

Chapter 5

Managing Your Network

This chapter describes how to perform network management tasks with your FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Network Management Information

The FR328S provides a variety of status and usage information which is discussed below.

Viewing Router Status and Usage Statistics

From the Main Menu, under Maintenance, select Router Status to view the screen in [Figure 5-1](#).

The figure shows the Router Status screen from the FR328S web interface. On the left is a vertical menu bar with the following options:

- Maintenance
 - Router Status
 - Attached Devices
 - Settings Backup
 - Set Password
 - Diagnostics
 - Router Upgrade

The main content area is titled "Router Status". It displays two tables of network configuration and status information:

System Name	
FR328S	Firmware Version
Version 1.0 Release 10	

WAN Port	
MAC Address	00:09:5b:2a:24:05
IP Address	0.0.0.0
DHCP	Dynamic
IP Subnet Mask	0.0.0.0
Domain Name Server	10.1.1.6 10.1.1.7

LAN Port	
MAC Address	00:09:5b:2a:24:04
IP Address	192.168.0.1
DHCP	ON
IP Subnet Mask	255.255.255.0

At the bottom of the screen are two buttons: "Show Statistics" and "Show WAN Status".

Figure 5-1: Router Status screen

The Router Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, under Maintenance, select Router Status to view the status screen, shown in [Figure 5-1](#).

This screen shows the following parameters:

Table 5-1. Menu 3.2 - Router Status Fields

Field	Description
System Name	This field displays the Host Name assigned to the firewall in the Basic Settings menu.
Firmware Version	This field displays the firewall firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the firewall.
MAC Address	This field displays the Ethernet MAC address being used by the Internet (WAN) port of the firewall.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the firewall. If no address is shown, the firewall cannot connect to the Internet.
DHCP	If set to None, the firewall is configured to use a fixed IP address on the WAN. If set to Client, the firewall is configured to obtain an IP address dynamically from the ISP
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the firewall.
Domain Name Servers (DNS)	This field displays the DNS Server IP addresses being used by the firewall. These addresses are usually obtained dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the firewall.
MAC Address	This field displays the Ethernet MAC address being used by the Local (LAN) port of the firewall.
IP Address	This field displays the IP address being used by the Local (LAN) port of the firewall. The default is 192.168.0.1
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the firewall. The default is 255.255.255.0
DHCP	If set to OFF, the firewall will not assign IP addresses to local PCs on the LAN. If set to ON, the firewall is configured to assign IP addresses to local PCs on the LAN.

Click on the “Show Statistics” button to display firewall usage statistics, as shown in [Figure 5-2](#) below:

The screenshot shows a table titled "System Up Time 3:10:5" displaying network port statistics. Below the table are controls for setting the poll interval.

System Up Time 3:10:5

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	10M/Half	6529	147307	0	118	0	3:10:5
LAN	100M/Full	8440	11540	0	673	404	3:10:5
Serial	Not Connected	0	0	n/a	0	0	0:0:0

Poll Interval : (secs) Set Interval Stop

Figure 5-2. Router Statistics screen

This screen shows the following statistics.:

Table 5-2. Router Statistics Fields

Field	Description
WAN, LAN, or Serial Port	The statistics for the WAN (Internet), LAN (local), and Serial ports. For each port, the screen displays:
Status	The link status of the port.
TxPkts	The number of packets transmitted on this port since reset or manual clear.
RxPkts	The number of packets received on this port since reset or manual clear.
Collisions	The number of collisions on this port since reset or manual clear.
Tx B/s	The current line utilization—percentage of current bandwidth used on this port.
Tx B/s	The average line utilization —average CLU for this port.
Up Time	The time elapsed since this port acquired link.
System up Time	The time elapsed since the last power cycle or reset.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.

Viewing Attached Devices

The Attached Devices menu contains a table of all IP devices that the firewall has discovered on the local network. From the Main Menu of the browser interface, under the Maintenance heading, select Attached Devices to view the table, shown in [Figure 5-3](#)

The screenshot shows the 'Attached Devices' page from the FVM318's web interface. On the left, a sidebar titled 'Maintenance' lists several options: Router Status, Attached Devices (which is selected and highlighted in blue), Set Password, Settings Backup, Diagnostics, and Router Upgrade. The main content area is titled 'Attached Devices'. It features a table with four rows of data. The table has three columns: 'IP Address', 'Device Name', and 'MAC Address'. The data is as follows:

IP Address	Device Name	MAC Address
192.168.0.35	NETGEARAC1B80	00:40:33:AC:1B:80
192.168.0.4	ATRON002568	00:04:32:00:25:68
192.168.0.2	PLAYROOM	00:A0:CC:3A:8F:9F
192.168.0.10	OFFICE	00:A0:CC:74:4C:76

A 'Refresh' button is located at the bottom of the table.

Figure 5-3: Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name, if available, and the Ethernet MAC address. Note that if the firewall is rebooted, the table data is lost until the firewall redisCOVERS the devices. To force the firewall to look for attached devices, click the Refresh button.

Viewing, Selecting, and Saving Logged Information

The firewall will log security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enabled content filtering in the Block Sites menu, the Logs page shows you when someone on your network tried to access a blocked site. If you enabled e-mail notification, you'll receive these logs in an e-mail message. If you don't have e-mail notification enabled, you can view the logs here. An example is shown below.

The screenshot shows the 'Logs' section of the Security menu. On the left is a sidebar with links: Security, Logs, Block Sites, Rules, Services, Schedule, and E-mail. The 'Logs' link is highlighted. The main area has a title 'Logs' and a date header 'Date: 2002-08-27 10:36:40'. Below is a scrollable list of log entries:

```

Tue, 2002-08-27 07:08:14 - NETGEAR activated
Tue, 2002-08-27 07:15:32 - Administrator login successful - IP:192.168.0.2
Tue, 2002-08-27 07:29:19 - UDP packet dropped - Source:10.1.1.170
,2775 WAN - Destination:10.1.1.63,161 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:29:21 - UDP packet dropped - Source:10.1.1.170
,3128 WAN - Destination:10.1.1.63,5632 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:32:47 - TCP packet dropped - Source:10.1.1.170
,4035 WAN - Destination:10.1.1.63,23[TELNET] LAN - [Inbound Default rule m
Tue, 2002-08-27 07:32:53 - TCP packet dropped - Source:10.1.1.170
,4071 WAN - Destination:10.1.1.63,3535 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:12 - TCP packet dropped - Source:10.1.1.170
,4094 WAN - Destination:10.1.1.63,280 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:31 - TCP packet dropped - Source:10.1.1.170
,4118 WAN - Destination:10.1.1.63,411 LAN - [Inbound Default rule match]
Tue, 2002-08-27 07:33:49 - TCP packet dropped - Source:10.1.1.170

```

Below the log list are three buttons: Refresh, Clear Log, and Send Log.

Include in Log

- All incoming and Outgoing traffic
- Attempted access to blocked sites
- Connections to the Web-based interface of this Router
- Router operation (start up, get time, etc)
- Known DoS attacks and Port Scans

Enable Syslog

Syslog server IP address:

Buttons: Apply, Cancel

Figure 5-4: Security Logs menu

Log entries are described in [Table 5-5](#)

Table 5-5: Security Log entry descriptions

Field	Description
Date and Time	The date and time the log entry was recorded.
Description or Action	The type of event and what action was taken if any.
Source IP	The IP address of the initiating device for this log entry.
Source port and interface	The service port number of the initiating device, and whether it originated from the LAN or WAN
Destination	The name or IP address of the destination device or website.
Destination port and interface	The service port number of the destination device, and whether it's on the LAN or WAN.

Log action buttons are described in [Table 5-6](#)

Table 5-6: Security Log action buttons

Field	Description
Refresh	Click this button to refresh the log screen.
Clear Log	Click this button to clear the log entries.
Send Log	Click this button to email the log immediately.
Apply	Click this button to apply the current settings.
Cancel	Click this button to clear the current settings.

Selecting What Information to Log

Besides the standard information listed above, you can choose to log additional information. Those optional selections are as follows:

- All incoming and outgoing traffic
- Attempted access to blocked site
- Connections to the Web-based interface of this Router

- Router operation (start up, get time, etc.)
- Known DoS attacks and Port Scans

Saving Log Files on a Server

You can choose to write the logs to a PC running a syslog program. To activate this feature, check the box under Syslog and enter the IP address of the server where the log file will be written.

Examples of log messages

Following are examples of log messages. In all cases, the log entry shows the timestamp as: Day, Year-Month-Date Hour:Minute:Second

Activation and Administration

Tue, 2002-05-21 18:48:39 - NETGEAR activated

[This entry indicates a power-up or reboot with initial time entry.]

Tue, 2002-05-21 18:55:00 - Administrator login successful - IP:192.168.0.2

Thu, 2002-05-21 18:56:58 - Administrator logout - IP:192.168.0.2

[This entry shows an administrator logging in and out from IP address 192.168.0.2.]

Tue, 2002-05-21 19:00:06 - Login screen timed out - IP:192.168.0.2

[This entry shows a time-out of the administrator login.]

Wed, 2002-05-22 22:00:19 - Log emailed

[This entry shows when the log was emailed.]

Dropped Packets

Wed, 2002-05-22 07:15:15 - TCP packet dropped - Source:64.12.47.28,4787,WAN - Destination:134.177.0.11,21,LAN - [Inbound Default rule match]

Sun, 2002-05-22 12:50:33 - UDP packet dropped - Source:64.12.47.28,10714,WAN - Destination:134.177.0.11,6970,LAN - [Inbound Default rule match]

Sun, 2002-05-22 21:02:53 - ICMP packet dropped - Source:64.12.47.28,0,WAN - Destination:134.177.0.11,0,LAN - [Inbound Default rule match]

[These entries show an inbound FTP (port 21) packet, UDP packet (port 6970), and ICMP packet (port 0) being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

Enabling Security Event E-mail Notification

In order to receive logs and alerts by e-mail, you must provide your e-mail information in the E-Mail subheading:

Security

- Logs
- Block Sites
- Rules
- Services
- Schedule
- E-mail

E-mail

Turn e-mail notification on

Send alert and logs by e-mail

Outgoing Mail Server

E-mail Address

Send E-Mail alerts immediately

If a DoS attack is detected.

If a Port Scan is detected.

If someone attempts to access a blocked site.

Send logs according to this schedule

Daily

Day a.m. p.m.

Time a.m. p.m.

- Turn e-mail notification on

Check this box if you wish to receive e-mail logs and alerts from the firewall.

- Your outgoing mail server

Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You may be able to find this information in the configuration menu of your e-mail program. If you leave this box blank, log and alert messages will not be sent via e-mail.

- Send to this e-mail address

Enter the e-mail address to which logs and alerts are sent. This e-mail address will also be used as the From address. If you leave this box blank, log and alert messages will not be sent via e-mail.

You can specify that logs are automatically sent to the specified e-mail address with these options:

- Send alert immediately

Check this box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.

- Send logs according to this schedule

Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.

- Day for sending log

Specifies which day of the week to send the log. Relevant when the log is sent weekly or daily.

- Time for sending log

Specifies the time of day to send the log. Relevant when the log is sent daily or weekly.

If the Weekly, Daily or Hourly option is selected and the log fills up before the specified period, the log is automatically e-mailed to the specified e-mail address. After the log is sent, the log is cleared from the firewall's memory. If the firewall cannot e-mail the log file, the log buffer may fill up. In this case, the firewall overwrites the log and discards its contents.

Backing Up, Restoring, or Erasing Your Settings

The configuration settings of the FVM318 firewall are stored in a configuration file in the firewall. This file can be backed up to your computer, restored, or reverted to factory default settings. The procedures below explain how to do these tasks.



Procedure 5-5: Backup the Configuration to a File

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the firewall.

2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in **Figure 5-7**.

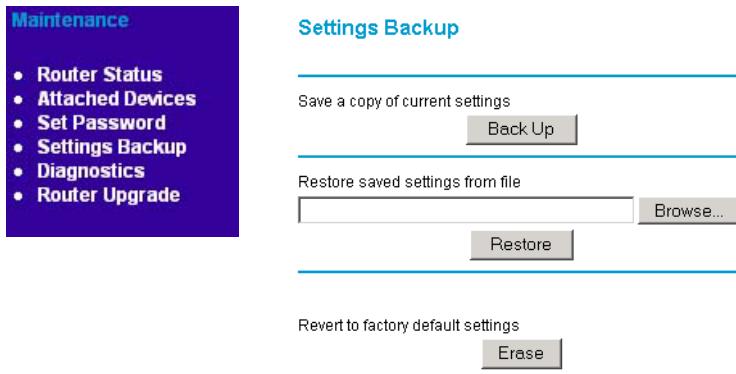


Figure 5-7: Settings Backup menu

3. Click **Backup** to save a copy of the current settings.
4. Store the .cfg file on a computer on your network.



Procedure 5-6: Restore a Configuration from a File

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the firewall.
2. From the Maintenance heading of the Main Menu, select the Settings Backup menu as seen in [Figure 5-7](#).
3. Enter the full path to the file on your network or click the Browse button to browse to the file.
4. When you have located the .cfg file, click the Restore button to upload the file to the firewall.
5. The firewall will then reboot automatically.



Procedure 5-7: Erase the Configuration

It is sometimes desirable to restore the firewall to the factory default settings. This can be done by using the Erase function.

1. To erase the configuration, from the Maintenance menu Settings Backup link, click the Erase button on the screen.
2. The firewall will then reboot automatically.

After an erase, the firewall's password will be **password**, the LAN IP address will be 192.168.0.1, and the router's DHCP client will be enabled.

Note: To restore the factory default configuration settings without knowing the login password or IP address, you must use the Default Reset button on the rear panel of the firewall. See “[Using the Default Reset button](#)“ on page 8-8.

Running Diagnostic Utilities and Rebooting the Router

The FVM318 firewall has a diagnostics feature. You can use the diagnostics menu to perform the following functions from the firewall:

- Ping an IP Address to test connectivity to see if you can reach a remote host.
- Perform a DNS Lookup to test if an Internet name resolves to an IP address to verify that the DNS server configuration is working.
- Display the Routing Table to identify what other routers the router is communicating with.
- Trace the Routing Path to identify any connectivity or congestion problems in the network.
- Reboot the Router to enable new network configurations to take effect or to clear problems with the router's network connection.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Diagnostics heading to display the menu shown in [Figure 5-8](#).

The screenshot shows the 'Maintenance' menu on the left with 'Diagnostics' selected. The main area is titled 'Diagnostics' and contains five sections: 'Ping an IP address', 'Perform a DNS Lookup', 'Display the Routing table', 'Trace the routing path', and 'Reboot the router'. Each section has input fields and a corresponding button ('Ping', 'Lookup', 'Display', 'TraceRoute', 'Reboot').

Maintenance
• Router Status
• Attached Devices
• Set Password
• Settings Backup
• Diagnostics
• Router Upgrade

Diagnostics

Ping an IP address

Internet Name

Perform a DNS Lookup

Internet Name

Display the Routing table

Trace the routing path

To this IP address

Reboot the router

Figure 5-8: Diagnostics menu

Enabling Remote Management

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your NETGEAR Cable/DSL ProSafe VPN Firewall.



Note: Be sure to change the router's default password to a very secure password. The ideal password should contain no dictionary words from any language, and should be a mixture of letters (both upper and lower case), numbers, and symbols. Your password can be up to 30 characters.



Procedure 5-8: Configure Remote Management

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the firewall.
2. Select the Allow Remote Management check box.
3. Specify what external addresses will be allowed to access the firewall's remote management.

For security, NETGEAR recommends that you restrict access to as few external IP addresses as practical.

- a. To allow access from any IP address on the Internet, select Everyone.
 - b. To allow access from a range of IP addresses on the Internet, select IP address range. Enter a beginning and ending IP address to define the allowed range.
 - c. To allow access from a single IP address on the Internet, select Only this PC. Enter the IP address that will be allowed access.
4. Specify the Port Number that will be used for accessing the management interface.

Web browser access normally uses the standard HTTP service port 80. For greater security, you can change the remote management web interface to a custom port by entering that number in the box provided. Choose a number between 1024 and 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.
 5. Click Apply to have your changes take effect.

When accessing your router from the Internet, you will type your router's WAN IP address into your browser's Address (in IE) or Location (in Netscape) box, followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter in your browser:

`http://134.177.0.123:8080`

Upgrading the Router's Firmware

The software of the FVM318 firewall is stored in FLASH memory, and can be upgraded as new software is released by NETGEAR.

Upgrade files can be downloaded from NETGEAR's website. If the upgrade file is compressed (.ZIP file), you must first extract the binary (.BIN or .IMG) file before uploading it to the firewall.

Note: The Web browser used to upload new firmware into the firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or Netscape Navigator 4.7 and above.



Procedure 5-1: Router Upgrade

1. Download and unzip the new software file from NETGEAR.
2. Log in to the firewall at its default LAN address of `http://192.168.0.1` with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the firewall.
3. From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown in [Figure 5-9](#).

A screenshot of a web-based configuration interface. On the left, there is a vertical navigation menu with a purple background and white text, titled "Maintenance". It contains a bulleted list: "Router Status", "Attached Devices", "Set Password", "Settings Backup", "Diagnostics", and "Router Upgrade". The "Router Upgrade" item is highlighted with a blue border. To the right of this menu is the main content area, which has a white background. At the top of the content area, the title "Router Upgrade" is displayed in blue. Below the title, there is a form field with the placeholder text "Locate and select the upgrade file from your hard disk:". To the right of this field is a "Browse..." button. At the bottom of the form are two buttons: "Upload" and "Cancel".

Maintenance

- Router Status
- Attached Devices
- Set Password
- Settings Backup
- Diagnostics
- Router Upgrade

Router Upgrade

Locate and select the upgrade file from your hard disk:

Upload Cancel

Figure 5-9: Router Upgrade menu

4. In the Router Upgrade menu, click the **Browse** to locate the binary (.BIN or .IMG) upgrade file.
5. Click **Upload**.

Note: When uploading software to the firewall, it is important not to interrupt the Web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it may corrupt the software. When the upload is complete, your firewall will automatically restart. The upgrade process will typically take about one minute. In some cases, you may need to clear the configuration and reconfigure the firewall after upgrading.

Chapter 6

Wireless Configuration

This chapter describes how to configure the wireless features of your DG824M Wireless ADSL Modem Gateway.

Considerations For A Wireless Network

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your router in order to maximize the network speed. For further information on wireless networking, refer to “[Wireless Networking](#)” in [Appendix B, “Network, Routing, Firewall, and Wireless Basics.”](#)

Security

Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, NETGEAR strongly recommends that you make use of the security features of your wireless equipment. As a minimum security precaution, you should change the SSID setting of all devices on your network from the factory setting to a unique password. Restricting access by MAC address filtering adds another obstacle against unwanted hosts joining your network. To hinder a determined eavesdropper, you should enable Wired Equivalent Privacy (WEP) data encryption. However, there may be a significant degradation of the data throughput on the wireless link when WEP is enabled.

Placement and Range

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless router.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the router.

For best results, place your router:

- Near the center of the area in which your PCs will operate,
- In an elevated location such as a high shelf,
- Away from potential sources of interference, such as PCs, microwaves, and cordless phones,
- Away from large metal surfaces.

Wireless Settings

To configure the Wireless interface of your router, click on the Wireless heading in the Main Menu of the browser interface. The Wireless Settings menu will appear, as shown in [Figure 6-1](#):

The screenshot shows the 'Wireless Settings' page of a web-based configuration interface. On the left, a vertical navigation bar lists 'Setup' at the top, followed by three bullet points: 'Basic Settings', 'VPN Settings', and 'Wireless Settings'. The 'Wireless Settings' option is highlighted with a blue background. The main content area has a light gray background. At the top, the title 'Wireless Settings' is displayed in green. Below it, a section titled 'Wireless Network' contains three input fields: 'Name(SSID)' with the value 'Wireless', 'Region' with a dropdown menu showing '- Select Region -', and 'Channel' with a dropdown menu showing '6'. A horizontal line separates this from the 'Wireless Card Access List' section. This section includes two radio buttons: 'Everyone' (selected) and 'Trusted PCs only', and a 'Trusted PCs' button. Another horizontal line follows. The 'Security Encryption' section contains two dropdown menus: 'Authentication Type' set to 'Automatic' and 'Encryption Strength' set to 'IPSec'. A horizontal line is present below this. At the bottom of the page are three buttons: 'Add', 'Edit', and 'Delete' on the left, and 'Apply' and 'Cancel' on the right.

Figure 6-1: Wireless Settings menu

Wireless Network Settings

In the Wireless Network section are the following parameters:

- SSID (Service Set ID)

Enter a value of up to 32 alphanumeric characters. The same SSID must be assigned to all wireless devices in your network. The default SSID is **Wireless**, but NETGEAR strongly recommends that you change your network's SSID to a different value.



Note: The SSID of any wireless access cards must match the SSID you configure in the DG824M Wireless ADSL Modem Gateway. If they do not match, you will not get a wireless connection to the DG824M.

- Region

This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the router in a region other than the region shown here.

- Channel

This field determines which operating frequency will be used. It should not be necessary to change the wireless channel unless you notice interference problems with another nearby access point.

Be sure to click **Apply** to save any settings from this menu.



Note: If you are configuring the router from a wireless PC and you change the router's SSID, channel, or WEP settings, you will lose your wireless connection when you click on **Apply**. You must then change the wireless settings of your PC to match the router's new settings.

Using the Wireless Card Access List to Restrict Wireless Access by MAC Address

By default, any wireless PC that is configured with the correct SSID will be allowed access to your network. For increased security, you can restrict access to the wireless network to only allow specific PCs based on their MAC addresses. From the Wireless Settings menu, click the Trusted PCs button to display the Wireless Access menu, shown in [Figure 6-2](#):

The screenshot shows the 'Wireless Access' menu. At the top, there's a section titled 'Manually Add Trusted PC' with fields for 'Device Name' and 'MAC Address', and an 'Add' button. Below this is a table with columns for '#', 'Device Name', and 'MAC Address'. A 'Delete' button is located below the table. At the bottom is a 'Back' button.

#	Device Name	MAC Address

Figure 6-2: Wireless Access List menu

The Wireless Access window displays a list of MAC addresses that will be allowed to connect to the router. These PCs must also have the correct SSID and WEP settings. To restrict access based on MAC addresses:

1. Click the Add button to go to the Add/Edit menu shown in:
For your convenience, this menu displays a list of currently active wireless cards and their Ethernet MAC addresses.
2. If the desired PC appears in the list, you can click on it to capture its MAC address; otherwise, you can manually enter the MAC address of the authorized PC.
The MAC address is usually printed on the wireless card.
3. If no Device Name appears, you can type a descriptive name for the PC that you are adding.
4. Click Add.
5. When you have finished entering MAC addresses, return to the Wireless Access List menu and check the Turn Access Control On box, then click Apply.

To edit a MAC address from the table, click on it to select it, then click the Edit or Delete button.

Configuring Wired Equivalent Privacy (WEP)

In the Wireless Settings menu you can configure WEP data encryption using the following parameters:

- Authentication Type

Normally this can be left at the default value of "Automatic." If that fails, select the appropriate value - "Open System" or "Shared Key." Check your wireless card's documentation to see what method to use.

- Encryption Strength

Select the WEP Encryption level:

- Off - no data encryption (Open System)
- 64-bit (sometimes called 40-bit) encryption
- 128-bit encryption

- Keys

If WEP is enabled, you can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.

- Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
- Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F)
Select which of the four keys will be active.

Be sure to click Apply to save your settings in this menu.

Chapter 7

Advanced Configuration

This chapter describes how to configure the advanced features of your FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Configuring Advanced Security

The FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall provides a variety of advanced features, such as:

- Setting up a Demilitarized Zone (DMZ) Server
- The flexibility of configuring your LAN TCP/IP settings
- Connecting a Remote Access Server through the serial port

These features are discussed below.

Setting Up A Default DMZ Server

The Default DMZ Server feature is helpful when using some online games and videoconferencing applications that are incompatible with NAT. The firewall is programmed to recognize some of these applications and to work properly with them, but there are other applications that may not function well. In some cases, one local PC can run the application properly if that PC's IP address is entered as the Default DMZ Server.



Note: For security, you should avoid using the Default DMZ Server feature. When a computer is designated as the Default DMZ Server, it loses much of the protection of the firewall, and is exposed to many exploits from the Internet. If compromised, the computer can be used to attack your network.

Incoming traffic from the Internet is normally discarded by the firewall unless the traffic is a response to one of your local computers or a service that you have configured in the Ports menu. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the Default DMZ Server.

To assign a computer or server to be a Default DMZ server:

1. Click Default DMZ Server.
2. Type the IP address for that server.
3. Click Apply.

Respond to Ping on Internet WAN Port

If you want the firewall to respond to a 'ping' from the Internet, click the 'Respond to Ping on Internet WAN Port' check box. This should only be used as a diagnostic tool, since it allows your firewall to be discovered. Don't check this box unless you have a specific reason to do so.

Configuring LAN IP Settings

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP and RIP. These features can be found under the Advanced heading in the Main Menu of the browser interface.

LAN TCP/IP Setup

The firewall is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The firewall's default LAN IP configuration is:

- LAN IP addresses—192.168.0.1
- Subnet mask—255.255.255.0

These addresses are part of the IETF-designated private address range for use in private networks, and should be suitable in most applications. If your network has a requirement to use a different IP addressing scheme, you can make those changes in this menu.

The LAN TCP/IP Setup parameters are:

- IP Address
This is the LAN IP address of the firewall.

- IP Subnet Mask

This is the LAN Subnet Mask of the firewall. Combined with the IP address, the IP Subnet Mask allows a device to know which other addresses are local to it, and which must be reached through a gateway or router.

- RIP Direction

RIP (Router Information Protocol) allows a router to exchange routing information with other routers. The RIP Direction selection controls how the firewall sends and receives RIP packets. Both is the default.

- When set to Both or Out Only, the firewall will broadcast its routing table periodically.
- When set to Both or In Only, it will incorporate the RIP information that it receives.
- When set to None, it will not send any RIP packets and will ignore any RIP packets received.

- RIP Version

This controls the format and the broadcasting method of the RIP packets that the router sends. It recognizes both formats when receiving. By default, this is set for RIP-1.

- RIP-1 is universally supported. RIP-1 is probably adequate for most networks, unless you have an unusual network setup.
- RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format.
 - RIP-2B uses subnet broadcasting.
 - RIP-2M uses multicasting.



Note: If you change the LAN IP address of the firewall while connected through the browser, you will be disconnected. You must then open a new connection to the new IP address and log in again.

MTU Size

The normal MTU (Maximum Transmit Unit) value for most Ethernet networks is 1500 Bytes. For some ISPs, particularly some using PPPoE, you may need to reduce the MTU. This is rarely required, and should not be done unless you are sure it is necessary for your ISP connection.

Any packets sent through the firewall that are larger than the configured MTU size will be repackaged into smaller packets to meet the MTU requirement. To change the MTU size:

1. Under MTU Size, select Custom.

2. Enter a new size between 64 and 1500.
3. Click Apply to save the new configuration.

DHCP

By default, the firewall will function as a DHCP (Dynamic Host Configuration Protocol) server, allowing it to assign IP, DNS server, and default gateway addresses to all computers connected to the router's LAN. The assigned default gateway address is the LAN address of the firewall. IP addresses will be assigned to the attached PCs from a pool of addresses specified in this menu. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN.

For most applications, the default DHCP and TCP/IP settings of the firewall are satisfactory. See “[IP Configuration by DHCP” on page B-10](#)” for an explanation of DHCP and information about how to assign IP addresses for your network.

Use router as DHCP server

If another device on your network will be the DHCP server, or if you will manually configure the network settings of all of your computers, clear the ‘Use router as DHCP server’ check box. Otherwise, leave it checked.

Specify the pool of IP addresses to be assigned by setting the Starting IP Address and Ending IP Address. These addresses should be part of the same IP address subnet as the firewall’s LAN IP address. Using the default addressing scheme, you should define a range between 192.168.0.2 and 192.168.0.253, although you may wish to save part of the range for devices with fixed addresses.

The firewall will deliver the following parameters to any LAN device that requests DHCP:

- An IP Address from the range you have defined
- Subnet Mask
- Gateway IP Address is the firewall’s LAN IP address
- Primary DNS Server, if you entered a Primary DNS address in the Basic Settings menu; otherwise, the firewall’s LAN IP address
- Secondary DNS Server, if you entered a Secondary DNS address in the Basic Settings menu

- WINS Server, short for *Windows Internet Naming Service Server*, determines the IP address associated with a particular Windows computer. A WINS server records and reports a list of names and IP address of Windows PCs on its local network. If you connect to a remote network that contains a WINS server, enter the server's IP address here. This allows your PCs to browse the network using the Network Neighborhood feature of Windows.

Reserved IP addresses

When you specify a reserved IP address for a PC on the LAN, that PC will always receive the same IP address each time it access the firewall's DHCP server. Reserved IP addresses should be assigned to servers that require permanent IP settings.

To reserve an IP address:

1. Click the **Add** button.
2. In the IP Address box, type the IP address to assign to the PC or server.
Choose an IP address from the router's LAN subnet, such as 192.168.0.X.
3. Type the MAC Address of the PC or server.
Tip: If the PC is already present on your network, you can copy its MAC address from the Attached Devices menu and paste it here.
4. Click **Apply** to enter the reserved address into the table.

Note: The reserved address will not be assigned until the next time the PC contacts the router's DHCP server. Reboot the PC or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry:

1. Click the button next to the reserved address you want to edit or delete.
2. Click Edit or Delete.



Procedure 7-1: Configure LAN TCP/IP Setup

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the firewall.
2. From the Main Menu, under Advanced, click the LAN IP Setup link to view the menu, shown in [Figure 7-1](#)

Figure 7-1: LAN IP Setup Menu

3. Enter the TCP/IP, MTU, or DHCP parameters.
4. Click Apply to save your changes.

Configuring Dynamic DNS

If your network has a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). However, if your Internet account uses a dynamically assigned IP address, you will not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial dynamic DNS service, who will allow you to register your domain to their IP address, and will forward traffic directed at your domain to your frequently-changing IP address.

The firewall contains a client that can connect to a dynamic DNS service provider. To use this feature, you must select a service provider and obtain an account with them. After you have configured your account information in the firewall, whenever your ISP-assigned IP address changes, your firewall will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.



Procedure 7-2: Configure Dynamic DNS

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the firewall.
2. From the Main Menu of the browser interface, under Advanced, click on Dynamic DNS.
3. Access the website of one of the dynamic DNS service providers whose names appear in the ‘Select Service Provider’ box, and register for an account.
For example, for dyndns.org, go to www.dyndns.org.
4. Select the “Use a dynamic DNS service” check box.
5. Select the name of your dynamic DNS Service Provider.
6. Type the Host Name that your dynamic DNS service provider gave you.
The dynamic DNS service provider may call this the domain name. If your URL is myName.dyndns.org, then your Host Name is “myName.”
7. Type the User Name for your dynamic DNS account.
8. Type the Password (or key) for your dynamic DNS account.
9. If your dynamic DNS provider allows the use of wildcards in resolving your URL, you may select the Use wildcards check box to activate this feature.
For example, the wildcard feature will cause *.yourhost.dyndns.org to be aliased to the same IP address as yourhost.dyndns.org
10. Click Apply to save your configuration.



Note: If your ISP assigns a private WAN IP address such as 192.168.x.x or 10.x.x.x, the dynamic DNS service will not work because private addresses will not be routed on the Internet.

Using Static Routes

Static Routes provide additional routing information to your firewall. Under normal circumstances, the firewall has adequate routing information after it has been configured for Internet access, and you do not need to configure additional static routes. You must configure static routes only for unusual cases such as multiple routers or multiple IP subnets located on your network.

Static Route Example

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN router on your home network for connecting to the company where you are employed. This router's address on your LAN is 192.168.0.100.
- Your company's network is 134.177.0.0.

When you first configured your firewall, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your firewall will forward your request to the ISP. The ISP forwards your request to the company where you are employed, and the request will likely be denied by the company's firewall.

In this case you must define a static route, telling your firewall that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like [Figure 7-3](#).

In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address fields specifies that all traffic for these addresses should be forwarded to the ISDN router at 192.168.0.100.
- A Metric value of 1 will work since the ISDN router is on the LAN.
This represents the number of routers between your network and the destination. This is a direct connection so it is set to 1.
- Private is selected only as a precautionary security measure in case RIP is activated.



Procedure 7-3: Configuring Static Routes

1. Log in to the firewall at its default LAN address of <http://192.168.0.1> with its default User Name of **admin**, default password of **password**, or using whatever User Name, Password and LAN address you have chosen for the firewall.
2. From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Routes menu, shown in [Figure 7-2](#).

#	Name	Destination	Gateway	Metric	Active	Private

Add Edit Delete

Figure 7-2: Static Routes Table

3. To add or edit a Static Route:
 - a. Click the **Edit** button to open the Edit Menu, shown in [Figure 7-3](#).

Route Name	isdn_router
<input checked="" type="checkbox"/> Active	<input checked="" type="checkbox"/> Private
Destination IP Address	134.177.0.0
IP Subnet Mask	255.255.0.0
Gateway IP Address	192.168.0.100
Metric	1

Apply Cancel

Figure 7-3: Static Route Entry and Edit Menu

- b. Type a route name for this static route in the Route Name box under the table. This is for identification purpose only.
- c. Select **Active** to make this route effective.

- d. Select **Private** if you want to limit access to the LAN only.
The static route will not be reported in RIP.
 - e. Type the Destination IP Address of the final destination.
 - f. Type the IP Subnet Mask for this destination.
If the destination is a single host, type 255.255.255.255.
 - g. Type the Gateway IP Address, which must be a router on the same LAN segment as the firewall.
 - h. Type a number between 1 and 15 as the Metric value.
This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
4. Click **Apply** to have the static route entered into the table.

Chapter 8

Troubleshooting

This chapter gives information about troubleshooting your FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall. For the common problems listed, go to the section indicated.

- Is the firewall on?
- Have I connected the firewall correctly?

Go to “[Basic Functions](#)“ on page 8-1.

- I can’t access the firewall’s configuration with my browser.

Go to “[Troubleshooting the Web Configuration Interface](#)“ on page 8-4.

- I’ve configured the firewall but I can’t access the Internet.

Go to “[Troubleshooting the ISP Connection](#)“ on page 8-5.

- I can’t remember the firewall’s configuration password.
- I want to clear the configuration and start over again.

Go to “[Restoring the Default Configuration and Password](#)“ on page 8-8.

Basic Functions

After you turn on power to the firewall, the following sequence of events should occur:

1. When power is first applied, verify that the Power LED is on.
2. Verify that the Test LED lights within a few seconds, indicating that the self-test procedure is running.
3. After approximately 10 seconds, verify that:
 - a. The Test LED is not lit.

- b. The Local port Link LEDs are lit for any local ports that are connected.
- c. The Internet Link port LED is lit.

If a port's Link LED is lit, a link has been established to the connected device. If a port is connected to a 100 Mbps device, verify that the port's 100 LED is lit.

If any of these conditions does not occur, refer to the appropriate following section.

Power LED Not On

If the Power and other LEDs are off when your firewall is turned on:

- Make sure that the power cord is properly connected to your firewall and that the power supply adapter is properly connected to a functioning power outlet.
- Check that you are using the 12VDC power adapter supplied by NETGEAR for this product.

If the error persists, you have a hardware problem and should contact technical support.

Test LED Never Turns On or Test LED Stays On

When the firewall is turned on, the Test LED turns on for about 10 seconds and then turns off. If the Test LED does not turn on, or if it stays on, there is a fault within the firewall.

If you experience problems with the Test LED:

- Cycle the power to see if the firewall recovers and the LED blinks for the correct amount of time.

If all LEDs including the Test LED are still on one minute after power up:

- Cycle the power to see if the firewall recovers.
- Clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.0.1. This procedure is explained in “[Using the Default Reset button](#)“ on page 8-8.

If the error persists, you might have a hardware problem and should contact technical support.

Local or Internet Port Link LEDs Not On

If either the Local or Internet Port Link LEDs do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the firewall and at the hub or PC.
- Make sure that power is turned on to the connected hub or PC.
- Be sure you are using the correct cable:
 - When connecting the firewall's Internet port to a cable or DSL modem, use the cable that was supplied with the cable or DSL modem. This cable could be a standard straight-through Ethernet cable or an Ethernet crossover cable.

Troubleshooting the Web Configuration Interface

If you are unable to access the firewall's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the firewall as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the firewall. If you are using the recommended addressing scheme, your PC's address should be in the range of 192.168.0.2 to 192.168.0.254. Refer to “[Verifying TCP/IP Properties](#)“ on page C-5 or “[Configuring the Macintosh for TCP/IP Networking](#)“ on page C-6 to find your PC's IP address. Follow the instructions in [Appendix C](#) to configure your PC.

Note: If your PC's IP address is shown as 169.254.x.x:

Recent versions of Windows and MacOS will generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the PC to the firewall and reboot your PC.

- If your firewall's IP address has been changed and you don't know the current IP address, clear the firewall's configuration to factory defaults. This will set the firewall's IP address to 192.168.0.1. This procedure is explained in “[Using the Default Reset button](#)“ on page 8-8.
- Make sure your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure you are using the correct login information. The factory default login name is **admin** and the password is **password**. Make sure that CAPS LOCK is off when entering this information.

If the firewall does not save changes you have made in the Web Configuration Interface, check the following:

- When entering configuration settings, be sure to click the APPLY button before moving to another menu or tab, or your changes are lost.
- Click the Refresh or Reload button in the Web browser. The changes may have occurred, but the Web browser may be caching the old configuration.

Troubleshooting the ISP Connection

If your firewall is unable to access the Internet, you should first determine whether the firewall is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your firewall must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as www.netgear.com
2. Access the Main Menu of the firewall's configuration at <http://192.168.0.1>
3. Under the Maintenance heading, select Router Status
4. Check that an IP address is shown for the WAN Port
If 0.0.0.0 is shown, your firewall has not obtained an IP address from your ISP.

If your firewall is unable to obtain an IP address from the ISP, you may need to force your cable or DSL modem to recognize your new firewall by performing the following procedure:

1. Turn off power to the cable or DSL modem.
2. Turn off power to your firewall.
3. Wait five minutes and reapply power to the cable or DSL modem.
4. When the modem's LEDs indicate that it has reacquired sync with the ISP, reapply power to your firewall.

If your firewall is still unable to obtain an IP address from the ISP, the problem may be one of the following:

- Your ISP may require a login program.
Ask your ISP whether they require PPP over Ethernet (PPPoE) or some other type of login.
- If your ISP requires a login, you may have incorrectly set the login name and password.
- Your ISP may check for your PC's host name.
Assign the PC Host Name of your ISP account as the Account Name in the Basic Settings menu.
- Your ISP only allows one Ethernet MAC address to connect to Internet, and may check for your PC's MAC address. In this case:

Inform your ISP that you have bought a new network device, and ask them to use the firewall's MAC address.

OR

Configure your firewall to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to “[“ on page 2-21](#).

If your firewall can obtain an IP address, but your PC is unable to load any web pages from the Internet:

- Your PC may not recognize any DNS server addresses.

A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP will provide the addresses of one or two DNS servers for your use. If you entered a DNS address during the firewall's configuration, reboot your PC and verify the DNS address as described in “[Verifying TCP/IP Properties“ on page C-6](#). Alternatively, you may configure your PC manually with DNS addresses, as explained in your operating system documentation.

- Your PC may not have the firewall configured as its TCP/IP gateway.

If your PC obtains its information from the firewall by DHCP, reboot the PC and verify the gateway address as described in “[Verifying TCP/IP Properties“ on page C-6](#).

Troubleshooting a TCP/IP Network Using a Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. Troubleshooting a TCP/IP network is made easier by using the ping utility in your PC or workstation.

Testing the LAN Path to Your Firewall

You can ping the firewall from your PC to verify that the LAN path to your firewall is set up correctly.

To ping the firewall from a PC running Windows 95 or later:

1. From the Windows toolbar, click on the Start button and select Run.
2. In the field provided, type Ping followed by the IP address of the firewall, as in this example:

`ping 192.168.0.1`

3. Click on OK.

You should see a message like this one:

Pinging <IP address> with 32 bytes of data

If the path is working, you see this message:

Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

If the path is not working, you see this message:

Request timed out

If the path is not functioning correctly, you could have one of the following problems:

- Wrong physical connections
 - Make sure the LAN port LED is on. If the LED is off, follow the instructions in “[Local or Internet Port Link LEDs Not On](#)” on [page 8-2](#).
 - Check that the corresponding Link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and firewall.
- Wrong network configuration
 - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your PC or workstation.
 - Verify that the IP address for your firewall and your workstation are correct and that the addresses are on the same subnet.

Testing the Path from Your PC to a Remote Device

After verifying that the LAN path works correctly, test the path from your PC to a remote device. From the Windows run menu, type:

PING -n 10 <IP address>

where *<IP address>* is the IP address of a remote device such as your ISP’s DNS server.

If the path is functioning correctly, replies as in the previous section are displayed. If you do not receive replies:

- Check that your PC has the IP address of your firewall listed as the default gateway. If the IP configuration of your PC is assigned by DHCP, this information will not be visible in your PC’s Network Control Panel. Verify that the IP address of the firewall is listed as the default gateway as described in “[Verifying TCP/IP Properties](#)” on [page C-5](#).
- Check to see that the network address of your PC (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.

- If your ISP assigned a host name to your PC, enter that host name as the Account Name in the Basic Settings menu.
- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your PCs. Many broadband ISPs restrict access by only allowing traffic from the MAC address of your broadband modem, but some ISPs additionally restrict access to the MAC address of a single PC connected to that modem. If this is the case, you must configure your firewall to “clone” or “spoof” the MAC address from the authorized PC. Refer to “[“ on page 2-21](#).

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the firewall’s administration password to **password** and the IP address to 192.168.0.1. You can erase the current configuration and restore factory defaults in two ways:

- Use the Erase function of the Web Configuration Manager (see “[Backing Up, Restoring, or Erasing Your Settings“ on page 5-9](#)).
- Use the Default Reset button on the rear panel of the firewall. Use this method for cases when the administration password or IP address is not known.

Using the Default Reset button

To restore the factory default configuration settings without knowing the administration password or IP address, you must use the Default Reset button on the rear panel of the firewall.

To restore the factory default configuration settings, follow these steps:

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).

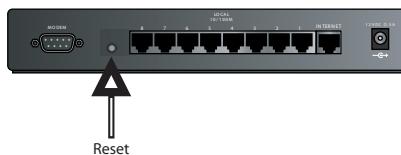


Figure 8-1.Reset Button

2. Release the Default Reset button and wait for the firewall to reboot.

Problems with Date and Time

The E-Mail menu in the Content Filtering section displays the current date and time of day. The FVM318 firewall uses the Network Time Protocol (NTP) to obtain the current time from one of several Network Time Servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include:

- Date shown is January 1, 2000

Cause: The firewall has not yet successfully reached a Network Time Server. Check that your Internet access settings are configured correctly. If you have just completed configuring the firewall, wait at least five minutes and check the date and time again.

- Time is off by one hour

Cause: The firewall does not automatically sense Daylight Savings Time. In the E-Mail menu, check or uncheck the box marked “Adjust for Daylight Savings Time”.

Appendix A

Technical Specifications

This appendix provides technical specifications for the FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall.

Network Protocol and Standards Compatibility

Data and Routing Protocols: TCP/IP, RIP-1, RIP-2, DHCP
 PPP over Ethernet (PPPoE)

Power Adapter

North America:	120V, 60 Hz, input
United Kingdom, Australia:	240V, 50 Hz, input
Europe:	230V, 50 Hz, input
Japan:	100V, 50/60 Hz, input
All regions (output):	12 V DC @ 1.2A output, 20W maximum

Physical Specifications

Dimensions:	H: 1.56 in (3.96 cm) W: 10.0 in (25.4 cm) D: 9.0 in (17.8 cm)
Weight:	2.72 lb. (1.23 Kg)

Environmental Specifications

Operating temperature: 32°-140° F (0° to 40° C)

Operating humidity: 90% maximum relative humidity, noncondensing

Electromagnetic Emissions

Meets requirements of: FCC Part 15 Class B

VCCI Class B

EN 55 022 (CISPR 22), Class B

Interface Specifications

Local: 10BASE-T or 100BASE-Tx, RJ-45

Internet: 10BASE-T or 100BASE-Tx, RJ-45

Appendix B

Network, Routing, Firewall, and Wireless Basics

This chapter provides an overview of IP networks, routing, and wireless networking.

Related Publications

As you read this document, you may be directed to various RFC documents for further information. An RFC is a Request For Comment (RFC) published by the Internet Engineering Task Force (IETF), an open organization that defines the architecture and operation of the Internet. The RFC documents outline and define the standard protocols and procedures for the Internet. The documents are listed on the World Wide Web at www.ietf.org and are mirrored and indexed at many other sites worldwide.

Basic Router Concepts

Large amounts of bandwidth can be provided easily and relatively inexpensively in a local area network (LAN). However, providing high bandwidth between a local network and the Internet can be very expensive. Because of this expense, Internet access is usually provided by a slower-speed wide-area network (WAN) link such as a cable or DSL modem. In order to make the best use of the slower WAN link, a mechanism must be in place for selecting and transmitting only the data traffic meant for the Internet. The function of selecting and forwarding this data is performed by a router.

What is a Router?

A router is a device that forwards traffic between networks based on network layer information in the data and on routing tables maintained by the router. In these routing tables, a router builds up a logical picture of the overall network by gathering and exchanging information with other routers in the network. Using this information, the router chooses the best path for forwarding network traffic.

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall is a small office router that routes the IP protocol over a single-user broadband connection.

Routing Information Protocol

One of the protocols used by a router to build and maintain a picture of the network is the Routing Information Protocol (RIP). Using RIP, routers periodically update one another and check for changes to add to the routing table.

The FVM318 firewall supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

Because TCP/IP networks are interconnected across the world, every machine on the Internet must have a unique address to make sure that transmitted data reaches the correct destination. Blocks of addresses are assigned to organizations by the Internet Assigned Numbers Authority (IANA). Individual users and small organizations may obtain their addresses either from the IANA or from an Internet service provider (ISP). You can contact IANA at www.iana.org.

The Internet Protocol (IP) uses a 32-bit address structure. The address is usually written in dot notation (also called dotted-decimal notation), in which each group of eight bits is written in decimal form, separated by decimal points.

For example, the following binary address:

11000011 00100010 00001100 00000111

is normally written as:

195.34.12.7

The latter version is easier to remember and easier to enter into your computer.

In addition, the 32 bits of the address are subdivided into two parts. The first part of the address identifies the network, and the second part identifies the host node or station on the network. The dividing point may vary depending on the address range and the application.

There are five standard classes of IP addresses. These address classes have different ways of determining the network and host sections of the address, allowing for different numbers of hosts on a network. Each address type begins with a unique bit pattern, which is used by the TCP/IP software to identify the address class. After the address class has been determined, the software can correctly identify the host section of the address. The follow figure shows the three main address classes, including network and host sections of the address for each address type.

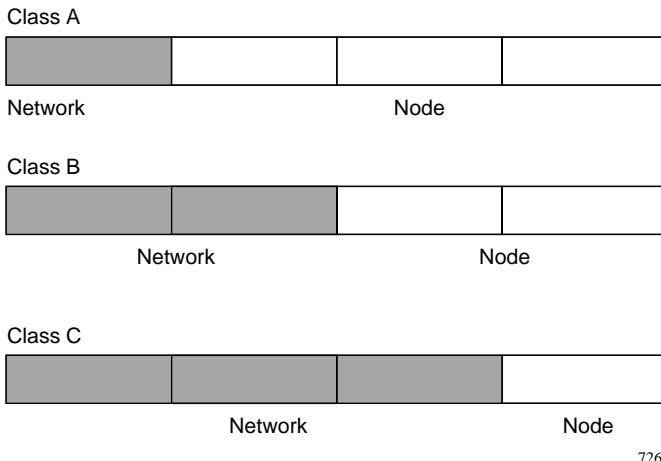


Figure 8-2: Three Main Address Classes

The five address classes are:

- Class A

Class A addresses can have up to 16,777,214 hosts on a single network. They use an eight-bit network number and a 24-bit node number. Class A addresses are in this range:

1.x.x.x to 126.x.x.x.

- Class B

Class B addresses can have up to 65,354 hosts on a network. A Class B address uses a 16-bit network number and a 16-bit node number. Class B addresses are in this range:

128.1.x.x to 191.254.x.x.

- Class C

Class C addresses can have 254 hosts on a network. Class C addresses use 24 bits for the network address and eight bits for the node. They are in this range:

192.0.1.x to 223.255.254.x.

- Class D

Class D addresses are used for multicasts (messages sent to many hosts). Class D addresses are in this range:

224.0.0.0 to 239.255.255.255.

- Class E

Class E addresses are for experimental use.

This addressing structure allows IP addresses to uniquely identify each physical network and each node on each physical network.

For each unique value of the network portion of the address, the base address of the range (host address of all zeros) is known as the network address and is not usually assigned to a host. Also, the top address of the range (host address of all ones) is not assigned, but is used as the broadcast address for simultaneously sending a packet to all hosts with the same network address.

Netmask

In each of the address classes previously described, the size of the two parts (network address and host address) is implied by the class. This partitioning scheme can also be expressed by a netmask associated with the IP address. A netmask is a 32-bit quantity that, when logically combined (using an AND operator) with an IP address, yields the network address. For instance, the netmasks for Class A, B, and C addresses are 255.0.0.0, 255.255.0.0, and 255.255.255.0, respectively.

For example, the address 192.168.170.237 is a Class C IP address whose network portion is the upper 24 bits. When combined (using an AND operator) with the Class C netmask, as shown here, only the network portion of the address remains:

11000000 10101000 10101010 11101101 (192.168.170.237)

combined with:

11111111 11111111 11111111 00000000 (255.255.255.0)

Equals:

11000000 10101000 10101010 00000000 (192.168.170.0)

As a shorter alternative to dotted-decimal notation, the netmask may also be expressed in terms of the number of ones from the left. This number is appended to the IP address, following a backward slash (/), as “/n.” In the example, the address could be written as 192.168.170.237/24, indicating that the netmask is 24 ones followed by 8 zeros.

Subnet Addressing

By looking at the addressing structures, you can see that even with a Class C address, there are a large number of hosts per network. Such a structure is an inefficient use of addresses if each end of a routed link requires a different network number. It is unlikely that the smaller office LANs would have that many devices. You can resolve this problem by using a technique known as subnet addressing.

Subnet addressing allows us to split one IP network address into smaller multiple physical networks known as subnetworks. Some of the node numbers are used as a subnet number instead. A Class B address gives us 16 bits of node numbers translating to 64,000 nodes. Most organizations do not use 64,000 nodes, so there are free bits that can be reassigned. Subnet addressing makes use of those bits that are free, as shown below.



Figure 8-3: Example of Subnetting a Class B Address

A Class B address can be effectively translated into multiple Class C addresses. For example, the IP address of 172.16.0.0 is assigned, but node addresses are limited to 255 maximum, allowing eight extra bits to use as a subnet address. The IP address of 172.16.97.235 would be interpreted as IP network address 172.16, subnet number 97, and node number 235. In addition to extending the number of addresses available, subnet addressing provides other benefits. Subnet addressing allows a network manager to construct an address scheme for the network by using different subnets for other geographical locations in the network or for other departments in the organization.

Although the preceding example uses the entire third octet for a subnet address, note that you are not restricted to octet boundaries in subnetting. To create more network numbers, you need only shift some bits from the host address to the network address. For instance, to partition a Class C network number (192.68.135.0) into two, you shift one bit from the host address to the network address. The new netmask (or subnet mask) is 255.255.255.128. The first subnet has network number 192.68.135.0 with hosts 192.68.135.1 to 129.68.135.126, and the second subnet has network number 192.68.135.128 with hosts 192.68.135.129 to 192.68.135.254.



Note: The number 192.68.135.127 is not assigned because it is the broadcast address of the first subnet. The number 192.68.135.128 is not assigned because it is the network address of the second subnet.

The following table lists the additional subnet mask bits in dotted-decimal notation. To use the table, write down the original class netmask and replace the 0 value octets with the dotted-decimal value of the additional subnet bits. For example, to partition your Class C network with subnet mask 255.255.255.0 into 16 subnets (4 bits), the new subnet mask becomes 255.255.255.240.

Table 8-1. Netmask Notation Translation Table for One Octet

Number of Bits	Dotted-Decimal Value
1	128
2	192
3	224
4	240
5	248
6	252
7	254
8	255

The following table displays several common netmask values in both the dotted-decimal and the masklength formats.

Table 8-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

Table 8-2. Netmask Formats

255.255.255.0	/24
255.255.255.128	/25
255.255.255.192	/26
255.255.255.224	/27
255.255.255.240	/28
255.255.255.248	/29
255.255.255.252	/30
255.255.255.254	/31
255.255.255.255	/32

NETGEAR strongly recommends that you configure all hosts on a LAN segment to use the same netmask for the following reasons:

- So that hosts recognize local IP broadcast packets

When a device broadcasts to its segment neighbors, it uses a destination address of the local network address with all ones for the host address. In order for this scheme to work, all devices on the segment must agree on which bits comprise the host address.

- So that a local router or bridge recognizes which addresses are local and which are remote

Private IP Addresses

If your local network is isolated from the Internet (for example, when using NAT), you can assign any IP addresses to the hosts without problems. However, the IANA has reserved the following three blocks of IP addresses specifically for private networks:

10.0.0.0 – 10.255.255.255
172.16.0.0 – 172.31.255.255
192.168.0.0 – 192.168.255.255

NETGEAR recommends that you choose your private network number from this range. The DHCP server of the FVM318 firewall is preconfigured to automatically assign private addresses.

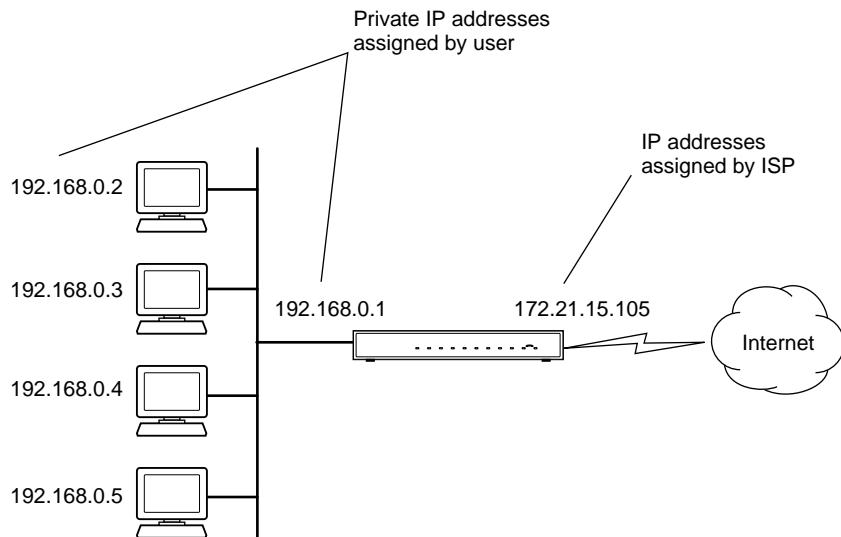
Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at www.ietf.org.

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The FVM318 firewall employs an address-sharing method called Network Address Translation (NAT). This method allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your ISP.

The router accomplishes this address sharing by translating the internal LAN IP addresses to a single address that is globally unique on the Internet. The internal LAN IP addresses can be either private addresses or registered addresses. For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

The following figure illustrates a single IP address operation.



7786EA

Figure 8-4: Single IP Address Operation Using NAT

This scheme offers the additional benefit of firewall-like protection because the internal LAN addresses are not available to the Internet through the translated connection. All incoming inquiries are filtered out by the router. This filtering can prevent intruders from probing your system. However, using port forwarding, you can allow one PC (for example, a Web server) on your local network to be accessible to outside users.

MAC Addresses and Address Resolution Protocol

An IP address alone cannot be used to deliver data from one LAN device to another. To send data between LAN devices, you must convert the IP address of the destination device to its media access control (MAC) address. Each device on an Ethernet network has a unique MAC address, which is a 48-bit number assigned to each device by the manufacturer. The technique that associates the IP address with a MAC address is known as address resolution. Internet Protocol uses the Address Resolution Protocol (ARP) to resolve MAC addresses.

If a device sends data to another station on the network and the destination MAC address is not yet recorded, ARP is used. An ARP request is broadcast onto the network. All stations on the network receive and read the request. The destination IP address for the chosen station is included as part of the message so that only the station with this IP address responds to the ARP request. All other stations discard the request.

Related Documents

The station with the correct IP address responds with its own MAC address directly to the sending device. The receiving station provides the transmitting station with the required destination MAC address. The IP address data and MAC address data for each station are held in an ARP table. The next time data is sent, the address can be obtained from the address information in the table.

For more information about address assignment, refer to the IETF documents RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*.

For more information about IP address translation, refer to RFC 1631, *The IP Network Address Translator (NAT)*.

Domain Name Server

Many of the resources on the Internet can be addressed by simple descriptive names such as *www.NETGEAR.com*. This addressing is very helpful at the application level, but the descriptive name must be translated to an IP address in order for a user to actually contact the resource. Just as a telephone directory maps names to phone numbers, or as an ARP table maps IP addresses to MAC addresses, a domain name system (DNS) server maps descriptive names of network resources to IP addresses.

When a PC accesses a resource by its descriptive name, it first contacts a DNS server to obtain the IP address of the resource. The PC sends the desired message using the IP address. Many large organizations, such as ISPs, maintain their own DNS servers and allow their customers to use the servers to look up addresses.

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The FVM318 firewall has the capacity to act as a DHCP server.

The FVM318 firewall also functions as a DHCP client when connecting to the ISP. The firewall can automatically obtain an IP address, subnet mask, DNS server addresses, and a gateway address if the ISP provides this information by DHCP.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal "straight-through" UTP Ethernet cable follows the EIA568B standard wiring as described in [Table 8-3](#).

Table 8-1. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Uplink Switches and Crossover Cables

In the wiring table, the concept of transmit and receive are from the perspective of the PC. For example, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable. The second method is to use a crossover cable, which is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

Cable Quality

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or "Cat 5", by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Internet Security and Firewalls

When your LAN connects to the Internet through a router, an opportunity is created for outsiders to access or disrupt your network. A NAT router provides some protection because by the very nature of the Network Address Translation (NAT) process, the network behind the NAT router is shielded from access by outsiders on the Internet. However, there are methods by which a determined hacker can possibly obtain information about your network or at the least can disrupt your Internet access. A greater degree of protection is provided by a firewall router.

What is a Firewall?

A firewall is a device that protects one network from another, while allowing communication between the two. A firewall incorporates the functions of the NAT router, while adding features for dealing with a hacker intrusion or attack. Several known types of intrusion or attack can be recognized when they occur. When an incident is detected, the firewall can log details of the attempt, and can optionally send email to an administrator notifying them of the incident. Using information from the log, the administrator can take action with the ISP of the hacker. In some types of intrusions, the firewall can fend off the hacker by discarding all further packets from the hacker's IP address for a period of time.

Stateful Packet Inspection

Unlike simple Internet sharing routers, a firewall uses a process called stateful packet inspection to ensure secure firewall filtering to protect your network from attacks and intrusions. Since user-level applications such as FTP and Web browsers can create complex patterns of network traffic, it is necessary for the firewall to analyze groups of network connection "states." Using Stateful Packet Inspection, an incoming packet is intercepted at the network layer and then analyzed for state-related information associated with all network connections. A central cache within the firewall keeps track of the state information associated with all network connections. All traffic passing through the firewall is analyzed against the state of these connections in order to determine whether or not it will be allowed to pass through or rejected.

Denial of Service Attack

A hacker may be able to prevent your network from operating or communicating by launching a Denial of Service (DoS) attack. The method used for such an attack can be as simple as merely flooding your site with more requests than it can handle. A more sophisticated attack may attempt to exploit some weakness in the operating system used by your router or gateway. Some operating systems can be disrupted by simply sending a packet with incorrect length information.

Wireless Networking

The FVM318 firewall conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs). On an 802.11b wireless link, data is encoded using direct-sequence spread-spectrum (DSSS) technology and is transmitted in the unlicensed radio spectrum at 2.5GHz. The maximum data rate for the wireless link is 11 Mbps, but it will automatically back down from 11 Mbps to 5.5, 2, and 1 Mbps when the radio signal is weak or when interference is detected.

The 802.11b standard is also called Wireless Ethernet or Wi-Fi by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standard group promoting interoperability among 802.11b devices.

Wireless Network Configuration

The 802.11b standard offers two methods for configuring a wireless network - ad hoc and infrastructure.

Ad-hoc Mode (Peer-to-Peer Workgroup)

In an ad hoc network, computers are brought together as needed; thus, there is no structure or fixed points to the network - each node can generally communicate with any other node. There is no Access Point involved in this configuration. This mode enables you to quickly set up a small wireless workgroup and allows workgroup members to exchange data or share printers as supported by Microsoft Networking in the various Windows operating systems. Some vendors also refer to ad hoc networking as Peer-to-Peer group networking.

In this configuration, network packets are directly sent and received by the intended transmitting and receiving stations. As long as the stations are within range of one another, this is the easiest and least expensive way to set up a wireless network.

Infrastructure Mode

With a wireless Access Point, you can operate the wireless LAN in the infrastructure mode. This mode provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage, interacting with wireless nodes via an antenna.

In the infrastructure mode, the wireless access point converts airwave data into wired Ethernet data, acting as a bridge between the wired LAN and wireless clients. Connecting multiple Access Points via a wired Ethernet backbone can further extend the wireless network coverage. As a mobile computing device moves out of the range of one access point, it moves into the range of another. As a result, wireless clients can freely roam from one Access Point domain to another and still maintain seamless network connection.

Extended Service Set Identification (ESSID)

The Extended Service Set Identification (ESSID) is one of two types of Service Set Identification (SSID). In an ad-hoc wireless network with no access points, the Basic Service Set Identification (BSSID) is used. In an infrastructure wireless network that includes an access point, the Extended Service Set Identification (ESSID) is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network. Some vendors refer to the SSID as network name. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

Authentication and WEP Encryption

The absence of a physical connection between nodes makes the wireless links vulnerable to eavesdropping and information theft. To provide a certain level of security, the IEEE 802.11 standard has defined two types of authentication methods, Open System and Shared Key. With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted. With Shared Key authentication, only those PCs that possess the correct authentication key can join the network. By default, IEEE 802.11 wireless devices operate in an Open System network.

Wired Equivalent Privacy (WEP) data encryption is utilized when the wireless nodes or access points are configured to operate in Shared Key authentication mode. There are two shared key methods implemented in most commercially available products, 64-bit and 128-bit WEP data encryption.

The 64-bit WEP data encryption method, allows for a five-character (40-bit) input. Additionally, 24 factory-set bits are added to the forty-bit input to generate a 64-bit encryption key. (The 24 factory-set bits are not user-configurable). This encryption key will be used to encrypt/decrypt all data transmitted via the wireless interface. Some vendors refer to the 64-bit WEP data encryption as 40-bit WEP data encryption since the user-configurable portion of the encryption key is 40 bits wide.

The 128-bit WEP data encryption method consists of 104 user-configurable bits. Similar to the forty-bit WEP data encryption method, the remaining 24 bits are factory set and not user configurable. Some vendors allow passphrases to be entered instead of the cryptic hexadecimal characters to ease encryption key entry.

Wireless Channel Selection

IEEE 802.11 wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4Ghz and 2.5Ghz. Neighboring channels are 5Mhz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5Mhz above and below the center channel frequency. As a result, two separate wireless networks using neighboring channels (for example, channel 1 and channel 2) in the same general vicinity will interfere with each other. Applying two channels that allow the maximum channel separation will decrease the amount of channel cross-talk, and provide a noticeable performance increase over networks with minimal channel separation.

The radio frequency channels used are listed in Table 8-2:

Table 8-2. 802.11 Radio Frequency Channels

Channel	Center Frequency	Frequency Spread
1	2412Mhz	2399.5Mhz - 2424.5Mhz
2	2417Mhz	2404.5Mhz - 2429.5Mhz
3	2422Mhz	2409.5Mhz - 2434.5Mhz
4	2427Mhz	2414.5Mhz - 2439.5Mhz
5	2432Mhz	2419.5Mhz - 2444.5Mhz
6	2437Mhz	2424.5Mhz - 2449.5Mhz
7	2442Mhz	2429.5Mhz - 2454.5Mhz
8	2447Mhz	2434.5Mhz - 2459.5Mhz
9	2452Mhz	2439.5Mhz - 2464.5Mhz
10	2457Mhz	2444.5Mhz - 2469.5Mhz
11	2462Mhz	2449.5Mhz - 2474.5Mhz
12	2467Mhz	2454.5Mhz - 2479.5Mhz
13	2472Mhz	2459.5Mhz - 2484.5Mhz

Note: The available channels supported by the wireless products in various countries are different.

The preferred channel separation between the channels in neighboring wireless networks is 25 MHz (5 channels). This means that you can apply up to three different channels within your wireless network. There are only 11 usable wireless channels in the United States. It is recommended that you start using channel 1 and grow to use channel 6, and 11 when necessary, as these three channels do not overlap.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal "straight-through" UTP Ethernet cable follows the EIA568B standard wiring and pinout as described in [Table 8-3](#).

Table 8-3. UTP Ethernet cable wiring, straight-through

Pin	Wire color	Signal
1	Orange/White	Transmit (Tx) +
2	Orange	Transmit (Tx) -
3	Green/White	Receive (Rx) +
4	Blue	
5	Blue/White	
6	Green	Receive (Rx) -
7	Brown/White	
8	Brown	

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms:

- Uplink switch

Most hubs provide an Uplink switch which will exchange the pairs on one port, allowing that port to be connected to another hub using a normal Ethernet cable.

- Crossover cable

A crossover cable is a special cable in which the transmit and receive pairs are exchanged at one of the two cable connectors. Crossover cables are often unmarked as such, and must be identified by comparing the two connectors. Since the cable connectors are clear plastic, it is easy to place them side by side and view the order of the wire colors on each. On a straight-through cable, the color order will be the same on both connectors. On a crossover cable, the orange and blue pairs will be exchanged from one connector to the other.

Cable Quality

A twisted pair Ethernet network operating at 10 Mbits/second (10BASE-T) will often tolerate low quality cables, but at 100 Mbits/second (10BASE-Tx) the cable must be rated as Category 5, or "Cat 5" or "Cat V", by the Electronic Industry Association (EIA). This rating will be printed on the cable jacket. A Category 5 cable will meet specified requirements regarding loss and crosstalk. In addition, there are restrictions on maximum cable length for both 10 and 100 Mbits/second networks.

Appendix C

Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the FVM318 Cable/DSL ProSafe Wireless VPN Security Firewall and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).



Note: If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to “[Obtaining ISP Configuration Information for Windows Computers](#)” on page C-10 or “[Obtaining ISP Configuration Information for Macintosh Computers](#)” on page C-11 for further information.

Preparing Your Computers for TCP/IP Networking

Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Each computer on your network must have TCP/IP installed and selected as its networking protocol. If a Network Interface Card (NIC) is already installed in your PC, then TCP/IP is probably already installed as well.

Most operating systems include the software components you need for networking with TCP/IP:

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.

- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

In your IP network, each PC and the firewall must be assigned a unique IP addresses. Each PC must also have certain other IP configuration information such as a subnet mask (netmask), a domain name server (DNS) address, and a default gateway address. In most cases, you should install TCP/IP so that the PC obtains its specific network configuration information automatically from a DHCP server during bootup. For a detailed explanation of the meaning and purpose of these configuration items, refer to “[Appendix B, “Network, Routing, Firewall, and Wireless Basics.”](#)

The FVM318 firewall is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

- PC or workstation IP addresses—192.168.0.2 through 192.168.0.254
- Subnet mask—255.255.255.0
- Gateway address (the firewall)—192.168.0.1

These addresses are part of the IETF-designated private address range for use in private networks.

Configuring Windows 95, 98, and ME for TCP/IP Networking

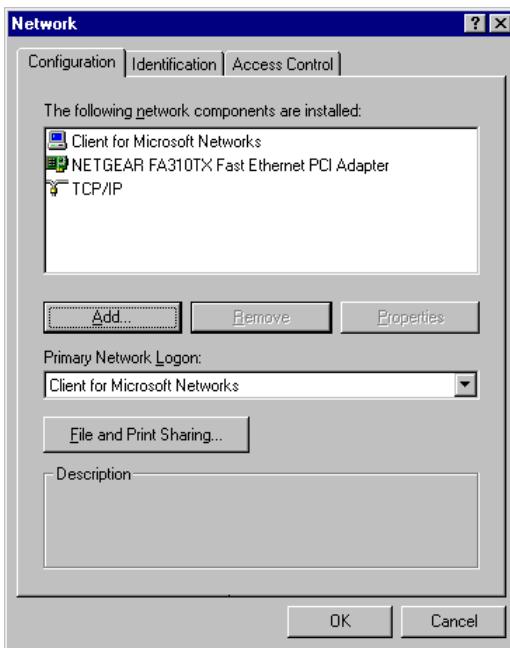
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

The Network window opens, which displays a list of installed components:



You must have an Ethernet adapter, the TCP/IP protocol, and Client for Microsoft Networks.



Note: It is not necessary to remove any other network components shown in the Network window in order to install the adapter, TCP/IP, or Client for Microsoft Networks.

If you need to install a new adapter, follow these steps:

- a. Click the Add button.
- b. Select Adapter, and then click Add.
- c. Select the manufacturer and model of your Ethernet adapter, and then click OK.

If you need TCP/IP:

- a. Click the Add button.
- b. Select Protocol, and then click Add.
- c. Select Microsoft.
- d. Select TCP/IP, and then click OK.

If you need Client for Microsoft Networks:

- a. Click the Add button.
 - b. Select Client, and then click Add.
 - c. Select Microsoft.
 - d. Select Client for Microsoft Networks, and then click OK.
3. Restart your PC for the changes to take effect.

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from the internal DHCP server of the FVM318 firewall. To use DHCP with the recommended default addresses, follow these steps:

1. Connect all PCs to the firewall, then restart the firewall and allow it to boot.
2. On each attached PC, open the Network control panel (refer to the previous section) and select the Configuration tab.
3. From the components list, select TCP/IP->(your Ethernet adapter) and click Properties.
4. In the IP Address tab, select “Obtain an IP address automatically”.
5. Select the Gateway tab.
6. If any gateways are shown, remove them.
7. Click OK.
8. Restart the PC.

Repeat steps 2 through 8 for each PC on your network.

Selecting Windows’ Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select “I want to set up my Internet connection manually” or “I want to connect through a Local Area Network” and click Next.
4. Select “I want to connect through a Local Area Network” and click Next.

5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

After your PC is configured and has rebooted, you can check the TCP/IP configuration using the utility *winipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.
 2. Type **winipcfg**, and then click OK.
- The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.
3. From the drop-down box, select your Ethernet adapter.

The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP address is between 192.168.0.2 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

Configuring Windows NT, 2000 or XP for IP Networking

As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network and Dialup Connections icon.
3. If an Ethernet adapter is present in your PC, you should see an entry for Local Area Connection. Double-click that entry.
4. Select Properties.

5. Verify that ‘Client for Microsoft Networks’ and ‘Internet Protocol (TCP/IP)’ are present. If not, select Install and add them.
6. Select ‘Internet Protocol (TCP/IP)’, click Properties, and verify that “Obtain an IP address automatically is selected.
7. Click OK and close all Network and Dialup Connections windows.
8. Make sure your PC is connected to the firewall, then reboot your PC.

Verifying TCP/IP Properties

To check your PC’s TCP/IP configuration:

1. On the Windows taskbar, click the Start button, and then click Run.

The Run window opens.

2. Type `cmd` and then click OK.

A command window opens

3. Type `ipconfig /all`

Your IP Configuration information will be listed, and should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP address is between 192.168.0.2 and 192.168.0.254
- The subnet mask is 255.255.255.0
- The default gateway is 192.168.0.1

4. Type `exit`

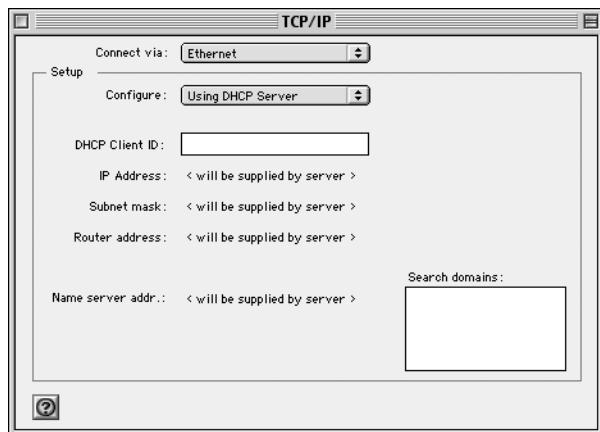
Configuring the Macintosh for TCP/IP Networking

Beginning with Macintosh Operating System 7, TCP/IP is already installed on the Macintosh. On each networked Macintosh, you will need to configure TCP/IP to use DHCP.

MacOS 8.6 or 9.x

1. From the Apple menu, select Control Panels, then TCP/IP.

The TCP/IP Control Panel opens:



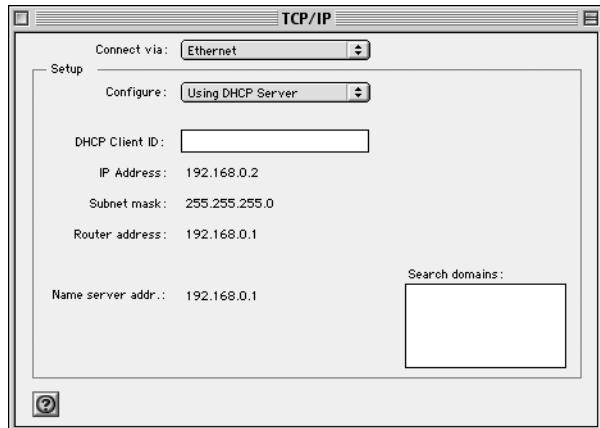
2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.
You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

MacOS X

1. From the Apple menu, choose System Preferences, then Network.
2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

After your Macintosh is configured and has rebooted, you can check the TCP/IP configuration by returning to the TCP/IP Control Panel. From the Apple menu, select Control Panels, then TCP/IP.



The panel is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends:

- The IP Address is between 192.168.0.2 and 192.168.0.254
- The Subnet mask is 255.255.255.0
- The Router address is 192.168.0.1

If you do not see these values, you may need to restart your Macintosh or you may need to switch the “Configure” setting to a different option, then back again to “Using DHCP Server”.

Verifying the Readiness of Your Internet Account

For broadband access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using a cable modem or DSL modem. This modem must be a separate physical box (not a card) and must provide an Ethernet port intended for connection to a Network Interface Card (NIC) in a computer. Your firewall does not support a USB-connected broadband modem.

For a single-user Internet account, your ISP supplies TCP/IP configuration information for one computer. With a typical account, much of the configuration information is dynamically assigned when your PC is first booted up while connected to the ISP, and you will not need to know that dynamic information.

In order to share the Internet connection among several computers, your firewall takes the place of the single PC, and you need to configure it with the TCP/IP information that the single PC would normally use. When the firewall's Internet port is connected to the broadband modem, the firewall appears to be a single PC to the ISP. The firewall then allows the PCs on the local network to masquerade as the single PC to access the Internet through the broadband modem. The method used by the firewall to accomplish this is called Network Address Translation (NAT) or IP masquerading.

Are Login Protocols Used?

Some ISPs require a special login protocol, in which you must enter a login name and password in order to access the Internet. If you normally log in to your Internet account by running a program such as WinPOET or EnterNet, then your account uses PPP over Ethernet (PPPoE).

When you configure your router, you will need to enter your login name and password in the router's configuration menus. After your network and firewall are configured, the firewall will perform the login task when needed, and you will no longer need to run the login program from your PC. It is not necessary to uninstall the login program.

What Is Your Configuration Information?

More and more, ISPs are dynamically assigning configuration information. However, if your ISP does not dynamically assign configuration information but instead used fixed configurations, your ISP should have given you the following basic information for your account:

- An IP address and subnet mask
- A gateway IP address, which is the address of the ISP's router
- One or more domain name server (DNS) IP addresses
- Host name and domain suffix

For example, your account's full server names may look like this:

mail.ddd.aaa.com

In this example, the domain suffix is ddd.aaa.com.

If any of these items are dynamically supplied by the ISP, your firewall automatically acquires them.

If an ISP technician configured your PC during the installation of the broadband modem, or if you configured it using instructions provided by your ISP, you need to copy the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the FVM318 firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Network icon.

The Network window opens, which displays a list of installed components.

3. Select TCP/IP, and then click Properties.

The TCP/IP Properties dialog box opens.

4. Select the IP Address tab.

If an IP address and subnet mask are shown, write down the information. If an address is present, your account uses a fixed (static) IP address. If no address is present, your account uses a dynamically-assigned IP address. Click "Obtain an IP address automatically".

5. Select the Gateway tab.

If an IP address appears under Installed Gateways, write down the address. This is the ISP's gateway address. Select the address and then click Remove to remove the gateway address.

6. Select the DNS Configuration tab.

If any DNS server addresses are shown, write down the addresses. If any information appears in the Host or Domain information box, write it down. Click Disable DNS.

7. Click OK to save your changes and close the TCP/IP Properties dialog box.

You are returned to the Network window.

8. Click OK.

9. Reboot your PC at the prompt. You may also be prompted to insert your Windows CD.

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the FVM318 firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

To get the information you need to configure the firewall for Internet access:

1. From the Apple menu, select Control Panels, then TCP/IP.

The TCP/IP Control Panel opens, which displays a list of configuration settings. If the "Configure" setting is "Using DHCP Server", your account uses a dynamically-assigned IP address. In this case, close the Control Panel and skip the rest of this section.

2. If an IP address and subnet mask are shown, write down the information.
3. If an IP address appears under Router address, write down the address. This is the ISP's gateway address.
4. If any Name Server addresses are shown, write down the addresses. These are your ISP's DNS addresses.
5. If any information appears in the Search domains information box, write it down.
6. Change the "Configure" setting to "Using DHCP Server".
7. Close the TCP/IP Control Panel.

Restarting the Network

Once you've set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your FVM318 firewall, you are ready to access and configure the firewall.

Glossary

10BASE-T	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
100BASE-Tx	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
802.11b	IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.
Denial of Service attack	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
DHCP	<i>See</i> Dynamic Host Configuration Protocol.
DNS	<i>See</i> Domain Name Server.
domain name	A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as .com, .edu, .uk, etc. For example, in the address mail.NETGEAR.com, mail is a server name and NETGEAR.com is the domain.
Domain Name Server	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
Dynamic Host Configuration Protocol	DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.
Gateway	A local device, usually a router, that connects hosts on a local network to other networks.

IETF	Internet Engineering Task Force. An open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. Working groups of the IETF propose standard protocols and procedures for the Internet, which are published as RFCs (Request for Comment) at www.ietf.org .
IP	Internet Protocol. The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
IP Address	A four-position number uniquely defining each host on the Internet. Ranges of addresses are assigned by Internic, an organization formed for this purpose. Usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).
IPSec	Internet Protocol Security. IPSec is a series of guidelines for securing private information transmitted over public networks. IPSec is a VPN method providing a higher level of security than PPTP.
ISP	Internet service provider.
LAN	<i>See</i> local area network.
local area network	LAN. A communications network serving users within a limited area, such as one floor of a building. A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.
MAC address	Media Access Control address. A unique 48-bit hardware address assigned to every Ethernet node. Usually written in the form 01:23:45:67:89:ab.
Mbps	Megabits per second.
MSB	<i>See</i> Most Significant Bit or Most Significant Byte.
MTU	<i>See</i> Maximum Transmit Unit.
Maximum Transmit Unit	The size in bytes of the largest packet that can be sent or received.
Most Significant Bit or Most Significant Byte	The portion of a number, address, or field that is farthest left when written as a single number in conventional hexadecimal ordinary notation. The part of the number having the most value.
NAT	<i>See</i> Network Address Translation.

netmask	A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.
Network Address Translation	A technique by which several hosts share a single IP address for access to the Internet.
packet	A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.
PPP	<i>See</i> Point-to-Point Protocol.
PPP over Ethernet	PPPoE. PPP over Ethernet is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
PPTP	Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.
PSTN	Public Switched Telephone Network.
Point-to-Point Protocol	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
RFC	Request For Comment. Refers to documents published by the Internet Engineering Task Force (IETF) proposing standard protocols and procedures for the Internet. RFCs can be found at www.ietf.org .
RIP	<i>See</i> Routing Information Protocol.
router	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
Routing Information Protocol	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
subnet mask	<i>See</i> netmask.
URL	Universal Resource Locator, the global address of documents and other resources on the World Wide Web.
UTP	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

VPN	Virtual Private Network. A method for securely transporting data between two private networks by using a public network such as the Internet as a connection.
WAN	<i>See</i> wide area network.
WEP	Wired Equivalent Privacy. WEP is a data encryption protocol for 802.11b wireless networks. All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.
wide area network	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
Windows Internet Naming Service	WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses. If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using Network Neighborhood.
WINS	<i>See</i> Windows Internet Naming Service.

Index

Numerics

802.11b B-13

A

Account Name 2-10, 2-12, 2-15
ActiveX 3-3
Address Resolution Protocol B-9
ad-hoc mode B-14
Austria 2-15
Auto Uplink 1-2

B

backup configuration 5-9
BigPond 2-15
BSSID B-14

C

cables, pinout B-17
Cabling B-11, B-17
Cat5 cable 2-1, B-12, B-18
Channel 6-3, B-15
configuration
 automatic by DHCP 1-3
 backup 5-9
 erasing 5-11
 router, initial 2-1
Connection Monitor 4-22
content filtering 1-2
conventions
 typography 1-xiii
cookie 3-3
crossover cable 1-2, 8-3, B-11, B-18

customer support 1-iii

D

date and time 8-9
Daylight Savings Time 3-8, 8-9
daylight savings time 3-8
Default DMZ Server 7-1
default reset button 8-8
Denial of Service (DoS) protection 1-1, 3-3
denial of service attack B-13
DHCP 1-3, 7-4, B-10
DHCP Client ID C-7
DHCP Setup field, Ethernet Setup menu 5-2
DMZ Server 7-1
DNS Proxy 1-3
DNS server 2-11, 2-12, 2-15, C-11
DNS, dynamic 7-6
domain C-11
Domain Name 2-10, 2-12, 2-15
domain name server (DNS) B-10
DoS attack B-13
Dynamic DNS 1-3, 7-6

E

EnterNet C-9
EPROM, for firmware upgrade 1-4
ESSID B-14
Ethernet 1-2
Ethernet cable B-11, B-17

F

factory settings, restoring 5-11
features 1-1
firewall features 1-1
FLASH memory 5-14
front panel 1-5

G

gateway address C-11

H

host name 2-10, 2-12, 2-15

I

IANA
 contacting B-2
IETF B-1
 Web site address B-7
IKE 4-8, 4-14
IKE Life Time 4-8, 4-10, 4-15
infrastructure mode B-14
installation 1-3
Internet account
 address information C-9
 establishing C-9
IP addresses C-10, C-11
 and NAT B-8
 and the Internet B-2
 assigning B-2, B-9
 auto-generated 8-4
 private B-7
 translating B-9
IP configuration by DHCP B-10
IP networking
 for Macintosh C-6
 for Windows C-2, C-5

J

Java 3-3

K

Key Life 4-8, 4-10, 4-15

L

LAN IP Setup Menu 4-5, 7-6
LEDs
 description 1-6
 troubleshooting 8-2
log
 sending 5-8
Log Viewer 4-22

M

MAC 6-4
MAC address 8-8, B-9
 spoofing 2-12, 2-15, 8-6
MAC address filter 6-4
Macintosh C-10
 configuring for IP networking C-6
 DHCP Client ID C-7
 Obtaining ISP Configuration Information C-11
Manual Keying 4-24
masquerading C-9
MD5 authentication 4-25
MDI/MDI-X wiring B-17
metric 7-10
Modem 2-19, 2-20
modem 1-3, 1-6, 2-17
MTU 7-3
multicasting 7-3

N

NAT C-9
NAT. *See* Network Address Translation
NETGEAR
 contacting 1-xiv
netmask
 translation table B-6
Network Address Translation 1-2, B-8, C-9

Network Time Protocol 3-7, 8-9

NTP 3-7, 8-9

O

Open System authentication B-15

P

package contents 1-5

Passphrase 6-5

password

restoring 8-8

PC, using to configure C-12

Perfect Forward Secrecy 4-8, 4-10, 4-15

ping 7-2

pinout, Ethernet cable B-17

placement 6-1

port forwarding behind NAT B-9

PPP over Ethernet 1-3, C-9

PPPoE 1-3, 2-10, C-9

PPTP 2-15

PreShared Key 4-3, 4-8, 4-10, 4-12, 4-15, 4-26, 4-27

Primary DNS Server 2-11, 2-12, 2-13, 2-15

protocols

Address Resolution B-9

DHCP 1-3, B-10

Routing Information 1-2, B-2

support 1-2

TCP/IP 1-2

publications, related B-1

R

range 6-1

rear panel 1-6

Region 6-3

remote management 7-10

requirements

access device 2-1

hardware 2-1

reserved IP addresses 7-5

reset button, clearing config 8-8

restore factory settings 5-11

RFC

1466 B-7, B-9

1597 B-7, B-9

1631 B-8, B-9

finding B-7

RIP (Router Information Protocol) 7-3

router concepts B-1

Routing Information Protocol 1-2, B-2

S

SA 4-2

SafeNet Secure VPN Client 4-12

Secondary DNS Server 2-11, 2-12, 2-13, 2-15

security association 4-2

Serial 2-3, 2-17, 2-18, 2-19

serial 1-1, 1-4, 1-6, 2-3, 2-17

Setup Wizard 2-1

SHA-1 authentication 4-25

Shared Key authentication B-15

SMTP 5-8

SPI (Security Parameter Index) 4-24

spoof MAC address 8-6

SSID 6-3, B-14

stateful packet inspection 1-1, B-13

Static Routes 7-6

subnet addressing B-5

subnet mask B-6, C-10, C-11

Syslog 5-7

T

TCP/IP

configuring C-1

network, troubleshooting 8-6

TCP/IP properties

verifying for Macintosh C-8

verifying for Windows C-5, C-6

technical support 1-xiv

Telstra 2-15
time of day 8-9
time zone 3-8
timeout, administrator login 3-3
time-stamping 3-8
troubleshooting 8-1
Trusted Host 3-5
typographical conventions 1-xiii

U

Uplink switch B-11
uplink switch B-17
USB C-9

W

web proxy 3-3
WEP 6-5, B-15
WEP, Keys 6-5
Wi-Fi B-13
Windows, configuring for IP routing C-2, C-5
winipcfg utility C-5
WinPOET C-9
WINS 7-5
Wired Equivalent Privacy. *See* WEP
Wireless Ethernet B-13
World Wide Web 1-iii