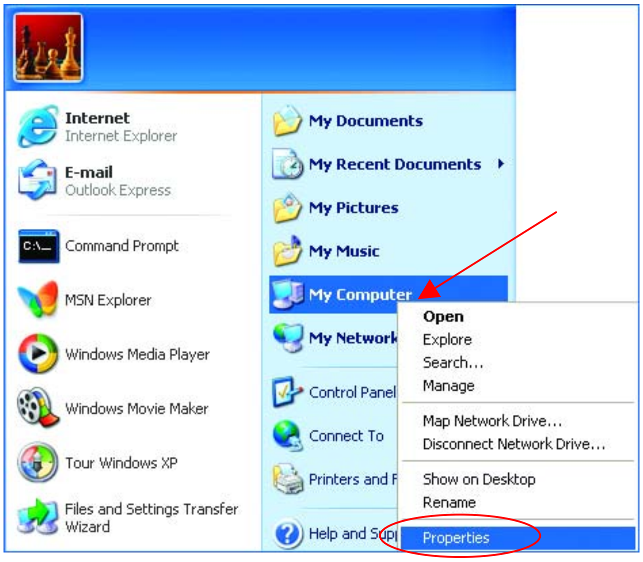
You have completed configuring this computer. Next, you will need to run the Network Setup Disk on all the other computers on your network. After running the Network Setup Disk on all your computers, your new wireless network will be ready to use.

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**

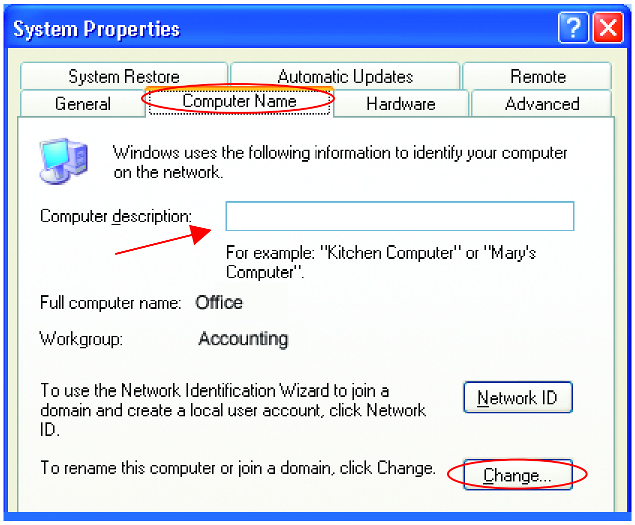


- Select the **Computer Name Tab** in the **System Properties** window.

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

To rename the computer and join a domain:

- Click **Change**



Windows uses the following information to identify your computer on the network.

Computer description:

For example: "Kitchen Computer" or "Mary's Computer".

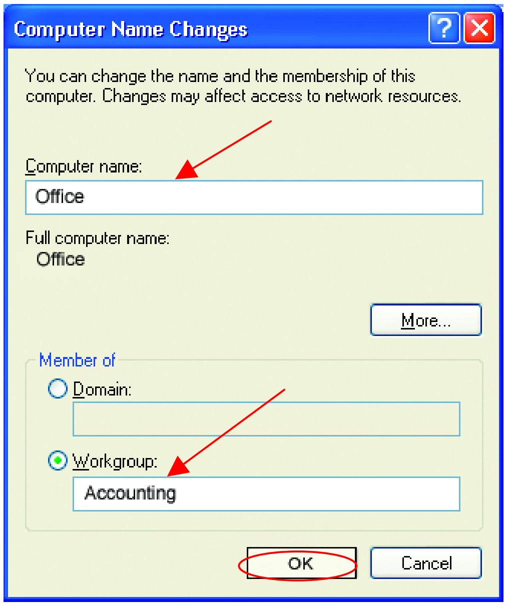
Full computer name: Office

Workgroup: Accounting

To use the Network Identification Wizard to join a domain and create a local user account, click Network ID.

To rename this computer or 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**



Computer Name Changes

You can change the name and the membership of this computer. Changes may affect access to network resources.

Computer name: Office

Full computer name: Office

Member of

○ Domain:

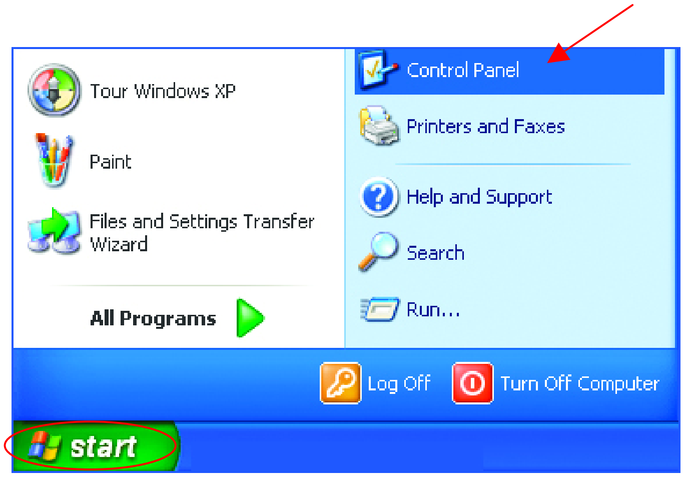
● Workgroup: Accounting

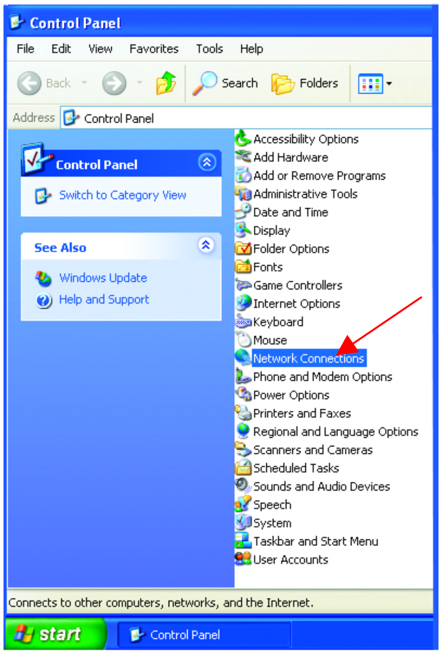
Assigning a Static IP Address

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



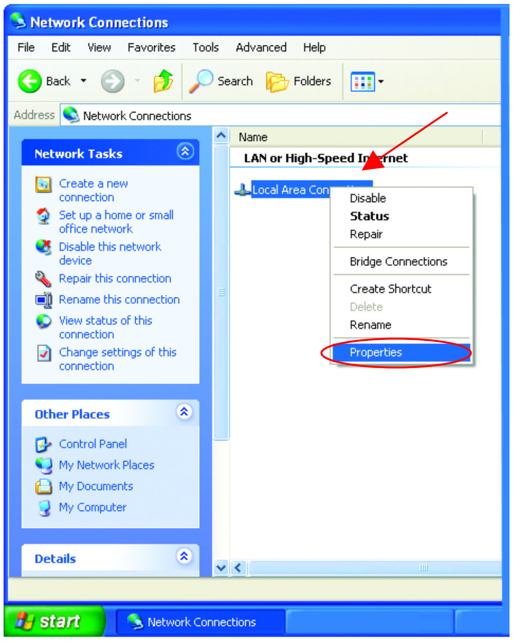


Double-click on
Network Connections

Download from Www.Somanuals.com. All Manuals Search And Download.

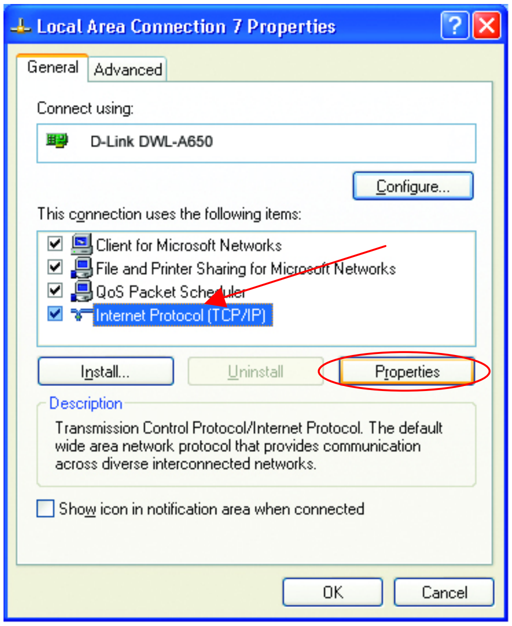
Right-click on **Local Area Connections**.

Double-click **Properties**



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

Click **Properties**



Connect using:

D-Link DWL-A650

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

Description

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

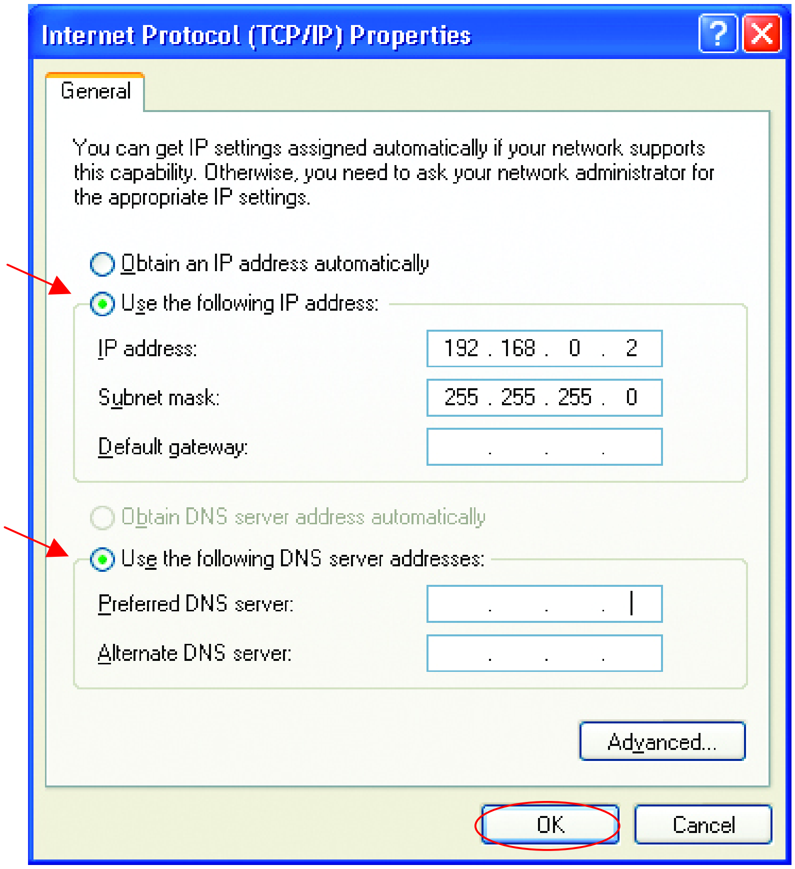
□ Show icon in notification area when connected

Download from Www.Somanuals.com. All Manuals Search And Download.

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.)



Internet Protocol (TCP/IP) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

Click **OK**

Download from Www.Somanuals.com. All Manuals Search And Download.

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.)

Download from Www.Somanuals.com. All Manuals Search And Download.

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

Download from Www.Somanuals.com. All Manuals Search And Download.

Limited Warranty and Registration

D-Link

1-Year

Limited Warranty

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

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

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

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

- Hardware (including power supplies and fans) One (1) Year
- Spare parts and spare kits Ninety (90) days.

D-Link's sole obligation shall be to repair or replace the defective Hardware at no charge to the original owner. Such repair or replacement will be rendered by D-Link at an Authorized D-Link Service Office. The replacement Hardware need not be new or of an identical make, model or part; D-Link may in its discretion replace the defective Hardware (or any part thereof) with any reconditioned product that D-Link reasonably determines is substantially equivalent (or superior) in all material respects to the defective Hardware. The Warranty Period shall extend for an additional ninety (90) days after any repaired or replaced Hardware is delivered. If a material defect is incapable of correction, or if D-Link determines in its sole discretion that it is not practical to repair or replace the defective Hardware, the price paid by the original purchaser for the defective Hardware will be refunded by D-Link upon return to D-Link of the defective Hardware. All Hardware (or part thereof) that is replaced by D-Link, or for which the purchase price is refunded, shall become the property of D-Link upon replacement or refund.

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

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

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

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

- The customer must submit as part of the claim a written description of the Hardware defect or Software nonconformance in sufficient detail to allow D-Link to confirm the same.
- The original product owner must obtain a Return Material Authorization (RMA) number from the Authorized D-Link Service Office and, if requested, provide written proof of purchase of the product (such as a copy of the dated purchase invoice for the product) before the warranty service is provided.

Download from Www.Somanuals.com. All Manuals Search And Download.

- 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.

Download from Www.Somanuals.com. All Manuals Search And Download.

- 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

Download from Www.Somanuals.com. All Manuals Search And Download.

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com