

# Reference Manual for the Model FR114P, FR114W and FM114P Cable/DSL ProSafe Firewall Family

## **NETGEAR**

**NETGEAR**, Inc.  
4500 Great America Parkway  
Santa Clara, CA 95054 USA  
Phone 1-888-NETGEAR

SM-FM114PNA-0  
May 2002

© 2002 by NETGEAR, Inc. All rights reserved.

## **Trademarks**

NETGEAR and Auto Uplink are trademarks or registered trademarks of Netgear, Inc.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation.

Other brand and product names are registered trademarks or trademarks of their respective holders.

## **Statement of Conditions**

In the interest of improving internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice.

NETGEAR does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

## **Federal Communications Commission (FCC) Compliance Notice: Radio Frequency Notice**

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

## **EN 55 022 Declaration of Conformance**

This is to certify that the FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall is shielded against the generation of radio interference in accordance with the application of Council Directive 89/336/EEC, Article 4a. Conformity is declared by the application of EN 55 022 Class B (CISPR 22).

## **Bestätigung des Herstellers/Importeurs**

Es wird hiermit bestätigt, daß das FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall gemäß der im BMPT-AmtsblVfg 243/1991 und Vfg 46/1992 aufgeführten Bestimmungen entstört ist. Das vorschriftsmäßige Betreiben einiger Geräte (z.B. Testsender) kann jedoch gewissen Beschränkungen unterliegen. Lesen Sie dazu bitte die Anmerkungen in der Betriebsanleitung.

Das Bundesamt für Zulassungen in der Telekommunikation wurde davon unterrichtet, daß dieses Gerät auf den Markt gebracht wurde und es ist berechtigt, die Serie auf die Erfüllung der Vorschriften hin zu überprüfen.

## **Certificate of the Manufacturer/Importer**

It is hereby certified that the FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall has been suppressed in accordance with the conditions set out in the BMPT-AmtsblVfg 243/1991 and Vfg 46/1992. The operation of some equipment (for example, test transmitters) in accordance with the regulations may, however, be subject to certain restrictions. Please refer to the notes in the operating instructions.

Federal Office for Telecommunications Approvals has been notified of the placing of this equipment on the market and has been granted the right to test the series for compliance with the regulations.

## **Voluntary Control Council for Interference (VCCI) Statement**

This equipment is in the second category (information equipment to be used in a residential area or an adjacent area thereto) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in such residential areas.

When used near a radio or TV receiver, it may become the cause of radio interference.

Read instructions for correct handling.

## **Technical Support**

Refer to the Support Information Card that shipped with your FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall.

## **World Wide Web**

NETGEAR maintains a World Wide Web home page that you can access at the universal resource locator (URL) <http://www.netgear.com>. A direct connection to the Internet and a Web browser such as Internet Explorer or Netscape are required.



# Contents

## About This Guide

Typographical Conventions .....	xv
Special Message Formats .....	xvi
Technical Support .....	xvi
Related Publications .....	xvi

## Chapter 1

### Introduction

About the NETGEAR ProSafe Firewalls .....	1-1
Key Features .....	1-1
A Powerful, True Firewall .....	1-2
Content Filtering .....	1-3
Configurable Ethernet Connection .....	1-3
Protocol Support .....	1-3
Easy Installation and Management .....	1-4
Maintenance and Support .....	1-5

## Chapter 2

### Setting Up the Hardware

Package Contents .....	2-1
Local Network Hardware Requirements .....	2-2
PC Requirements .....	2-2
Access Device Requirement .....	2-2
The Firewall's Front Panel .....	2-3
The Firewall's Rear Panel .....	2-4
Connecting the Firewall .....	2-4
Connecting to Your Internet Access Device .....	2-5
Connecting to your Local Ethernet Network .....	2-5
Preparing your Wireless Devices .....	2-6
Installing a Wireless Card in the FR114W .....	2-6
Connecting the Power Adapter .....	2-6

Verifying Connections .....	2-7
<b>Chapter 3</b>	
<b>Preparing Your Network</b>	
Preparing Your Personal Computers for IP Networking .....	3-1
Configuring Windows 95, 98, and ME for IP Networking .....	3-2
Install or Verify Windows Networking Components .....	3-2
Assign TCP/IP configuration by DHCP .....	3-4
Selecting Internet Access Method .....	3-4
Verifying TCP/IP Properties .....	3-5
Configuring Windows NT or 2000 for IP Networking .....	3-5
Install or Verify Windows Networking Components .....	3-5
Verifying TCP/IP Properties .....	3-6
Configuring the Macintosh for IP Networking .....	3-6
MacOS 8.6 or 9.x .....	3-7
MacOS X .....	3-7
Verifying TCP/IP Properties (Macintosh) .....	3-8
Your Internet Account .....	3-8
Login Protocols .....	3-9
Account Information .....	3-9
Obtaining ISP Configuration Information (Windows) .....	3-10
Obtaining ISP Configuration Information (Macintosh) .....	3-11
Restarting the Network .....	3-11
Ready for Configuration .....	3-12
<b>Chapter 4</b>	
<b>Basic Configuration</b>	
Accessing the Web Configuration Manager .....	4-1
Configuration using the Setup Wizard .....	4-4
Configuring for Dynamic IP Account .....	4-5
Configuring for Fixed IP Account .....	4-6
Configuring for an Account with Login .....	4-7
Manual Configuration .....	4-8
Completing the Configuration .....	4-9
<b>Chapter 5</b>	
<b>Security</b>	
What is a Firewall .....	5-1

Security Log .....	5-2
Examples of log messages .....	5-4
Activation and Administration .....	5-4
Dropped Packets .....	5-4
Block Sites .....	5-5
Rules .....	5-6
Inbound Rules (Port Forwarding) .....	5-8
Inbound Rule Example: A Local Public Web Server .....	5-9
Inbound Rule Example: Allowing Videoconference from Restricted Addresses .....	5-10
Considerations for Inbound Rules: .....	5-10
Outbound Rules (Service Blocking) .....	5-11
Following is an application example of outbound rules: .....	5-11
Outbound Rule Example: Blocking Instant Messenger .....	5-11
Order of Precedence for Rules .....	5-12
Default DMZ Server .....	5-12
Respond to Ping on Internet WAN Port .....	5-13
Services .....	5-14
Schedule .....	5-16
Time Zone .....	5-17
E-Mail .....	5-18

**Chapter 6**  
**Wireless**

Wireless Settings .....	6-2
Identification .....	6-2
Options .....	6-3
Access Point .....	6-3
Configuring WEP (Wired Equivalent Privacy) .....	6-4
Restricting Wireless Access by MAC Address .....	6-5
Additional Notes .....	6-6
Security .....	6-6
Placement and Range .....	6-6

**Chapter 7**  
**Print Server**

Network Printing from Windows .....	7-1
Installing the PTP Driver .....	7-1

Printer Management .....	7-3
Port Options .....	7-3
LPD/LPR Printing from Windows .....	7-4
Windows NT 4.0 Server Configuration .....	7-5
Client PC Setup for LPD/LPR Printing .....	7-7
Network Printing from the Macintosh .....	7-9
MacOS 8 or 9 Configuration .....	7-9
MacOS X Configuration .....	7-10
Network Printing from Linux .....	7-10
Troubleshooting the Print Server .....	7-10

## **Chapter 8**

### **Maintenance**

System Status .....	8-1
Attached Devices .....	8-4
Changing the Administration Password .....	8-4
Configuration File Settings Management .....	8-5
Restore and Backup the Configuration .....	8-6
Erase the Configuration .....	8-6
Router Upgrade .....	8-7
Diagnostics .....	8-8
Ping an IP Address .....	8-8
Perform a DNS Lookup .....	8-8
Display the Routing Table .....	8-9
Reboot the Router .....	8-9

## **Chapter 9**

### **Advanced Configuration**

Dynamic DNS .....	9-1
LAN IP Setup .....	9-3
LAN TCP/IP Setup .....	9-3
MTU Size .....	9-5
DHCP .....	9-5
Use router as DHCP server .....	9-5
Reserved IP addresses .....	9-6
Static Routes .....	9-6
Static Route Example .....	9-8



Remote Management .....9-9

**Chapter 10  
Troubleshooting**

Basic Functioning .....10-1  
    Power LED Not On ..... 10-2  
    Test LED Never Turns On or Test LED Stays On .....10-2  
    Local or Internet Port Link LEDs Not On ..... 10-2  
Troubleshooting the Web Configuration Interface .....10-4  
Troubleshooting the ISP Connection ..... 10-5  
Troubleshooting a TCP/IP Network Using a Ping Utility .....10-6  
    Testing the LAN Path to Your Firewall ..... 10-6  
    Testing the Path from Your PC to a Remote Device .....10-7  
Restoring the Default Configuration and Password ..... 10-8  
    Using the Default Reset button ..... 10-8  
Problems with Date and Time ..... 10-8

**Appendix A  
Technical Specifications**

**Appendix B  
Networks, Routing, and Firewall Basics**

Basic Router Concepts ..... B-1  
    What is a Router? ..... B-1  
    Routing Information Protocol ..... B-2  
    IP Addresses and the Internet ..... B-2  
    Netmask ..... B-4  
    Subnet Addressing ..... B-5  
    Private IP Addresses ..... B-7  
    Single IP Address Operation Using NAT ..... B-8  
    MAC Addresses and Address Resolution Protocol ..... B-9  
    Domain Name Server ..... B-9  
    IP Configuration by DHCP ..... B-10  
Internet Security and Firewalls ..... B-10  
    What is a Firewall? ..... B-10  
    Stateful Packet Inspection ..... B-11  
    Denial of Service Attack ..... B-11  
Wireless Networking ..... B-12

Wireless Network Configuration .....	B-12
Ad-hoc Mode (Peer-to-Peer Workgroup) .....	B-12
Infrastructure Mode .....	B-12
Extended Service Set Identification (ESSID) .....	B-13
Authentication and WEP Encryption .....	B-13
Wireless Channel Selection .....	B-14
Ethernet Cabling .....	B-15
Uplink Switches and Crossover Cables .....	B-16
Cable Quality .....	B-16

**Glossary**

**Index**

Figure 2-1.	FR114P Front Panel .....	2-3
Figure 2-2.	FR114P Rear Panel .....	2-4
Figure 4-1.	Login window .....	4-2
Figure 4-2.	Browser-based configuration main menu .....	4-3
Figure 4-3.	Setup Wizard menu for Dynamic IP address .....	4-5
Figure 4-4.	Setup Wizard menu for Fixed IP address .....	4-6
Figure 4-5.	Setup Wizard menu for PPPoE login accounts .....	4-7
Figure 5-1.	Logs menu .....	5-2
Figure 5-2.	Block Sites menu .....	5-5
Figure 5-3.	Rules menu .....	5-6
Figure 5-4.	Rule example: A Local Public Web Server .....	5-9
Figure 5-5.	Rule example: Videoconference from Restricted Addresses .....	5-10
Figure 5-6.	Rule example: Blocking Instant Messenger .....	5-11
Figure 5-7.	Rules table with examples .....	5-12
Figure 5-8.	Services menu .....	5-14
Figure 5-9.	Add Custom Service menu .....	5-15
Figure 6-1.	Wireless Settings menu .....	6-2
Figure 6-2.	Wireless WEP menu .....	6-4
Figure 6-3.	Wireless Access menu .....	6-5
Figure 8-1.	System Status screen .....	8-1
Figure 8-2.	Router Statistics screen .....	8-3
Figure 8-3.	Attached Devices menu .....	8-4
Figure 8-4.	Set Password menu .....	8-5
Figure 8-5.	Settings Backup menu .....	8-6
Figure 8-6.	Router Upgrade menu .....	8-7
Figure 8-7.	Diagnostics menu .....	8-8
Figure 9-1.	Dynamic DNS menu .....	9-2
Figure 9-2.	LAN IP Setup Menu .....	9-3
Figure 9-3.	Static Routes Summary Table .....	9-7
Figure 9-4.	Static Route Entry and Edit Menu .....	9-7
Figure B-1.	Three Main Address Classes .....	B-3
Figure B-2.	Example of Subnetting a Class B Address .....	B-5
Figure B-3.	Single IP Address Operation Using NAT .....	B-8



Table 2-1.	LED Descriptions .....	2-3
Table 5-1.	Log entry descriptions .....	5-3
Table 5-2.	Log action buttons .....	5-3
Table 8-1.	Menu 3.2 - System Status Fields .....	8-2
Table 8-2.	Router Statistics Fields .....	8-3
Table B-1.	Netmask Notation Translation Table for One Octet .....	B-6
Table B-2.	Netmask Formats .....	B-6
Table B-3.	802.11 Radio Frequency Channels .....	B-14
Table B-4.	UTP Ethernet cable wiring, straight-through .....	B-15



# About This Guide

Congratulations on your purchase of the NETGEAR™ FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall. A firewall is a special type of router that incorporates features for security. The NETGEAR ProSafe Firewall is a complete security solution that protects your network from attacks and intrusions.

This guide describes the features of the firewall and provides installation and configuration instructions.

## Typographical Conventions

---


This guide uses the following typographical conventions:


<i>italics</i>	Book titles and UNIX file, command, and directory names.
<code>courier font</code>	Screen text, user-typed command-line entries.
Initial Caps	Menu titles and window and button names.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
[Ctrl]+C	Two or more keys that must be pressed simultaneously are shown in text linked with a plus (+) sign.
ALL CAPS	DOS file and directory names.


## Special Message Formats


---

This guide uses the following formats to highlight special messages:

	<b>Note:</b> This format is used to highlight information of importance or special interest.
---	--

	<b>Caution:</b> This format is used to highlight information that will help you prevent equipment failure or loss of data.
---	--

	<b>Warning:</b> This format is used to highlight information about the possibility of injury or equipment damage.
---	---

	<b>Danger:</b> This format is used to alert you that there is the potential for incurring an electrical shock if you mishandle the equipment.
---	---

## Technical Support

---

For help with any technical issues, contact Customer Support at 1-888-NETGEAR, or visit us on the Web at [www.NETGEAR.com](http://www.NETGEAR.com). The NETGEAR Web site includes an extensive knowledge base, answers to frequently asked questions, and a means for submitting technical questions online.

## 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](http://www.ietf.org) and are mirrored and indexed at many other sites worldwide.



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)*.



# Chapter 1

## Introduction

This chapter describes the features of the NETGEAR FR114P, FR114W and FM114P Cable/DSL ProSafe Firewalls.

### About the NETGEAR ProSafe Firewalls

---

The NETGEAR ProSafe Firewall is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing routers that rely on NAT for security, the NETGEAR ProSafe Firewall uses Stateful Packet Inspection for Denial of Service (DoS) attack protection and intrusion detection. The NETGEAR ProSafe Firewall allows Internet access for up to 253 users. The ProSafe Firewall family consists of these three products:

- FR114P Firewall with Print Server
- FR114W Wireless-Ready Firewall
- FM114P Wireless Firewall with Print Server

The FR114P and FM114P firewalls include a built-in print server, allowing the sharing of a printer by all PCs on your network. The FM114P firewall includes an 802.11b-compliant wireless access point, while the FR114W firewall can be upgraded to an access point by adding a NETGEAR 802.11b wireless adapter card.

### Key Features

---

The NETGEAR ProSafe Firewalls offer the following features.

## A Powerful, True Firewall

Unlike simple Internet sharing NAT routers, the NETGEAR ProSafe Firewall is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- Denial of Service (DoS) protection  
Automatically detects and thwarts Denial of Service (DoS) attacks such as Ping of Death, SYN Flood, LAND Attack and IP Spoofing.
- Blocks unwanted traffic from the Internet to your LAN.
- Blocks access from your LAN to Internet locations or services that you specify as off-limits.
- Logs security incidents  
The NETGEAR ProSafe Firewall will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the firewall to email the log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your email address or email pager whenever a significant event occurs.

## Wireless Access Point

The FM114P firewall includes an 802.11b-compliant wireless access point, while the FR114W firewall can be upgraded to an access point by adding a NETGEAR 802.11b wireless adapter card. With an integrated wireless access point, the firewall provides continuous, high-speed 11 Mbps access between your wireless and Ethernet devices. The access point provides:

- 802.11b Standards-based wireless networking at up to 11 Mbps
- 64-bit and 128-bit WEP encryption security
- WEP keys can be generated manually or by passphrase
- Wireless access can be restricted by MAC address

## Integrated Print Server

The FR114P and FM114P NETGEAR ProSafe Firewalls include a built-in print server. A print server eliminates the bottleneck of a dedicated always-on PC print server and supports multiple print jobs simultaneously.

- Protocol Support  
PTP (Peer-to-Peer) over TCP/IP for Windows  
LPR printing for Windows, Macintosh, or Linux

- High-speed Parallel Port Connection  
36 pin Centronics, bi-directional IEEE 1284 compliant (supports Nibble mode) with up to 1.5Mbps transfer rate

## Content Filtering

With its content filtering feature, the NETGEAR ProSafe Firewall prevents objectionable content from reaching your PCs. The firewall allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the firewall to log and report attempts to access objectional Internet sites.

## Configurable Ethernet Connection

With its internal 4-port 10/100 switch, the NETGEAR ProSafe Firewall can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. The local LAN interface is autosensing and is capable of full-duplex or half-duplex operation. An uplink switch is provided for cascading to an external Ethernet hub or switch.

## Protocol Support

The NETGEAR ProSafe Firewall supports the Transmission Control Protocol/Internet Protocol (TCP/IP) and Routing Information Protocol (RIP).

For further information about TCP/IP, refer to [Appendix B, “Networks, Routing, and Firewall Basics.”](#)

- IP Address Sharing by NAT  
The NETGEAR ProSafe Firewall allows several networked PCs to share an Internet account using only a single IP address, which may be statically or dynamically assigned by your Internet service provider (ISP). This technique, known as Network Address Translation (NAT), allows the use of an inexpensive single-user ISP account.
- Automatic Configuration of Attached PCs by DHCP  
The NETGEAR ProSafe Firewall dynamically assigns network configuration information, including IP, gateway, and domain name server (DNS) addresses, to attached PCs on the LAN using the Dynamic Host Configuration Protocol (DHCP). This feature greatly simplifies configuration of PCs on your local network.

- **DNS Proxy**  
When DHCP is enabled and no DNS addresses are specified, the firewall provides its own address as a DNS server to the attached PCs. The firewall obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE)**  
PPP over Ethernet is a protocol for connecting remote hosts to the Internet over a DSL connection by simulating a dial-up connection. This feature eliminates the need to run a login program such as EnterNet or WinPOET on your PC.
- **Dynamic DNS**  
Dynamic DNS services allow remote users to find your network using a domain name when your IP address is not permanently assigned. The firewall contains a client that can connect to many popular Dynamic DNS services to register your dynamic IP address.

## Easy Installation and Management

You can install, configure, and operate the NETGEAR ProSafe Firewall within minutes after connecting it to the network. The following features simplify installation and management tasks:

- **Browser-based management**  
Browser-based configuration allows you to easily configure your firewall from almost any type of personal computer, such as Windows, Macintosh, or Linux. A user-friendly Setup Wizard is provided and online help documentation is built into the browser-based Web Management Interface.
- **Smart Wizard**  
The firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **Remote management**  
The firewall allows you to login to the Web Management Interface from a remote location on the Internet. For security, you can limit remote management access to a specified remote IP address or range of addresses, and you can choose a nonstandard port number.
- **Diagnostic functions**  
The firewall incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot.
- **Visual monitoring**  
The firewall's front panel LEDs provide an easy way to monitor its status and activity.

## **Maintenance and Support**

NETGEAR offers the following features to help you maximize your use of the firewall:

- Flash EPROM for firmware upgrade
- Technical support seven days a week, twenty-four hours a day





# Chapter 2

## Setting Up the Hardware

This chapter describes the hardware installation of the FR114P, FR114W and FM114P Cable/DSL ProSafe Firewalls.

### Package Contents

---

The product package should contain the following items:

- FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall
- AC power adapter
- Category 5 (CAT5) Ethernet cable
- *Resource CD*, including:
  - This manual
  - Installer for Print server driver (applies to FR114P or FM114P only)
  - Application Notes, Tools, and other helpful information
- *NETGEAR Cable/DSL ProSafe Firewall Installation Guide* (for each model)
- Warranty and registration card
- Support information card

If any of the parts are incorrect, missing, or damaged, contact your NETGEAR dealer. Keep the carton, including the original packing materials, in case you need to return the product for repair.

## **Local Network Hardware Requirements**

---

The NETGEAR ProSafe Firewall is intended for use in a network of personal computers (PCs) that are interconnected by twisted-pair Ethernet cables.

### **PC Requirements**

To install and run the NETGEAR ProSafe Firewall over your network of PCs, each PC must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the PC will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the cable provided with your firewall.

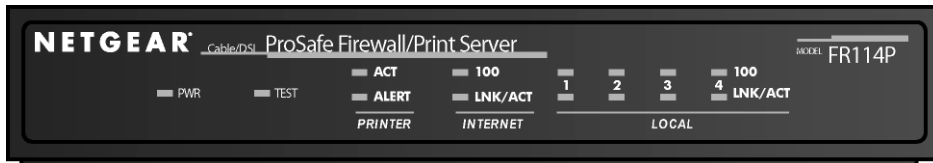
Any PC that will connect to the firewall (FR114W and FM114P only) by a wireless connection must have an 802.11b-compliant wireless adapter card.

### **Access Device Requirement**

The shared broadband access device (cable modem or DSL modem) must provide a standard 10 Mbps (10BASE-T) Ethernet interface.

## The Firewall's Front Panel

The front panel of the NETGEAR ProSafe Firewall contains status LEDs. The FR114P front panel is shown in [Figure 2-1](#)



**Figure 2-1. FR114P Front Panel**

You can use some of the LEDs to verify connections. [Table 2-1](#) lists and describes each LED on the front panel of the firewall. These LEDs are green when lit, except for the TEST LED, which is amber.

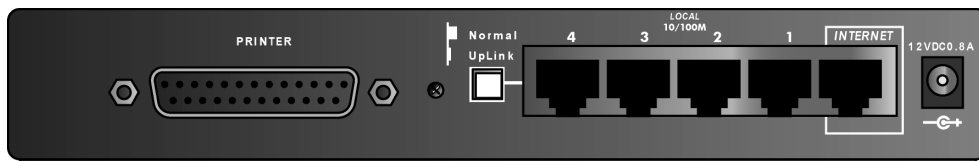
**Table 2-1. LED Descriptions**

Label	Activity	Description
POWER	On	Power is supplied to the firewall.
TEST	On Off	The system is initializing. The system is ready and running.
PRINTER ACT ALERT	Blinking On (Amber)	(These LEDs present only on FR114P and FM114P) Data is being transmitted or received by the Printer port. The connected printer is offline, is out of paper, or has a paper jam.
INTERNET 100 (100 Mbps) LINK/ACT (Link/Activity)	On Off On Blinking	The Internet (WAN) port is operating at 100 Mbps. The Internet (WAN) port is operating at 10 Mbps. The Internet port has detected a link with an attached device. Data is being transmitted or received by the Internet port.
LOCAL 100 (100 Mbps) LINK/ACT (Link/Activity)	On Off On Blinking	The Local port is operating at 100 Mbps. The Local port is operating at 10 Mbps. The Local port has detected a link with an attached device. Data is being transmitted or received by the Local port.
WLAN	On	The Wireless (WLAN) port is operating (FR114W and FM114P)

## The Firewall's Rear Panel

---

The rear panel of the NETGEAR ProSafe Firewall contains port connections. The FR114P Firewall rear panel is shown in [Figure 2-2](#)



**Figure 2-2. FR114P Rear Panel**

The rear panel contains the following features:

- AC power adapter outlet
- Internet (WAN) Ethernet port for connecting the firewall to a cable or DSL modem
- Four Local (LAN) Ethernet ports for connecting the firewall to the local PCs
- Uplink switch for converting LAN port 4 to uplink (crossover) wiring
- Factory Default Reset pushbutton
- Parallel Printer port (FR114P and FM114P only)
- Wireless adapter slot (FR114W only)
- Wireless antenna (FM114P only)

## Connecting the Firewall

---

Before using your firewall, you need to do the following:

- Connect your cable or DSL modem to the Internet port of the firewall (described next).
- Connect your local Ethernet network to the Local port(s) of the firewall (see [page 2-5](#)).
- Prepare your wireless devices.
- Install your wireless adapter card (FR114W only)
- Connect the power adapter (see [page 2-6](#))

**Note:** The Resource CD included with your firewall contains an animated Connection Guide to help you through this procedure.

## Connecting to Your Internet Access Device

Your cable or DSL modem must provide a standard 10BASE-T or 100BASE-Tx Ethernet connection (not USB) for connection to your PC or network. The FR114P Firewall does not include a cable for this connection. Instead, use the Ethernet cable provided with your access device or any other standard Ethernet cable. Follow these steps:

1. Locate the Ethernet cable currently going from your DSL or cable modem to the computer that you use to access the Internet.

**Note:** You **must** use the existing cable to connect the modem to your firewall, not to connect your PCs to your firewall. The Ethernet cable supplied by your ISP for connecting to your cable or DSL modem may be an Ethernet crossover cable rather than a normal straight-through cable.

2. Remove this cable from the computer and insert that end into the Internet port on the firewall.
3. Turn the cable or DSL modem off for ten seconds, then on again.

## Connecting to your Local Ethernet Network

Your local area network (LAN) will attach to the firewall's Local ports shown in [Figure 2-2](#). The Local ports are capable of operation at either 10 Mbps (10BASE-T) or 100 Mbps (100BASE-Tx), depending on the Ethernet interface of the attached PC, hub, or switch. For any connection which will operate at 100 Mbps, you must use a Category 5 (CAT5) rated Ethernet cable, such as the cable included with the firewall.

The FR114P Firewall incorporates a four-port switch for connection to your local network. Ports 1 through 3 are permanently configured for MDI-X wiring, for connection to a PC. Port 4 can be set to MDI (Uplink) or MDI-X (Normal) by using the Normal/Uplink pushbutton switch.

Connect up to four PCs directly to any of the four Local ports of the firewall using standard Ethernet cables such as the one included with your firewall. If a PC is connected to port 4, be sure that the Normal/Uplink pushbutton switch is in the Normal position.

If your local network consists of more than four hosts, you will need to connect your firewall to another hub or switch. In this case, connect port 4 of your firewall to any port of an Ethernet hub or switch, and set the Normal/Uplink pushbutton switch to the Uplink position.

## Preparing your Wireless Devices

For the FM114P Wireless Firewall with Print Server, rotate the antenna to a vertical position and tighten the base.

### Installing a Wireless Card in the FR114W

The FR114W Wireless-Ready Firewall can be upgraded to wireless operation by purchasing and installing a NETGEAR Model MA401 802.11b Wireless PC Card. The FR114W will function normally without a wireless adapter card, but will not have wireless connectivity. To install the MA401 Wireless PC Card in your FR114W, follow these steps:

1. Locate the wireless adapter card slot on the rear panel.
2. Remove the rubber dust cover from the slot.
3. Slide the MA401 card into the slot with the card's front label and LED facing up.
4. Be sure that the MA401 card is securely seated into the internal connector.  
The blue plastic end cap of the MA401 card should be outside of the FR114W's case.

### Initial Configuration of Your Wireless PCs

Detailed instructions on configuring your wireless devices for TCP/IP networking are provided in the next chapter. However, if you already have a functioning wireless network and you wish to use a wireless PC to initially configure the firewall, you will need to change the settings of that PC to match the default settings of the firewall:

- The SSID should be **Wireless** (note the capitalization).
- WEP encryption is disabled.
- Your IP address must be in the range of 192.168.0.2 to 192.168.0.254, with a netmask of 255.255.255.0.

## Connecting the Power Adapter

To connect the firewall to the power adapter:

1. Plug the connector of the power adapter into the power adapter outlet on the rear panel of the firewall.
2. Plug the other end of the adapter into a standard wall outlet.
3. Verify that the Power LED on the firewall is lit.

## **Verifying Connections**

---

After applying power to the firewall, complete the following steps to verify the connections to it:

1. When power is first applied, verify that the POWER LED is on.
2. Verify that the TEST LED turns on within a few seconds.
3. After approximately 10 seconds, verify that:
  - a. The TEST LED has turned off.
  - b. The LOCAL LINK/ACT LEDs are lit for any local ports that are connected.
  - c. The INTERNET LINK/ACT LED is lit.

If a LINK/ACT LED is lit, a link has been established to the connected device.

4. If any port is connected to a 100 Mbps device, verify that the 100 LED for that port is lit.

The firewall is now properly attached to the network. Next, you need to prepare your network to access the Internet through the firewall. See the following chapter.





# Chapter 3

## Preparing Your Network

This chapter describes how to prepare your PC network to connect to the Internet through the FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall and how to order broadband Internet service from an Internet service provider (ISP).



**Note:** If an ISP technician configured your PC 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 PCs. Refer to [“Obtaining ISP Configuration Information \(Windows\)”](#) on page 3-10 or [“Obtaining ISP Configuration Information \(Macintosh\)”](#) on page 3-11 for further information.

### Preparing Your Personal Computers for IP Networking

---

Personal Computers access the Internet using a protocol called TCP/IP (Transmission Control Protocol/Internet Protocol). Each PC 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.

**Note:** In this chapter, we use the term “PC” to refer to personal computers in general, and not necessarily Windows computers.

Most PC 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, “Networks, Routing, and Firewall Basics.”](#)”

The NETGEAR ProSafe 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 IP Networking**

---

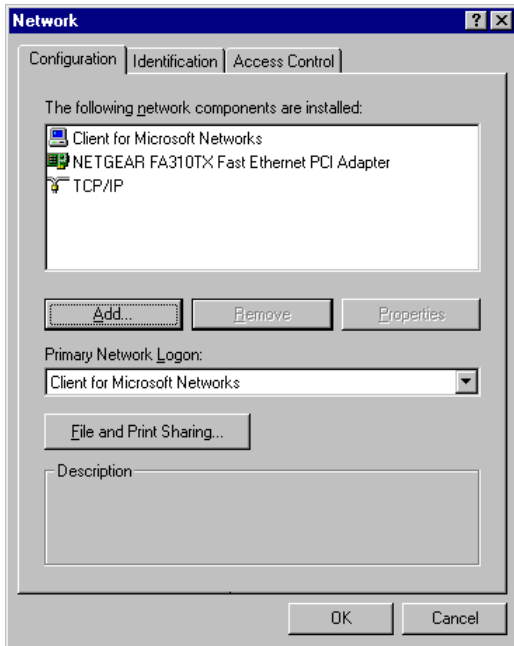
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

### **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 the adapter:

- 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.

## Assign TCP/IP configuration by DHCP

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 NETGEAR ProSafe 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 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 *winiipcfg.exe*:

1. On the Windows taskbar, click the Start button, and then click Run.
2. Type `winiipcfg`, 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 or 2000 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 IP Networking

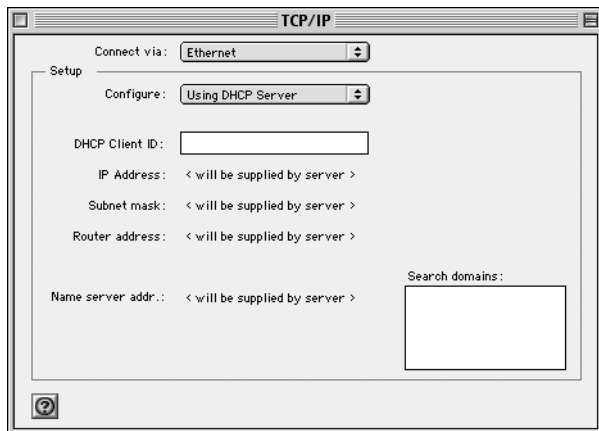
---

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:



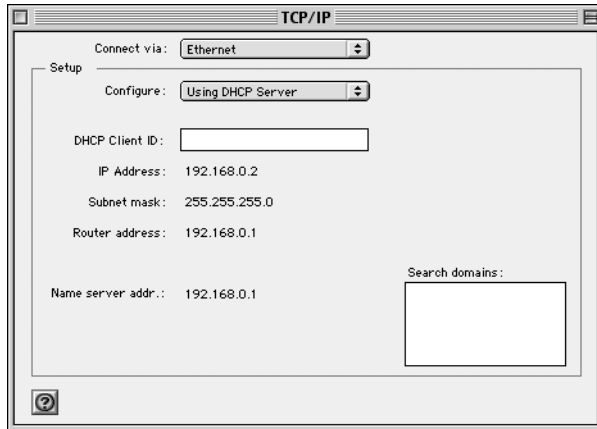
2. From the “Connect via” box, select your Macintosh’s Ethernet interface.
3. From the “Configure” box, select Using DHCP Server.  
You can leave the DHCP Client ID box empty.
4. Close the TCP/IP Control Panel.
5. Repeat this for each Macintosh on your network.

## 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 (Macintosh)

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”.

## Your Internet Account

---

For access to the Internet, you need to contract with an Internet service provider (ISP) for a single-user Internet access account using an external broadband access device such as 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 PC. 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 PC. 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.

## Login Protocols

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 firewall, you will need to enter your login name and password in the firewall'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.

## Account Information

Unless these items are dynamically assigned by the ISP, your ISP should give 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.xxx.yyy.com`

In this example, the domain suffix is `xxx.yyy.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 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 (Windows)**

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the NETGEAR ProSafe 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 (Macintosh)

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the NETGEAR ProSafe 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.

1. Turn off the DSL or cable modem, wait 15 seconds, and then turn it on again
2. Turn off the firewall, and then turn it on again and wait until the Test light turns off.
3. Restart any computer that is connected to the firewall.

**Note:** If the modem doesn’t have an on/off switch, either pull the modem’s power adapter out of the wall socket or power down the power strip.

## **Ready for Configuration**

---

After configuring all of your PCs for TCP/IP networking and connecting them to the local network of your NETGEAR ProSafe Firewall, you are ready to access and configure the firewall. Proceed to the next chapter.

# Chapter 4

## Basic Configuration

This chapter describes how to perform the basic configuration of your FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall using the Setup Wizard, which walks you through the configuration process for your Internet connection.

### Accessing the Web Configuration Manager

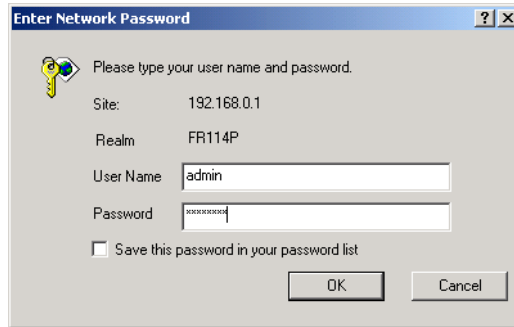
---

In order to use the browser-based Web Configuration Manager, your PC must have a web browser program installed such as Microsoft Internet Explorer or Netscape Navigator. Because the Configuration Manager uses Java, your Web browser must be Java-enabled and support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer 5.0 or Netscape Navigator 4.7 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

To configure for Internet access using your browser:

1. Connect your PC and firewall as described in the previous chapter. Make sure your PC has been rebooted since connecting with the firewall.
2. Launch your web browser.  
**Note:** If you normally use a login program (such as Enternet or WinPOET) to access the Internet, do not launch that program.
3. Click your browser's Stop button.
4. In the Address (or Location) box of your browser, type **http://192.168.0.1** and press ENTER.

A login window opens as shown in [Figure 4-1](#) below:



**Figure 4-1. Login window**

This screen may have a different appearance in other browsers.

5. Type **admin** in the User Name box, **password** in the Password box, and then click OK.  
(If your firewall password was previously changed, enter the current password.)

If your firewall has not yet been configured, the Setup Wizard should launch automatically. Otherwise, the main menu of the Web Configuration Manager will appear as shown in [Figure 4-2](#) below:

**NETGEAR FR114P Cable/DSL ProSafe Firewall with Print Server**

**settings**

**Router Status**

<b>System Name</b>	FR114P
<b>Firmware Version</b>	Version 1.0 Release 30

**WAN Port**

<b>MAC Address</b>	00c002f3250b
<b>IP Address</b>	
<b>DHCP</b>	DHCP Client
<b>IP Subnet Mask</b>	0.0.0.0
<b>Domain Name Server</b>	

**LAN Port**

<b>MAC Address</b>	00-c0-02-f3-25-0a
<b>IP Address</b>	192.168.0.1
<b>DHCP</b>	ON
<b>IP Subnet Mask</b>	255.255.255.0

**Router Status Help**

The *Router Status* page displays current settings and statistics for your router. As this information is read-only, any changes must be made on other pages.

**System Name:** This is the Account Name that you entered in the *Basic Settings* page.

**Firmware Version:** This is the current software the router is using. This will change if you upgrade your router.

**WAN Port Information:** These are the current settings for MAC address, IP address, DHCP role and Subnet Mask that you set in the *Basic Settings* page. DHCP can be either Client or None.

**LAN Port Information:** These are the current settings for MAC address, IP address, DHCP role and Subnet Mask that you set in the *LAN IP Setup* page. DHCP can be either Server or None.

Click **Show Statistics** to see router performance statistics such as number of packets sent and number of packets received for each port.

Buttons: Show Statistics, Show DHCP Status

Browser status: Done, Internet

**Figure 4-2. Browser-based configuration main menu**

You can manually configure your firewall using this menu as described in “[Manual Configuration](#)” on page 4-8, or you can allow the Setup Wizard to determine your configuration as described in the following chapter.

## Configuration using the Setup Wizard

---

The Web Configuration Manager contains a Setup Wizard that can automatically determine your network connection type. If the Setup Wizard does not launch automatically, click on the Setup Wizard heading in the upper left of the opening screen, shown in [Figure 4-2](#).

When the Wizard launches, allow the firewall to automatically determine your connection type by selecting Yes in the menu below and clicking Next:

### Setup Wizard

---

**System Can Now Detect The Connection Type Of WAN Port, Or You Can Configure It By Yourself.**

**Do You Want System To Detect The Connection Type?**

- Yes.
- No. I Want To Configure By Myself.
- 

Next

The Setup Wizard will now check for a connection on the Internet port. If the Setup Wizard determines that there is no connection to the Internet port, you will be prompted to check the physical connection between your firewall and cable or DSL modem. When the connection is properly made, the firewall's Internet LED should be on.

Next, the Setup Wizard will attempt to determine which of the following connection types your Internet service account uses:

- Dynamic IP assignment
- Fixed IP address assignment
- A login protocol such as PPPoE

The Setup Wizard will report which connection type it has discovered, and it will then use the appropriate configuration menu for that connection type.



## Configuring for Dynamic IP Account

If the Setup Wizard determines that your Internet service account uses Dynamic IP assignment, you will be directed to the menu shown in [Figure 4-3](#) below:

**Dynamic IP**

---

**Account Name** (If Required)

**Domain Name** (If Required)

---

**Domain Name Server (DNS) Address**

Get Automatically From ISP

Use These DNS Servers

Primary DNS

Secondary DNS

---

**Router's MAC Address**

Use Default Address

Use This MAC Address

---

**Figure 4-3. Setup Wizard menu for Dynamic IP address**

1. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.
2. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP transfers the IP addresses of one or two DNS servers to your firewall during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the firewall.

3. Router's MAC Address: This section determines the Ethernet MAC address that will be used by the firewall on the Internet port. If your ISP allows access by only one specific PC's Ethernet MAC address, select "Use this MAC address". The firewall will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP.

Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your firewall to masquerade as that PC by using its MAC address.

4. Click on Apply, then proceed to ["Completing the Configuration" on page 4-9](#).

## Configuring for Fixed IP Account

If the Setup Wizard determines that your Internet service account uses Fixed IP assignment, you will be directed to the menu shown in [Figure 4-4](#) below:

**Fixed IP**

---

**Internet IP Address**

IP Address

IP Subnet Mask

Gateway IP Address

---

**Domain Name Server (DNS) Address**

Primary DNS

Secondary DNS

---

**Figure 4-4. Setup Wizard menu for Fixed IP address**

1. Enter your assigned IP Address, Subnet Mask, and the IP Address of your ISP's gateway router. This information should have been provided to you by your ISP.
2. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP transfers the IP addresses of one or two DNS servers to your firewall during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the firewall.

3. Click on Apply, then proceed to [“Completing the Configuration” on page 4-9](#).

## Configuring for an Account with Login

If the Setup Wizard determines that your Internet service account uses a login protocol such as PPP over Ethernet (PPPoE), you will be directed to a menu like the PPPoE menu shown in [Figure 4-5](#) below:

**PPPoE**

Account Name

Domain Name

Login

Password

Idle Timeout

**Domain Name Server (DNS) Address**

Get automatically from ISP

Use these DNS servers

Primary DNS

Secondary DNS

Apply Cancel Test

**Figure 4-5. Setup Wizard menu for PPPoE login accounts**

1. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP’s services such as mail or news servers. If you leave the Domain Name field blank, the firewall will attempt to learn the domain automatically from the ISP. If this is not successful, you may need to enter it manually.
2. Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. If you wish to change the login timeout, enter a new value in minutes.

**Note:** You will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your firewall will automatically log you in.

3. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select "Use these DNS servers" and enter the IP address of your ISP's Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP transfers the IP addresses of one or two DNS servers to your firewall during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the firewall.

4. Click on Apply, then proceed to ["Completing the Configuration" on page 4-9](#).

## Manual Configuration

---

You can manually configure the firewall in the Basic Settings menu shown in [Figure 4-2](#) using these steps:

1. Select whether your Internet connection requires a login.  
Select 'Yes' if you normally must launch a login program such as EnterNet or WinPOET in order to access the Internet.
2. Enter your Account Name (may also be called Host Name) and Domain Name. These parameters may be necessary to access your ISP's services such as mail or news servers.
3. (If displayed) Enter the PPPoE login user name and password provided by your ISP. These fields are case sensitive. If you wish to change the login timeout, enter a new value in minutes.  
**Note:** You will no longer need to launch the ISP's login program on your PC in order to access the Internet. When you start an Internet application, your firewall will automatically log you in.
4. Internet IP Address: If your ISP has assigned you a permanent, fixed (static) IP address for your PC, select "Use static IP address". Enter the IP address that your ISP assigned. Also enter the netmask and the Gateway IP address. The Gateway is the ISP's router to which your firewall will connect.

5. Domain Name Server (DNS) Address: If you know that your ISP does not automatically transmit DNS addresses to the firewall during login, select “Use these DNS servers” and enter the IP address of your ISP’s Primary DNS Server. If a Secondary DNS Server address is available, enter it also.

A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP transfers the IP addresses of one or two DNS servers to your firewall during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually here. If you enter an address here, you should reboot your PCs after configuring the firewall.

6. Router’s MAC Address: This section determines the Ethernet MAC address that will be used by the firewall on the Internet port. Some ISPs will register the Ethernet MAC address of the network interface card in your PC when your account is first opened. They will then only accept traffic from the MAC address of that PC. This feature allows your firewall to masquerade as that PC by “cloning” its MAC address.

To change the MAC address, select "Use this Computer’s MAC address". The firewall will then capture and use the MAC address of the PC that you are now using. You must be using the one PC that is allowed by the ISP.

7. Click Apply, then proceed to [Completing the Configuration](#).

## Completing the Configuration

---

Click on the Test button to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to [Chapter 10, “Troubleshooting”](#).

Your firewall is now configured to provide Internet access for your network. When your firewall and PCs are configured correctly, your firewall automatically accesses the Internet when one of your LAN devices requires access.



**Note:** After your firewall has been configured, it will not be necessary to run a dialer or login application such as Dial-Up Networking, EnterNet, or WinPOET to connect, log in, or disconnect. These functions will be performed by the firewall as needed. Any such login software installed on your PC can be disabled or uninstalled.

To access the Internet from any PC connected to your firewall, launch a browser such as Microsoft Internet Explorer or Netscape Navigator. You should see the firewall’s Internet LED blink, indicating communication to the ISP. The browser should begin to display a Web page.

The following chapters describe how to configure the Advanced features of your firewall, and how to troubleshoot problems that may occur.

# Chapter 5

## Security

This chapter describes how to use the security features of your FR114P, FR114W or FM114P Cable/DSL ProSafe Firewall. The firewall provides you with selective blocking of inbound and outbound services, Web content filtering by keyword, and with security incident logging. You can configure the firewall to e-mail its log to you at specified intervals. You can also configure the firewall to send immediate alert messages to your e-mail address or e-mail pager whenever a significant security event occurs.

To configure these features of your firewall, click on the subheadings under the Security heading in the Main Menu of the browser interface.

### What is a Firewall

---

A firewall is a special category of router that protects one network (the “trusted” network, such as your LAN) from another (the “untrusted” network, such as the Internet), while allowing communication between the two. A firewall incorporates the functions of a NAT (Network Address Translation) router, while adding features for dealing with a hacker intrusion or attack, and for controlling the types of traffic that can flow between the two networks. Unlike simple Internet sharing NAT routers, a firewall uses a process called stateful packet inspection to protect your network from attacks and intrusions. NAT performs a very limited stateful inspection in that it considers whether the incoming packet is in response to an outgoing request, but true Stateful Packet Inspection goes far beyond NAT.

## Security Log

---

The firewall will log security-related events such as denied incoming and outgoing service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites menu, the Log page will also show 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 in [Figure 5-1](#):

### Logs

---

Date: 2002-05-01 14:23:28

```
Wed, 2002-05-01 14:20:46 - NETGEAR activated
Wed, 2002-05-01 14:20:48 - UDP packet dropped - Source:10.
,1236,WAN - Destination:192.0.0.192,161,LAN - [Default ru
Wed, 2002-05-01 14:22:25 - TCP packet dropped - Source:10.
,445,WAN - Destination:10.1.1.222,2604,LAN - [Default rul
Wed, 2002-05-01 14:23:08 - Administrator login successful
```

---

**Include in Log**

- 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

---

**Figure 5-1.** Logs menu



Log entries are described in [Table 5-1](#)

**Table 5-1. 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 5-2](#)

**Table 5-2. 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.

## 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 18:53:28 - Administrator login failed - IP:192.168.0.2

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 logging out of the firewall 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 timeout 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, and ICMP packet being dropped as a result of the default inbound rule, which states that all inbound packets are denied.]

## Block Sites

The NETGEAR ProSafe Firewall allows you to restrict access based on Web addresses and Web address keywords. Up to 255 entries are supported in the Keyword list. The Keyword Blocking menu is shown in [Figure 5-2](#):

The screenshot shows the 'Block Sites' configuration window. At the top, there is a checked checkbox labeled 'Turn Keyword Blocking On'. Below this is a text input field for entering a keyword, followed by an 'Add Keyword' button. A section titled 'Block Sites Containing These Keywords Or Domain Names:' contains a list box with the entry 'yahoo'. Below the list box are 'Delete Keyword' and 'Clear List' buttons. At the bottom, there is an unchecked checkbox labeled 'Allow Trusted IP Address To Visit Blocked Sites', followed by a 'Trusted IP address' field with four input boxes containing the number '0'. At the very bottom are 'Apply' and 'Cancel' buttons.

**Figure 5-2. Block Sites menu**

To enable keyword blocking, check “Turn keyword blocking on”, then click Apply.

To add a keyword or domain, type it in the Keyword box, click Add Keyword, then click Apply.

To delete a keyword or domain, select it from the list, click Delete Keyword, then click Apply.

Keyword application examples:

- If the keyword "XXX" is specified, the URL <http://www.badstuff.com/xxx.html> is blocked.
- If the keyword “.com” is specified, only websites with other domain suffixes (such as .edu or .gov) can be viewed.
- If you wish to block all Internet browsing access, enter the keyword “.”.

To specify a Trusted User, enter that PC’s IP address in the Trusted User box and click Apply.

You may specify one Trusted User, which is a PC that will be exempt from blocking and logging. Since the Trusted User will be identified by an IP address, you should configure that PC with a fixed or reserved IP address.

## Rules

Firewall rules are used to block or allow specific traffic passing through from one side to the other. Inbound rules (WAN to LAN) restrict access by outsiders to private resources, selectively allowing only specific outside users to access specific resources. Outbound rules (LAN to WAN) determine what outside resources local users can have access to.

A firewall has two default rules, one for inbound traffic and one for outbound. The default rules of the NETGEAR ProSafe Firewall are:

- Inbound: Block all access from outside except responses to requests from the LAN side.
- Outbound: Allow all access from the LAN side to the outside.

These default rules are shown in the Rules table of the Rules menu in [Figure 5-3](#):

**Rules**

---

**Outbound Services**

#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
Default	Yes	Any	ALLOW always	Any	Any	Never

**Inbound Services**

#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
Default	Yes	Any	BLOCK always	--	Any	Match

---

Default DMZ Server     
  .  .  .

Respond to Ping on Internet WAN Port

**Figure 5-3. Rules menu**

You may define additional rules that will specify exceptions to the default rules. By adding custom rules, you can block or allow access based on the service or application, source or destination IP addresses, and time of day. You can also choose to log traffic that matches or does not match the rule you have defined.

To create a new rule, click the Add button.

To edit an existing rule, select its button on the left side of the table and click Edit.

To delete an existing rule, select its button on the left side of the table and click Delete.

To move an existing rule to a different position in the table, select its button on the left side of the table and click Move. At the script prompt, enter the number of the desired new position and click OK.

An example of the menu for defining or editing a rule is shown in [Figure 5-4](#). The parameters are:

- **Service**  
From this list, select the application or service to be allowed or blocked. The list already displays many common services, but you are not limited to these choices. Use the Services menu to add any additional services or applications that do not already appear.
- **Action**  
Choose how you would like this type of traffic to be handled. You can block or allow always, or you can choose to block or allow according to the schedule you have defined in the Schedule menu.
- **Source Address**  
Specify traffic originating on the LAN (outbound) or the WAN (inbound), and choose whether you would like the traffic to be restricted by source IP address. You can select Any, a Single address, or a Range. If you select a range of addresses, enter the range in the start and finish boxes. If you select a single address, enter it in the start box.
- **Destination Address**  
The Destination Address will be assumed to be from the opposite (LAN or WAN) of the Source Address. As with the Source Address, you can select Any, a Single address, or a Range unless NAT is enabled and the destination is the LAN. In that case, you must enter a Single LAN address in the start box.
- **Log**  
You can select whether the traffic will be logged. The choices are:
  - Never - no log entries will be made for this service.
  - Always - any traffic for this service type will be logged.

- Match - traffic of this type which matches the parameters and action will be logged.
- Not match - traffic of this type which does not match the parameters and action will be logged.

## Inbound Rules (Port Forwarding)

Because the NETGEAR ProSafe Firewall uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet. The rule tells the firewall to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding. .



**Note:** Some residential broadband ISP accounts do not allow you to run any server processes (such as a Web or FTP server) from your location. Your ISP may periodically check for servers and may suspend your account if it discovers any active services at your location. If you are unsure, refer to the Acceptable Use Policy of your ISP.

Remember that allowing inbound services opens holes in your firewall. Only enable those ports that are necessary for your network. Following are two application examples of inbound rules:

## Inbound Rule Example: A Local Public Web Server

If you host a public web server on your local network, you can define a rule to allow inbound web (HTTP) requests from any outside IP address to the IP address of your web server at any time of day. This rule is shown in [Figure 5-4](#):

**Inbound Services**

---

Service: HTTP(TCP:80) [v]  
Action: ALLOW always [v]  
Send to LAN Server: 192 . 168 . 0 . 99  
WAN Users: Any [v]  
start: 0 . 0 . 0 . 0  
finish: 0 . 0 . 0 . 0  
Log: Never [v]

---

Back Apply Cancel

**Figure 5-4.** Rule example: A Local Public Web Server

## Inbound Rule Example: Allowing Videoconference from Restricted Addresses

If you want to allow incoming videoconferencing to be initiated from a restricted range of outside IP addresses, such as from a branch office, you can create an inbound rule. In the example shown in [Figure 5-5](#), CU-SeeMe connections are allowed only from a specified range of external IP addresses. In this case, we have also specified logging of any incoming CU-SeeMe requests that do not match the allowed parameters.

### Inbound Services

The screenshot shows the configuration for an inbound service rule. The fields are as follows:

- Service:** CU-SEEME(TCP/UDP:7648)
- Action:** ALLOW always
- Send to LAN Server:** 192 . 168 . 0 . 11
- WAN Users:** Address Range
  - start: 134 . 177 . 88 . 1
  - finish: 134 . 177 . 88 . 254
- Log:** Not Match

At the bottom of the form are three buttons: Back, Apply, and Cancel.

**Figure 5-5.** Rule example: Videoconference from Restricted Addresses

### Considerations for Inbound Rules:

- If your external IP address is assigned dynamically by your ISP, the IP address may change periodically as the DHCP lease expires. Consider using the Dynamic DNS feature in the Advanced menu so that external users can always find your network.
- If the IP address of the local server PC is assigned by DHCP, it may change when the PC is rebooted. To avoid this, use the Reserved IP address feature in the LAN IP menu to keep the PC's IP address constant.
- Local PCs must access the local server using the PCs' local LAN address (192.168.0.99 in this example). Attempts by local PCs to access the server using the external WAN IP address will fail.



## Outbound Rules (Service Blocking)

The NETGEAR ProSafe Firewall allows you to block the use of certain Internet services by PCs on your network. This is called service blocking or port filtering. You can define an outbound rule to block Internet access from a local PC based on:

- the IP address of the local PC (source address)
- the IP address of the Internet site being contacted (destination address)
- the time of day
- the type of service being requested (service port number)

Following is an application example of outbound rules:

### Outbound Rule Example: Blocking Instant Messenger

If you want to block Instant Messenger usage by employees during working hours, you can create an outbound rule to block that application from any internal IP address to any external address according to the schedule that you have created in the Schedule menu. You can also have the firewall log any attempt to use Instant Messenger during that blocked period.

#### Outbound Services

Service: AIM(TCP:5190)

Action: BLOCK by schedule,otherwise allow

LAN users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

WAN Users: Any

start: 0 . 0 . 0 . 0

finish: 0 . 0 . 0 . 0

Log: Match

Back Apply Cancel

**Figure 5-6. Rule example: Blocking Instant Messenger**

## Order of Precedence for Rules

As you define new rules, they are added to the tables in the Rules menu, as shown in [Figure 5-7](#):

**Rules**

---

**Outbound Services**

	#	Enable	Service Name	Action	LAN Users	WAN Servers	Log
<input type="radio"/>	1	<input checked="" type="checkbox"/>	AIM	BLOCK by schedule	Any	Any	Match
	Default	Yes	Any	ALLOW always	Any	Any	Never

**Inbound Services**

	#	Enable	Service Name	Action	LAN Server IP address	WAN Users	Log
<input checked="" type="radio"/>	1	<input checked="" type="checkbox"/>	CU-SEEME	ALLOW always	192.168.0.11	134.177.88.1 - 134.177.88.254	Not Match
<input type="radio"/>	2	<input checked="" type="checkbox"/>	HTTP	ALLOW always	192.168.0.99	Any	Never
	Default	Yes	Any	BLOCK always	--	Any	Match

---

Default DMZ Server

Respond to Ping on Internet WAN Port

**Figure 5-7. Rules table with examples**

For any traffic attempting to pass through the firewall, the packet information is subjected to the rules in the order shown in the Rules Table, beginning at the top and proceeding to the default rules at the bottom. In some cases, the order of precedence of two or more rules may be important in determining the disposition of a packet. The Move button allows you to relocate a defined rule to a new position in the table.

## Default DMZ Server

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 for which you have configured an inbound rule. Instead of discarding this traffic, you can have it forwarded to one computer on your network. This computer is called the 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, NETGEAR strongly recommends that you 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.

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.



**Note:** In this application, the use of the term 'DMZ' has become common, although it is a misnomer. In traditional firewalls, a DMZ is actually a separate physical network port. A true DMZ port is for connecting servers that require greater access from the outside, and will therefore be provided with a different level of security by the firewall. A better term for our application is Exposed Host.

## Respond to Ping on Internet WAN Port

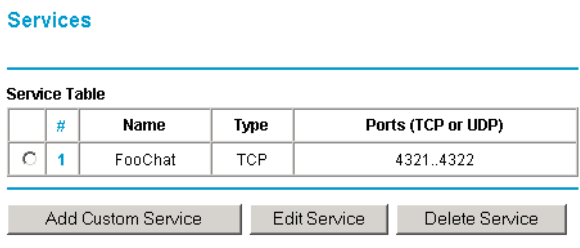
If you want the firewall to respond to a 'ping' from the Internet, click the 'Respond to Ping on Internet WAN Port' check box. This should only be used as a diagnostic tool, since it allows your firewall to be discovered. Don't check this box unless you have a specific reason to do so.

## Services


Services are functions performed by server computers at the request of client computers. For example, Web servers serve web pages, time servers serve time and date information, and game hosts serve data about other players' moves. When a computer on the Internet sends a request for service to a server computer, the requested service is identified by a service or port number. This number appears as the destination port number in the transmitted IP packets. For example, a packet that is sent with destination port number 80 is an HTTP (Web server) request.

The service numbers for many common protocols are defined by the Internet Engineering Task Force (IETF) and published in RFC1700, "Assigned Numbers." Service numbers for other applications are typically chosen from the range 1024 to 65535 by the authors of the application.

Although the NETGEAR ProSafe Firewall already holds a list of many service port numbers, you are not limited to these choices. Use the Services menu to add additional services and applications to the list for use in defining firewall rules. The Services menu shows a list of services that you have defined, as shown in [Figure 5-8](#):



The screenshot shows a web interface titled "Services". Below the title is a "Service Table" with the following data:

	#	Name	Type	Ports (TCP or UDP)
	1	FooChat	TCP	4321..4322

Below the table are three buttons: "Add Custom Service", "Edit Service", and "Delete Service".

**Figure 5-8. Services menu**

To define a new service, first you must determine which port number or range of numbers is used by the application. This information can usually be determined by contacting the publisher of the application or from user groups of newsgroups. When you have the port number information, go to the Services menu and click on the Add Custom Service button. The Add Services menu will appear, as shown in [Figure 5-9](#):

**Services**

---

**Service Definition**

Name:

Type:

Start Port:  (TCP or UDP)

Finish Port:  (TCP or UDP)

---

**Figure 5-9. Add Custom Service menu**

To add a service,

1. Enter a descriptive name for the service so that you will remember what it is.
2. Select whether the service uses TCP or UDP as its transport protocol.  
If you can't determine which is used, select both.
3. Enter the lowest port number used by the service.
4. Enter the highest port number used by the service.  
If the service only uses a single port number, enter the same number in both fields.
5. Click Apply.

The new service will now appear in the Services menu, and in the Service name selection box in the Rules menu.

## Schedule

If you enabled content filtering in the Block Sites menu, or if you defined an outbound rule to use a schedule, you can set up a schedule for when blocking occurs or when access is restricted. The firewall allows you to specify when blocking will be enforced by configuring the Schedule tab shown below:

**Schedule**

---

Use this schedule for rules

---

**Days to block:**

Every Day

Sunday

Monday

Tuesday

Wednesday

Thursday

Friday

Saturday

---

**Time of day to block:** (use 24-hour clock)

All Day

Start Blocking  hour  minute

End Blocking  hour  minute

---

**Time Zone**

(GMT-08:00)Pacific Time (US Canada) ▼

Adjust for daylight savings time

Use this NTP Server

**Current time:** Wed, 2002-05-01 15:32:06

---

To block keywords or Internet domains based on a schedule:

1. Select Every Day or select one or more days.
2. If you want to limit access completely for the selected days, select All Day. Otherwise, If you want to limit access during certain times for the selected days, type a Start Blocking time and an End Blocking time.

**Note:** Note: Enter the values as 24-hour time. For example, 10:30 am would be 10 hours and 30 minutes and 10:30 pm would be 22 hours and 30 minutes.

3. Click Apply

### **Time Zone**

The NETGEAR ProSafe Firewall uses the Network Time Protocol (NTP) to obtain the current time and date from one of several Network Time Servers on the Internet. In order to localize the time for your log entries, you must select your Time Zone from the list.

If your region uses Daylight Savings Time, you must manually check Adjust for Daylight Savings Time at the beginning of the Daylight Savings Time, and uncheck it at the end. Enabling Daylight Savings Time will cause one hour to be added to the standard time.

The firewall has a list of publicly available NTP servers. If you would prefer to use a particular NTP server as the primary server, enter its IP address under Use this NTP Server.

Be sure to click Apply when you have finished configuring this menu.

## E-Mail

---

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

**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**

Frequency:

Day:

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 immediately sent to the specified e-mail address when any of the following events occur:

- If a Denial of Service attack is detected
- If a Port Scan is detected
- If a user on your LAN attempts to access a website that you blocked using Keyword blocking.



You can specify that logs are sent to you according to a schedule. Select whether you would like to receive the logs Hourly, Daily, Weekly, or When Full. Depending on your selection, you may also need to specify:

- Day for sending log  
Relevant when the log is sent weekly or daily.
- Time for sending 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.

Be sure to click Apply when you have finished configuring this menu.



# Chapter 6

## Wireless

This chapter describes how to configure the Wireless networking features of your FR114W Wireless-Ready Firewall or FM114P Wireless Firewall with Print Server. This chapter does not apply to the FR114P Firewall with Print Server.

The FR114W Wireless-Ready Firewall can be upgraded to wireless operation by purchasing and installing a NETGEAR Model MA401 802.11b Wireless PC Card. For instructions on upgrading the FR114W, refer to [“Installing a Wireless Card in the FR114W” on page 2-6](#).



**Note:** If you are configuring the firewall from a wireless PC and you change the firewall'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 firewall's new settings.

## Wireless Settings

---

To configure the Wireless interface of your firewall, 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](#):

**Wireless Settings**

---

**Identification**  
Regulatory Domain: USA/Canada  
Station Name: FR114W  
SSID (Service Set Identifier):

---

**Options**  
Channel No:   
WEP Status: no data encryption

---

**Access Point**  
Allow access by:  
 Everyone  
 Trusted PCs only

---

**Figure 6-1. Wireless Settings menu**

### Identification

In the Identification section are the following parameters:

- **Regulatory Domain**  
This field displays the region of operation for which the wireless interface is intended. It may not be legal to operate the firewall in a region other than the region shown here.
- **Station Name**  
This is the Account Name that was defined in the Basic Settings menu. Some Wireless status screens may display this name as the Access Point in use.
- **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.

## Options

### Channel Number

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. The default wireless channel is 10.

### WEP Status

This field displays the current WEP (Wired Equivalent Privacy) setting. To enable WEP or change the encryption level or keys, click the Configure WEP button and follow the instructions in [“Configuring WEP \(Wired Equivalent Privacy\)” on page 6-4](#).

## Access Point

For increased security, you can restrict access to the wireless network to only allow specific PCs, based on their MAC addresses. You can allow access by:

- Everyone  
In this case, the firewall will allow access to any PC with the correct SSID.
- Trusted PCs only  
In this case, the firewall will authenticate each wireless PC by SSID and by MAC address, using the list of MAC addresses you have entered. To specify the allowed MAC addresses, click the Trusted PCs button and follow the instructions in [“Restricting Wireless Access by MAC Address” on page 6-5](#).

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

## Configuring WEP (Wired Equivalent Privacy)

From the Wireless menu, click the Configure WEP button to display the Wireless WEP menu, shown in [Figure 6-2](#):

### Wireless WEP

The screenshot shows the 'Wireless WEP' configuration window. At the top, 'Authentication Type' is a dropdown menu set to 'Automatic'. Below this, the 'Encryption' section has three radio buttons: 'Off - no data encryption', '64 Bit Encryption', and '128 Bit Encryption', with the last one selected. Underneath, there are four key input fields labeled 'Key 1' through 'Key 4'. Each key field contains 12 hexadecimal characters in individual boxes. Key 1 contains '93 1c 87 96 61 5d 4d e8 40 ae ad 74 2b'. Keys 2, 3, and 4 each contain '00 00 00 00 00 00 00 00 00 00 00 00'. Below the keys is a 'Default Key' dropdown menu set to '1'. At the bottom left is a 'Passphrase:' text input field, and at the bottom right is a 'Generate Keys' button. At the very bottom of the window are three buttons: 'Back', 'Apply', and 'Cancel'.

**Figure 6-2. Wireless WEP menu**

### 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

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.

- Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F)
- Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate Keys button.

#### Default Key

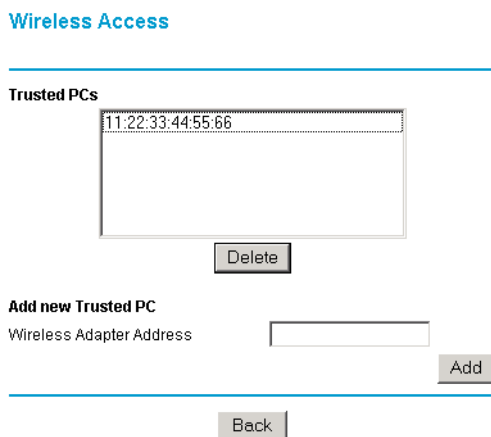
Select which of the four keys will be active.

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

## Restricting Wireless Access by MAC Address

---

For increased security, you can restrict access to the wireless network to only allow specific PCs, based on their MAC addresses. From the Wireless menu, click the Trusted PCs button to display the Wireless Access menu, shown in [Figure 6-3](#):



**Figure 6-3. Wireless Access menu**

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

1. Select “Trusted PCs only” in the Wireless Settings menu, then click Apply.
2. Click the “Trusted PCs” button to go to the Wireless Access menu.

3. Obtain the Ethernet MAC address of the wireless interface card of each authorized PC. This address is usually printed on the card itself, or it may appear in the router's DHCP table.
4. Enter each MAC address into the Wireless Adapter Address box, then click Add.

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

## Additional Notes

---

### 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.

If your wireless PCs need Internet access but don't require access to your private wired network, disable bridging between the wireless and wired PCs

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.

For further information on wireless networking, refer to [“Wireless Networking”](#) in [Appendix B, “Networks, Routing, and Firewall Basics.”](#)

### Placement and Range

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the wireless firewall. For best results, place your firewall:

- 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.



# Chapter 7

## Print Server

This chapter describes how to install and configure the print server in your FR114P Firewall with Print Server or FM114P Wireless Firewall with Print Server. This chapter does not apply to the FR114W Wireless-Ready Firewall.

### Network Printing from Windows

---

The NETGEAR ProSafe Firewall supports two methods for printing from Windows:

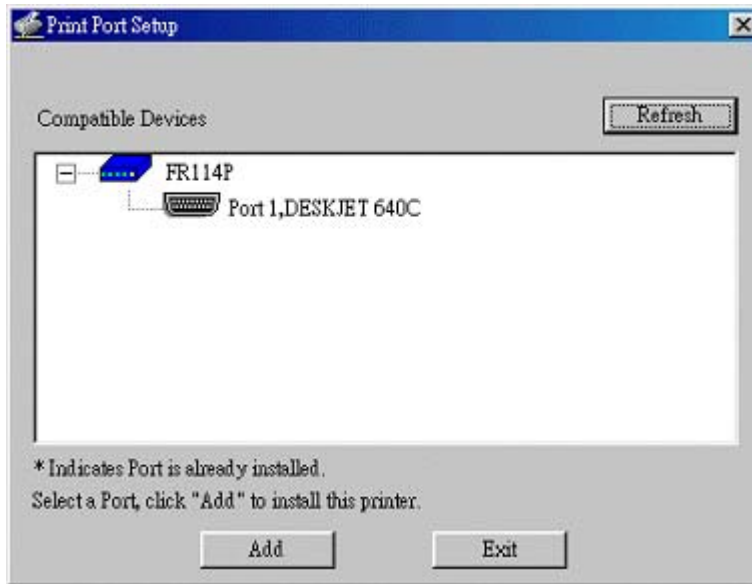
- **Print Port Driver**  
After installing the Print Port Driver, Windows users can print directly to the firewall. Print jobs are spooled (queued) on each PC. The supplied Print Port Driver supports Windows 95/98/ME, NT4.0, Windows 2000 and Windows XP.
- **LPD/LPR Printing**  
If using Windows NT 4.0 Server or Windows 2000 Server, LPD/LPR printing can be used. No software needs to be installed on either the Windows Server or each client PC. Print jobs will be spooled (queued) on the Windows Server, and can be managed using the standard Windows Server tools.

### Installing the PTP Driver

The following procedure is for all versions of Windows (95/98/ME, NT4.0, 2000, XP). The Windows 'Add Printer' screens will vary depending on your version of Windows, but the procedure is the same:

1. Make sure that the printer is ON and connected to the firewall's printer port.
2. Insert the supplied CD-ROM into your drive. If the setup program does not start automatically, run SETUP.EXE in the root folder.

3. Scroll down to the Drivers section and click on FR114P Print Server driver for Windows.
4. When asked, select 'Run this program from its current location'.
5. Follow the steps to install the Print Server driver.
6. When the installation is finished, make sure the 'Run Print Port Setup now' checkbox is checked, and click Finish.
7. The Print Port Setup will then run, and the following screen will be displayed:



The screen should show your firewall and printer.

8. Click on the Port 1 symbol, and then click the Add button.

**Note:** Under Windows95, you may receive an error message stating that SETUPAPI.DLL was not found. In this case, you should either upgrade your Internet Explorer to version 5 or later, or consult the Print Server Troubleshooting section in this chapter.

9. A pop-up message will inform you if the port has been created successfully, and then the Windows Add Printer wizard will start.
  - a. Click Next to browse for your printer on the network.
  - b. Select the correct Printer Manufacturer and Model, or use the 'Have Disk' option if appropriate.

- c. If desired, change the Printer name to be more descriptive (such as DeskJet on PrintServer)
- d. If prompted about Sharing, do NOT enable Sharing.

10. Installation is now complete. You can now print using this printer.

To make changes later, use the Start menu to run this program. The default installation is Start -> Programs -> NETGEAR Firewall Print Server -> Add Port.

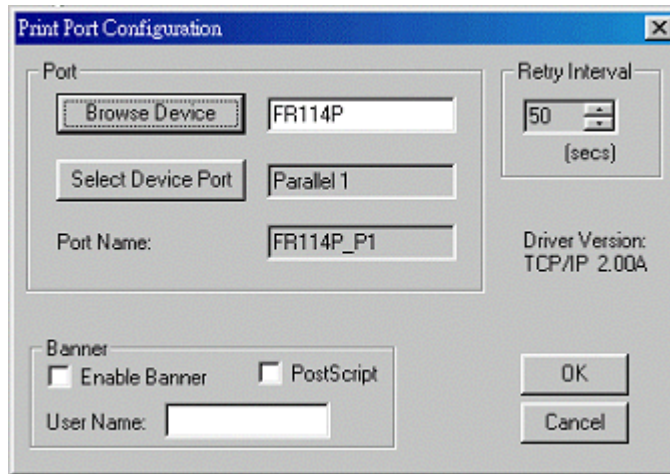
## **Printer Management**

- Using PTP printing, print jobs can be managed in the same manner as any Windows printer. Open the Printers folder (Start -> Settings -> Printers) and double-click any printer to see the current print jobs.
- If the printer attached to the firewall is changed, run the 'Add Port' program again and select the new printer.
- To delete a port created by this setup program, use the 'Windows Delete Port' facility:
  - a. Right-click any printer in the Printers folder, and select Properties.
  - b. Locate the Delete Port button. This button is on either the Details or Ports tab, depending on your version of Windows.

## **Port Options**

The options for the Print Port Driver are accessed via the Windows Port Settings button.

Use Start -> Settings -> Printers to open the Printers folder, then right-click the Printer and select Properties. The Port Settings button is on either the Details or Port tab, depending on your version of Windows. An example screen is shown below:



Items shown on this screen are as follows:

- **Port**  
If desired, click Browse to select a different device. The 'Select Device Port' button supports multi-port models, but the firewall is a single-port print server. The Port Name is shown in the Printer's Properties.
- **Banner**  
Check this option to print a banner page before each print job. The User Name will be printed on the banner page. If using a PostScript Printer, check the PostScript box.
- **Retry Interval**  
Determines how often Windows will poll the print server to establish a connection when the printer is busy.

## LPD/LPR Printing from Windows

LPD/LPR printing is supported by Windows NT 4.0 Server and Windows 2000/XP. No software needs to be installed on the client PCs. Third-party drivers are available for earlier versions of Windows.

## **Windows NT 4.0 Server Configuration**

To use LPD printing, Microsoft TCP/IP Printing must be installed and enabled. This can be checked using Start-Settings-Control Panel-Network - Services.

To configure your NT 4.0 Server for LPD printing, follow this procedure:

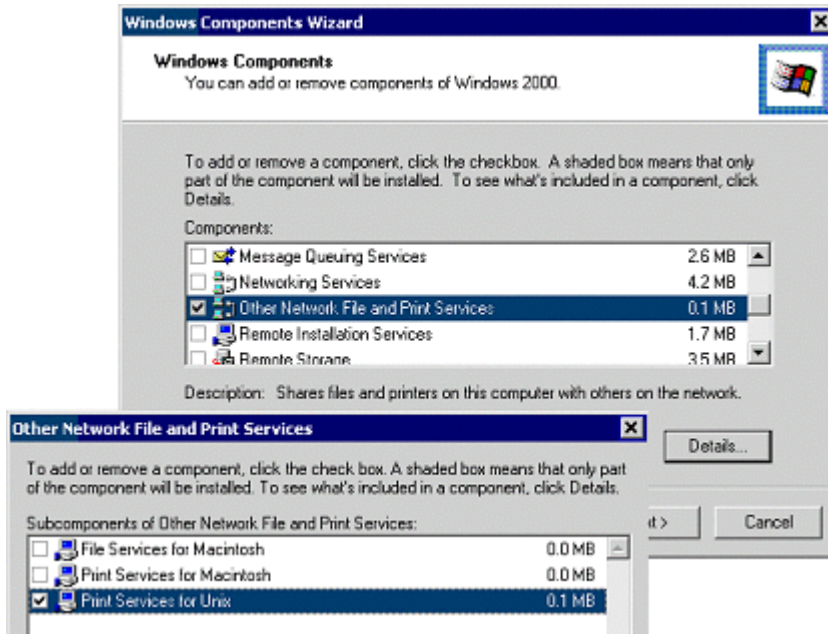
1. Go to Start->Settings->Printers and launch the Add Printer wizard.
2. When prompted with 'This printer will be managed by..', select My Computer and click Next.
3. Select Add Port, then select LPR Port and click New Port.
4. In the Dialog requesting 'Name or Address of server providing lpd', enter the IP address of the FR114P Firewall.
5. For Name of printer or print queue on that server, enter L1.
6. Click OK. When returned to the Printer Ports window, select Close and then install your printer driver as usual.
7. When prompted about Sharing, select the Sharing button.
8. In the Shared dialog box, enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
9. Click OK to save and exit.

## **Windows 2000 Server Configuration**

The LPD/LPR Port is not enabled by default. To enable it, use this procedure:

1. In Control Panel, select Add/Remove Programs, then Windows Components.

2. Select Other Network File and Print Services, then click the Details button.

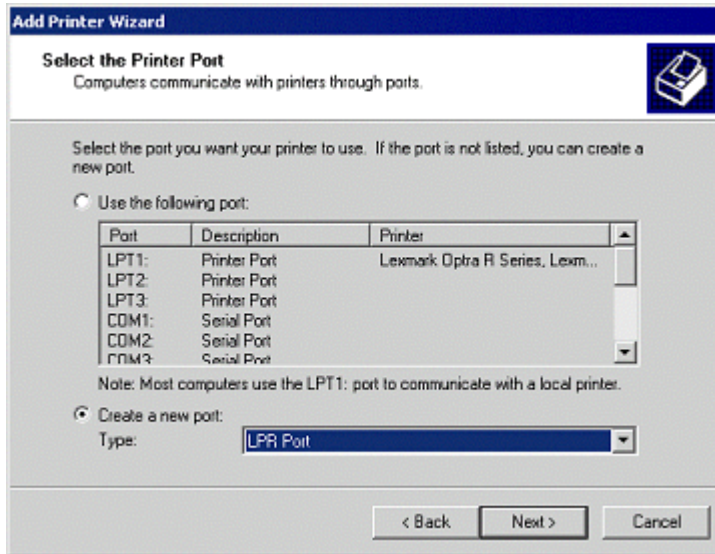


3. Enable Print Services for Unix, then click OK.
4. Click Next and complete the Wizard.

#### Adding the Printer:

1. Open your Printers folder, and start the Add Printer Wizard.
2. When prompted, select Local Printer.

3. In the Select the Printer Port screen, select LPR Port, as shown below. Click Next to continue.



4. In the Dialog requesting 'Name or Address of server providing lpd', enter the IP address of the FR114P Firewall.
5. For Name of printer or print queue on that server, enter L1.
6. Click OK, then Next, and continue the Wizard.
7. At the Select Sharing screen, select the button for Share As, and enter the shared printer name. The shared name is how other users will see this printer. You should advise client PCs of the Server name and this printer name.
8. Complete the Add Printer wizard.

## Client PC Setup for LPD/LPR Printing

After configuring the Windows Server, client PCs on the LAN can install the new printer.

The following procedure is for Windows 95/98/ME, Windows NT4.0, and Windows 2000 workstation.

1. From Start -> Settings, open the Printers folder, and start the Add Printer Wizard.
2. When prompted, select Network Printer.

3. When prompted for Network Path or Queue Name, click the Browse button, and locate the Server and Printer that your Network Administrator advised you to use.
4. Click OK, then Next.
5. Select the correct printer Manufacturer and Model, then click Next.
6. Follow the prompts to complete the Wizard.
7. The new printer will be listed with any other installed printers, and may be selected when printing from any Windows application.



## Network Printing from the Macintosh

---

Macintosh computers can connect to a TCP/IP network printer using the Line Printer Remote (LPR) protocol. LPR printing can be set up on any Macintosh that has Desktop Printing installed or available. Desktop Printing is supported on MacOS versions beginning from 8.1. LaserWriter8 version 8.5.1 or higher is also required.

### MacOS 8 or 9 Configuration

To configure the Macintosh to use the print server, follow these steps:

1. From the Apple Extras folder, under Apple LaserWriter Software, launch the Desktop Printing Utility.  
A new window titled New Desktop Printer will appear.
2. Select LaserWriter 8 in the 'With' drop-down menu.
3. Select Printer (LPR) and click OK.  
A new window titled Untitled 1 will open.
4. If the PostScript Printer Description does not match your printer, click Change... and select your actual printer.  
If your printer model does not appear, click the Generic button.
5. Click OK to return to the Untitled 1 window.
6. In the LPR Printer Selection box, click Change...
7. In the Printer Address field, type the name or IP address of the firewall.  
The IP address will usually be 192.168.0.1.  
You can leave the Queue Name blank.
8. Click Verify to make sure your computer can see the printer.  
You should see the IP address displayed above the button. If no IP address appears, check that you have correctly typed the queue name or IP Address.
9. Click OK to return to the Untitled 1 window.
10. At the bottom of the Untitled 1 dialog box, click 'Create...'.  
A printer icon should now appear on your desktop.
11. When prompted, rename the printer with a descriptive name and click Save.  
A printer icon should now appear on your desktop.
12. Quit the Desktop Printer Utility.

## MacOS X Configuration

To configure the Macintosh to use the print server, follow these steps:

1. Activate the Print Center.
2. Select Printers from the menu bar.
3. Click 'Add Printer' from the Printers drop-down menu.
4. Choose the 'LPR Printers using IP' option, and enter the following items:
  - a. LPR Printer's Address  
Enter the firewall's LAN IP address (usually 192.168.0.1).
  - b. Check 'Use default Queue on Server'.
  - c. Select the Printer Model that is connected to the firewall's printer port.
5. Click Add to add this printer.

## Network Printing from Linux

---

Linux, FreeBSD, and other similar operating systems can use the Line Printer Remote (LPR) protocol to connect to the network print server. Because of variations in the configuration environments for these operating systems, please refer to your operating system documentation for information on configuring for LPR printing.

The NETGEAR ProSafe Firewall's print server supports graphics mode printing.

## Troubleshooting the Print Server

---

*When I tried to install the Printer Driver for Peer-to-Peer printing, I received an error message and the installation was aborted.*

This may be caused by an existing installation of the printer port software. Before attempting another installation, remove the existing installation and restart your PC.

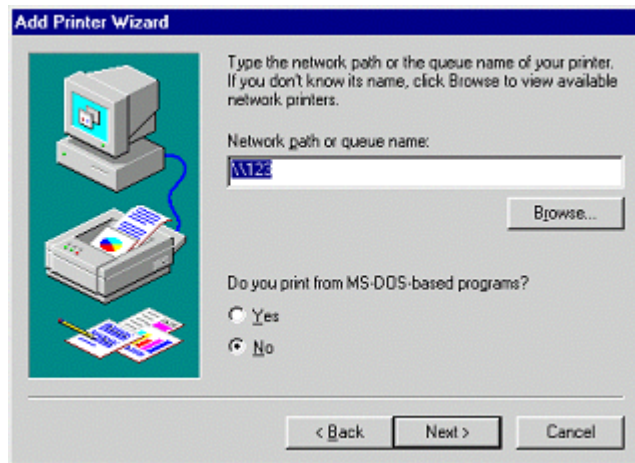
To remove an existing printer port installation:

- a. Open Start -> Settings -> Control Panel -> Add/Remove Programs.
- b. Look for an entry with a name like "NETGEAR ProSafe Firewall Router", "NETGEAR Print Server", "Print Server Driver" or "Print Server Port".
- c. Select this item, click Add/Remove, and confirm the deletion.

*I am using Windows 95. The Printer Driver installed and ran, but when I selected a port and clicked Add, the printer was not installed.*

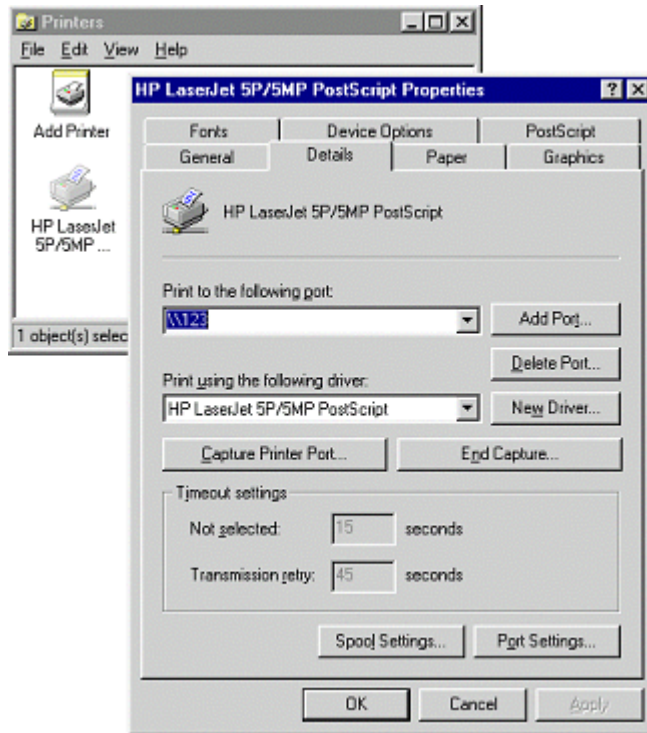
Try installing the printer using the standard Windows tools, as follows:

- a. From Start -> Settings, open the Printers folder, and start the Add Printer Wizard.
- b. When prompted, select Network Printer and click Next.
- c. For Network Path or Queue, enter a dummy value such as \\123, as shown below. Select NO for "Do you print from MS-DOS programs?".



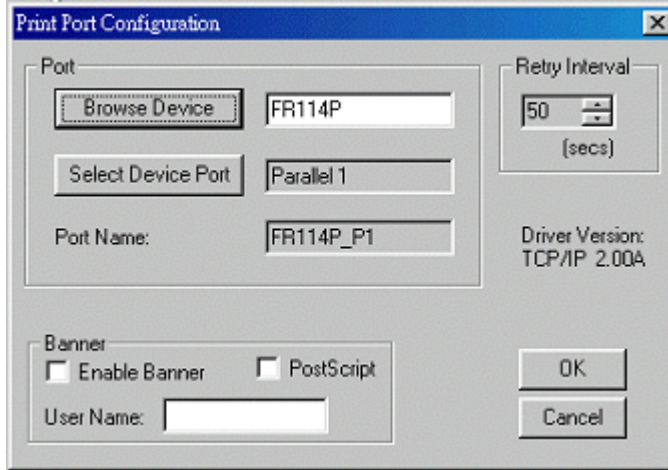
- d. The printer wizard will display a message stating that "The Network Printer is off-line". This is OK. Continue the Add Printer Wizard until finished.
- e. When finished, go to Start -> Settings -> Printers. The new printer icon will be grayed out indicating the printer is not ready.

- f. Right-click the new printer and select Properties. Then select the Details tab, as shown below.

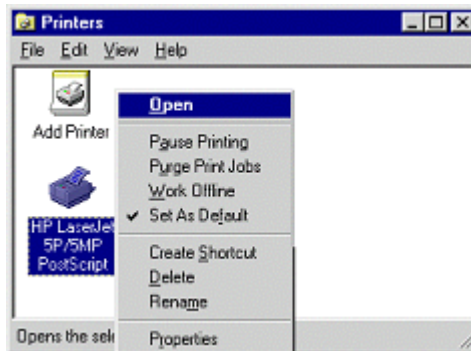


- g. Click the Add Port button. On the resulting screen, select Other, then select the NETGEAR Print Server Port as the port to add.

- h. Click OK to see the Print Port Configuration screen.



- i. Click the Browse Device button, select the firewall, and click OK.
- j. Click OK to return to the Printers folders, and right-click on the new printer. Make sure that the Work Offline option is NOT checked.



- k. The new printer should no longer be grayed out, and is ready for use.



# Chapter 8

## Maintenance

This chapter describes how to use the maintenance features of your FR114P, FR114W and FM114P Cable/DSL ProSafe Firewalls. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

### System Status

---

The System Status menu provides a limited amount of status and usage information. From the Main Menu of the browser interface, under Maintenance, select System Status to view the System Status screen, shown in [Figure 8-1](#).

**Router Status**

---

<b>System Name</b>	FR114P
<b>Firmware Version</b>	Version 1.0 Release 21

---

**WAN Port**

<b>MAC Address</b>	00-c0-02-f1-14-a2
<b>IP Address</b>	10.1.1.222
<b>DHCP</b>	DHCP Client
<b>IP Subnet Mask</b>	255.255.255.0
<b>Domain Name Server</b>	10.1.1.6 10.1.1.7

---

**LAN Port**

<b>MAC Address</b>	00-c0-02-f1-14-a1
<b>IP Address</b>	192.168.0.1
<b>DHCP</b>	ON
<b>IP Subnet Mask</b>	255.255.255.0

---

**Figure 8-1. System Status screen**

This screen shows the following parameters:

**Table 8-1. Menu 3.2 - System 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 MAC Address IP Address DHCP IP Subnet Mask Domain Name Servers (DNS)	These parameters apply to the Internet (WAN) port of the firewall. This field displays the Ethernet MAC address being used by the Internet (WAN) port of the firewall. 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. 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 This field displays the IP Subnet Mask being used by the Internet (WAN) port of the firewall. This field displays the DNS Server IP addresses being used by the firewall. These addresses are usually obtained dynamically from the ISP.
LAN Port MAC Address IP Address IP Subnet Mask DHCP	These parameters apply to the Local (LAN) port of the firewall. This field displays the Ethernet MAC address being used by the Local (LAN) port of the firewall. This field displays the IP address being used by the Local (LAN) port of the firewall. The default is 192.168.0.1 This field displays the IP Subnet Mask being used by the Local (LAN) port of the firewall. The default is 255.255.255.0 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 8-2](#) below:

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Down	0	0	0	0	0	00:00:00
LAN	100/Full	498	498	0	434	503	0:12:15

System up Time : 0:12:31

Poll Interval(s):

**Figure 8-2. Router Statistics screen**

This screen shows the following statistics:.

**Table 8-2. Router Statistics Fields**

Field	Description
Port	The statistics for the WAN (Internet) and LAN (local) 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.

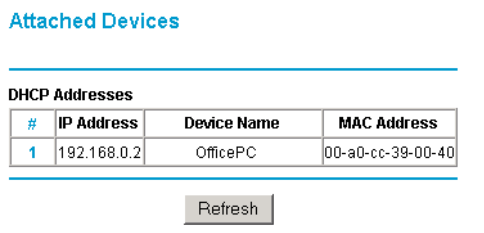
Click on the “Show PPPoE Status” button to display the progress of the PPPoE connection, as shown in [Figure 8-2](#).

Click on the “Show VPN Log” “Show VPN Status” buttons to display VPN connection information, as described in [Chapter 6, “Virtual Private Networking.”](#)

## 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 8-3](#)



The screenshot shows a web interface titled "Attached Devices". Below the title is a table with the heading "DHCP Addresses". The table has four columns: "#", "IP Address", "Device Name", and "MAC Address". There is one row of data with the following values: "# 1", "IP Address 192.168.0.2", "Device Name OfficePC", and "MAC Address 00-a0-cc-39-00-40". Below the table is a "Refresh" button.

#	IP Address	Device Name	MAC Address
1	192.168.0.2	OfficePC	00-a0-cc-39-00-40

Refresh

**Figure 8-3.** Attached Devices menu

For each device, the table shows the IP address, NetBIOS Host Name (if available), and 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.

## Changing the Administration Password

---

You can use the Set Password menu to change the firewall administrator's password for accessing the Settings pages. (Note that this is NOT your ISP account password).

The default password for the firewall’s Web Configuration Manager is **password**. NETGEAR recommends that you change this password to a more 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.

From the Main Menu of the browser interface, under the Maintenance heading, select Set Password to bring up the menu shown in [Figure 8-4](#).

**New Password**

---

Old Password	<input type="text"/>
New Password	<input type="text"/>
Repeat New Password	<input type="text"/>

---

Administrator login times out  
after idle for  minutes.

---

**Figure 8-4. Set Password menu**

To change the password, first enter the old password, and then enter the new password twice. Click Apply.

After changing the password, you may be required to log in again to continue the configuration. If you have backed up the firewall settings previously, you should do a new backup so that the saved settings file includes the new password.

For security, the administrator's login to the firewall configuration will timeout after a period of inactivity. To change the login timeout period:

1. Type the value in 'Administrator login times out' field. The suggested default value is 5 minutes.
2. Click Apply to save your changes or click Cancel to keep the current period.

## Configuration File Settings Management

---

The configuration settings of the FR114P Firewall are stored within the firewall in a configuration file. This file can be saved (backed up) to a user's PC, retrieved (restored) from the user's PC, or cleared to factory default settings.

From the Main Menu of the browser interface, under the Maintenance heading, select the Settings Backup heading to bring up the menu shown in [Figure 8-5](#).

**Settings Backup**

---

Save a copy of current settings

---

Restore saved settings from file

---

Revert to factory default settings

---

**Figure 8-5. Settings Backup menu**

Three options are available, and are described in the following sections.

## Restore and Backup the Configuration

The Restore and Backup options in the Settings Backup menu allow you to save and retrieve a file containing your firewall's configuration settings.

To save your settings, select the Backup tab. Click the Backup button. Your browser will extract the configuration file from the firewall and will prompt you for a location on your PC to store the file. You can give the file a meaningful name at this time, such as pacbell.cfg.

To restore your settings from a saved configuration file, enter the full path to the file on your PC or click the Browse button to browse to the file. When you have located it, click the Restore button to send the file to the firewall. The firewall will then reboot automatically.

## Erase the Configuration

It is sometimes desirable to restore the firewall to a known blank condition. This can be done by using the Erase function, which will restore all factory settings. After an erase, the firewall's password will be **password**, the LAN IP address will be 192.168.0.1, and the firewall's DHCP client will be enabled.

To erase the configuration, click the Erase button.

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 10-8](#).

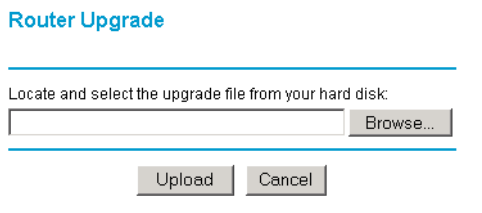
## Router Upgrade

---

The software of the FR114P 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 sending it to the firewall. The upgrade file can be sent to the firewall using your browser.

**Note:** The Web browser used to upload new firmware into the firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 4.0 or above.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown in [Figure 8-6](#).



Router Upgrade

---

Locate and select the upgrade file from your hard disk:

---

**Figure 8-6. Router Upgrade menu**

To upload new firmware:

1. Download and unzip the new software file from NETGEAR.
2. In the Router Upgrade menu, click the Browse button and browse to the location of the binary (.BIN or .IMG) upgrade file
3. 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 reset the firewall to factory defaults and reconfigure it after upgrading.

## Diagnostics

---

The NETGEAR ProSafe Firewall contains several tools to assist in diagnosing conditions on your network. From the Main Menu of the browser interface, under Maintenance, select Diagnostics to view the Diagnostics screen, shown in [Figure 8-7](#):

The screenshot shows the Diagnostics menu with the following sections:

- Diagnostics** (Section Header)
- Ping an IP address**: A form with four input boxes for IP address and a "Ping" button.
- Perform a DNS Lookup**: A form with an "Internet Name" input box containing "www.netgear.com", a "Lookup" button, and the resulting "IP address" (216.136.206.110) and "DNS Server" (10.1.1.6, 10.1.1.7) displayed below.
- Display the Routing Table**: A "Display" button.
- Reboot the Router**: A "Reboot" button.

**Figure 8-7. Diagnostics menu**

### Ping an IP Address

This function sends an echo request packet to the designated device and displays the response. Enter the IP address of the device and click the Ping button. A window will open to display the results.

### Perform a DNS Lookup

This function will contact your Domain Name Service (DNS) server to request the IP address that corresponds to the Internet name you have entered. Enter a fully qualified domain name, such as `www.netgear.com`, then click the Lookup button. The resulting IP address will be shown below the Lookup button. The IP addresses of your DNS servers also appear in this section.

## **Display the Routing Table**

This button will open a new window showing the table of routes that the firewall will use to determine where to send packets. Your LAN and WAN subnets will be shown, along with any Static Routes that you have defined.

## **Reboot the Router**

This button will force a reboot of the firewall.





# Chapter 9

## Advanced Configuration

This chapter describes how to configure the advanced features of your FR114P, FR114W and FM114P Cable/DSL ProSafe Firewalls. These features can be found under the Advanced heading in the Main Menu of the browser interface.

### 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.

From the Main Menu of the browser interface, under Advanced, click on Dynamic DNS to view the Dynamic DNS menu shown in [Figure 9-1](#):

**Dynamic DNS**

---

Use a dynamic DNS service

---

Select Service Provider

Service Provider

Host Name

User Name

Password

---

Use wildcards

---

**Figure 9-1. Dynamic DNS menu**

To configure Dynamic DNS:

1. 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](http://www.dyndns.org).
2. Select the Use a dynamic DNS service check box.
3. Select the name of your dynamic DNS Service Provider.
4. Type the Host Name that your dynamic DNS service provider gave you.  
The dynamic DNS service provider may call this the domain name.
5. Type the User Name for your dynamic DNS account.
6. Type the Password (or key) for your dynamic DNS account.
7. 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`

8. 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.

## LAN IP Setup

The LAN IP Setup menu allows configuration of LAN IP services such as DHCP and RIP. From the Main Menu of the browser interface, under Advanced, click on LAN IP Setup to view the LAN IP Setup menu, shown in [Figure 9-2](#)

**LAN IP Setup**

---

**LAN TCP/IP Setup**

IP Address  .  .  .

IP Subnet Mask  .  .  .

RIP Direction

RIP Version

---

**MTU Size**

Default (1500)  Custom

---

Use router as DHCP server

Starting IP Address  .  .  .

Ending IP Address  .  .  .

---

**Reserved IP Table**

#	IP Address	Mac Address	Device Name
1	192.168.0.11	112233445566	ftp_server

---

**Figure 9-2. LAN IP Setup Menu**

## 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 IP 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 (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)

## 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.

## 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.

From the Main Menu of the browser interface, under Advanced, click on Static Routes to view the Static Routes menu, shown in [Figure 9-3](#).

Static Routes

#	Name	Destination	Gateway	Metric	Active	Private
---	------	-------------	---------	--------	--------	---------

**Figure 9-3. Static Routes Summary Table**

To add or edit a Static Route, click the Add or Edit button to open the Edit Menu, shown in [Figure 9-4](#).

Static Routes

Route Name

Active  Private

Destination IP Address ...

IP Subnet Mask ...

Gateway IP Address ...

Metric

**Figure 9-4. Static Route Entry and Edit Menu**

3. Type a route name for this static route in the Route Name box under the table. (This is for identification purpose only.)
4. Select Active to make this route effective.
5. Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP.
6. Type the Destination IP Address of the final destination network.
7. Type the IP Subnet Mask for this destination network.  
If the destination is a single host, type 255.255.255.255.
8. Type the Gateway IP Address that will be used to reach the destination network.

- If the network is reached through another router on the same LAN segment as the firewall, type that router's LAN IP address.
  - If the network is another IP subnet located on your physical LAN, type your firewall's LAN IP address.
9. Type a number between 2 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 2.
10. Click Apply to have the static route entered into the table.

## 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 9-4](#).

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.
- Private is selected only as a precautionary security measure in case RIP is activated.



## 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 configuration 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.

To configure your firewall for Remote Management:

1. Select the Allow Remote Management check box.
2. 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.
3. 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.

4. 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`



---

# Chapter 10

## Troubleshooting

This chapter gives information about troubleshooting your FR114P, FR114W and FM114P Cable/DSL ProSafe Firewalls. For the common problems listed, go to the section indicated.

- Is the firewall on?
  - Go to [“Basic Functioning“ on page 10-1.](#)
- Have I connected the firewall correctly?
  - Go to [“Troubleshooting the Web Configuration Interface“ on page 10-4.](#)
- I can’t access the firewall’s configuration with my browser.
  - Go to [“Troubleshooting the ISP Connection“ on page 10-5.](#)
- I’ve configured the firewall but I can’t access the Internet.
  - Go to [“Restoring the Default Configuration and Password“ on page 10-8.](#)
- 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 10-8.](#)

### Basic Functioning

---

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 10-8](#).

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 3-5](#) or [“Verifying TCP/IP Properties \(Macintosh\)“ on page 3-8](#) to find your PC's IP address. Follow the instructions in [Chapter 3](#) 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 10-8](#).
- 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](http://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 [“Manual Configuration” on page 4-8](#).

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 addresses) 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 3-5](#). 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 3-5](#).

## 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 very easy by using the ping utility in 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 10-2.
  - 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 3-5.
- 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 [“Manual Configuration” on page 4-8](#).

## 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 [“Erase the Configuration” on page 8-6](#)).
- 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.

1. Press and hold the Default Reset button until the Test LED turns on (about 10 seconds).
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 FR114P 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 FR114P, FR114W and FM114P Cable/DSL ProSafe Firewalls.

### 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 @ 0.8A output, 20W maximum

### Physical Specifications

Dimensions: 191 by 127 by 35 mm  
7.4 by 5.1 by 1.3 in.  
Weight: 0.8 kg  
1.2 lb.

---

### **Environmental Specifications**

Operating temperature: 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

## Networks, Routing, and Firewall Basics

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

### 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 FR114P, FR114W and FM114P Cable/DSL ProSafe Firewalls 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 FR114P 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](http://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:

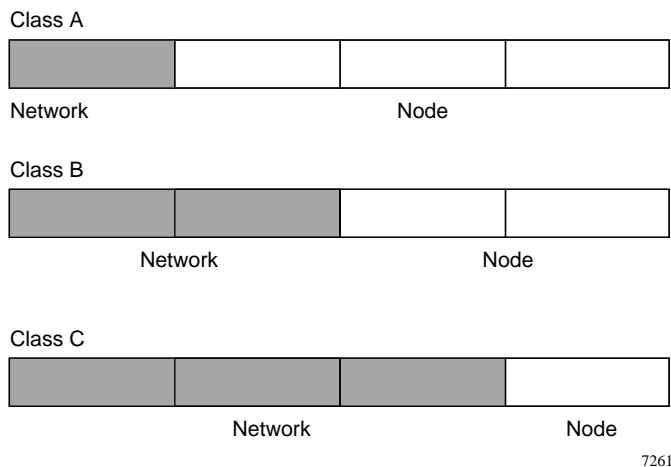
```
195.34.12.7
```

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 B-1. 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 B-2. 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 B-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 B-2. Netmask Formats**

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16
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

**Table B-2. Netmask Formats**

---

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 FR114P Firewall is preconfigured to automatically assign private addresses.

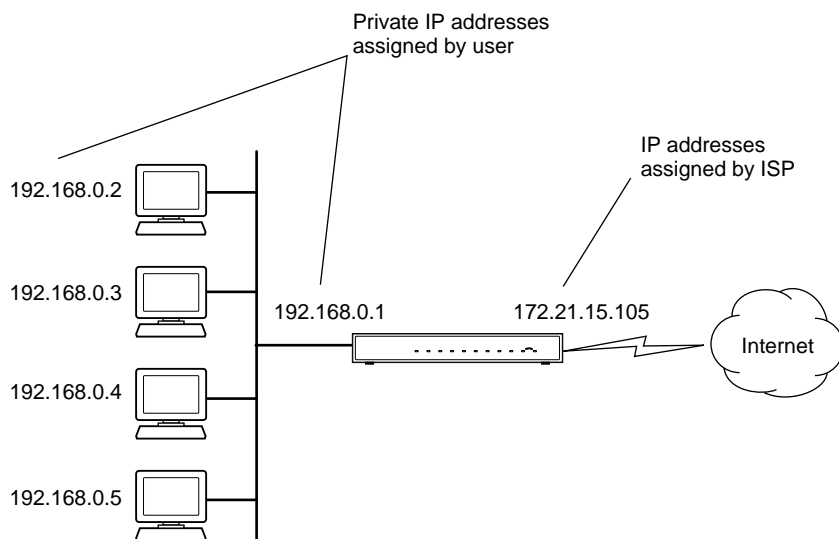
Regardless of your particular situation, do not create an arbitrary IP address; always follow the guidelines explained here. For more information about address assignment, refer to RFC 1597, *Address Allocation for Private Internets*, and RFC 1466, *Guidelines for Management of IP Address Space*. The Internet Engineering Task Force (IETF) publishes RFCs on its Web site at [www.ietf.org](http://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 FR114P 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 B-3. 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.

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.

## 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 FR114P Firewall has the capacity to act as a DHCP server.

The FR114P 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.

## **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 FR114W Wireless-Ready Firewall and FM114P Wireless Firewall with Print Server conform 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 B-3](#):

**Table B-3. 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 as described in [Table B-4](#).

**Table B-4. 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.

# Glossary

<b>10BASE-T</b>	IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.
<b>100BASE-Tx</b>	IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.
<b>802.11b</b>	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.
<b>Denial of Service attack</b>	DoS. A hacker attack designed to prevent your computer or network from operating or communicating.
<b>DHCP</b>	<i>See</i> Dynamic Host Configuration Protocol.
<b>DNS</b>	<i>See</i> Domain Name Server.
<b>domain name</b>	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.
<b>Domain Name Server</b>	A Domain Name Server (DNS) resolves descriptive names of network resources (such as www.NETGEAR.com) to numeric IP addresses.
<b>Dynamic Host Configuration Protocol</b>	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.
<b>ESSID</b>	The Extended Service Set Identification (ESS ID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.
<b>Gateway</b>	A local device, usually a router, that connects hosts on a local network to other networks.

<b>IETF</b>	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 <a href="http://www.ietf.org">www.ietf.org</a> .
<b>IKE</b>	Internet Key Exchange. An automated method for exchanging and managing encryption keys between two VPN devices.
<b>IP</b>	Internet Protocol. The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.
<b>IP Address</b>	A four-byte 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).
<b>IPSec</b>	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.
<b>ISP</b>	Internet service provider.
<b>LAN</b>	<i>See</i> local area network.
<b>local area network</b>	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.
<b>MAC address</b>	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.
<b>Mbps</b>	Megabits per second.
<b>MSB</b>	<i>See</i> Most Significant Bit or Most Significant Byte.
<b>MRU</b>	<i>See</i> Maximum Receive Unit.
<b>Maximum Receive Unit</b>	The size in bytes of the largest packet that can be sent or received.
<b>Most Significant Bit or Most Significant Byte</b>	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.



<b>NAT</b>	<i>See</i> Network Address Translation.
<b>netmask</b>	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.
<b>Network Address Translation</b>	A technique by which several hosts share a single IP address for access to the Internet.
<b>packet</b>	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.
<b>PPP</b>	<i>See</i> Point-to-Point Protocol.
<b>PPP over Ethernet</b>	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.
<b>PPTP</b>	Point-to-Point Tunneling Protocol. A method for establishing a virtual private network (VPN) by embedding Microsoft's network protocol into Internet packets.
<b>PSTN</b>	Public Switched Telephone Network.
<b>Point-to-Point Protocol</b>	PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.
<b>RFC</b>	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 <a href="http://www.ietf.org">www.ietf.org</a> .
<b>RIP</b>	<i>See</i> Routing Information Protocol.
<b>router</b>	A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.
<b>Routing Information Protocol</b>	A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.
<b>SSID</b>	Service Set Identification. A thirty-two character (maximum) alphanumeric key identifying the wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID.

<b>subnet mask</b>	<i>See</i> netmask.
<b>UTP</b>	Unshielded twisted pair. The cable used by 10BASE-T and 100BASE-Tx Ethernet networks.
<b>VPN</b>	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.
<b>WAN</b>	<i>See</i> wide area network.
<b>WEP</b>	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.
<b>wide area network</b>	WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.
<b>Wi-Fi</b>	<i>See</i> 802.11b. A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <a href="http://www.wi-fi.net">http://www.wi-fi.net</a> ), an industry standard group promoting interoperability among 802.11b devices.
<b>Windows Internet Naming Service</b>	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.
<b>WINS</b>	<i>See</i> Windows Internet Naming Service.

## Numerics

802.11b B-12

## A

Account Name 4-5, 4-7, 4-8

Address Resolution Protocol B-9

ad-hoc mode B-12, B-13

antenna orientation 2-6

## B

backup configuration 8-6

BSSID B-13

## C

Cabling B-15

Cat5 cable 2-2, 2-5, B-16

Channel B-14

Channel Number 6-3

configuration

    automatic by DHCP 1-3

    backup 8-6

    erasing 8-6

    router, initial 4-1

connections

    verifying 2-7

content filtering 1-3, 5-1

conventions

    typography xv

crossover cable 2-5, 10-3, B-16

customer support iii

## D

date and time 10-8

Daylight Savings Time 5-17, 10-9

Default Key 6-5

default password (is password) 8-4

default reset button 10-8

Denial of Service (DoS) protection 1-2

denial of service attack B-11

DHCP 1-3, 9-5, B-10

DHCP Client ID 3-7

DHCP Setup field, Ethernet Setup menu 8-2

diagnostics 8-8

DMZ Server 5-12

DNS Lookup 8-8

DNS Proxy 1-4

DNS server 3-10, 3-11, 4-5, 4-6, 4-8, 4-9

DNS, dynamic 9-1

domain 3-10

Domain Name 4-5, 4-7, 4-8

domain name server (DNS) B-9

DoS attack B-11

Dynamic DNS 1-4, 9-1

## E

EnterNet 3-9

EPROM, for firmware upgrade 1-5

erase configuration 8-6

ESSID 2-6, B-13

Ethernet 1-3

Ethernet cable B-15

exposed host 5-13

## F

factory settings, restoring 8-6  
features 1-1  
firewall features 1-2  
FLASH memory 8-7  
front panel 2-3

## G

gateway address 3-10, 3-11

## H

host name 4-5, 4-7, 4-8

## I

IANA

contacting B-2

IETF xvi

Web site address B-7

inbound rules 5-8

infrastructure mode B-12, B-13

installation 1-4

Internet account

address information 3-9

establishing 3-8

IP addresses 3-10, 3-11

and NAT B-8

and the Internet B-2

assigning xvii, B-2

auto-generated 10-4

private B-7

translating xvii

IP configuration by DHCP B-10

IP networking

for Macintosh 3-6

for Windows 3-2, 3-5

## L

LAN IP Setup Menu 9-3

LEDs

description 2-3

troubleshooting 10-2

log

sending 5-18

LPD/LPR Printing 7-1

## M

MAC address 10-8, B-9

spoofing 4-6, 4-9, 10-6

MAC address filter 6-6

Macintosh 3-10

configuring for IP networking 3-6

DHCP Client ID 3-7

network printing 7-9

Obtaining ISP Configuration Information 3-11

masquerading 3-9

metric 9-8

MTU 9-5

multicasting 9-4

## N

NAT 3-9

NAT. *See* Network Address Translation

NETGEAR

contacting xvi

netmask

translation table B-6

Network Address Translation 1-3, 3-9, B-8

Network Time Protocol 5-17, 10-8

NTP 5-17, 10-8

## O

Open System authentication B-13

order of precedence 5-12

outbound rules 5-11

## P

package contents 2-1

Passphrase 6-5

- password
  - restoring 10-8
- PC, using to configure 3-11
- ping 5-13, 8-8
- placement 6-6
- port filtering 5-11
- port forwarding 5-8
- port forwarding behind NAT B-9
- port numbers 5-14
- PPP over Ethernet 1-4, 3-9
- PPPoE 1-4, 3-9, 4-7
- Primary DNS Server 4-5, 4-6, 4-8, 4-9
- protocols
  - Address Resolution B-9
  - DHCP 1-3, B-10
  - Routing Information 1-3, B-2
  - support 1-3
  - TCP/IP 1-3
- PTP Driver 7-1
- publications, related xvi

## R

- range 6-6
- rear panel 2-4
- reboot 8-9
- Regulatory Domain 6-2
- remote management 9-9
- requirements
  - access device 2-2
  - hardware 2-2
- reserved IP addresses 9-6
- reset button, clearing config 10-8
- restore factory settings 8-6
- RFC
  - 1466 xvii, B-7
  - 1597 xvii, B-7
  - 1631 xvii, B-8
  - finding B-7
- RIP (Router Information Protocol) 9-4
- router concepts B-1

- Routing Information Protocol 1-3, B-2
- routing table 8-9
- rules
  - inbound 5-8
  - order of precedence 5-12
  - outbound 5-11

## S

- Secondary DNS Server 4-5, 4-6, 4-8, 4-9
- service blocking 5-11
- service numbers 5-14
- Setup Wizard 4-1
- Shared Key authentication B-13
- SMTP 5-18
- spoof MAC address 10-6
- SSID 2-6, 6-1, 6-2, B-13
- stateful packet inspection 1-2, 5-1, B-11
- Static Routes 9-6
- Station Name 6-2
- subnet addressing B-5
- subnet mask 3-10, 3-11, B-5

## T

- TCP/IP
  - configuring 3-1
  - network, troubleshooting 10-6
- TCP/IP properties
  - verifying for Macintosh 3-8
  - verifying for Windows 3-5, 3-6
- technical support xvi
- time of day 10-8
- Time Zone 5-17
- timeout, administrator login 8-5
- troubleshooting 10-1
- Trusted Host 5-6
- typographical conventions xv

## U

- upgrading the FR114W 2-6

Uplink switch B-16

USB 3-8

## **W**

WEP 6-4, B-13

WEP, Keys 6-4

Wi-Fi B-12

Windows, configuring for IP routing 3-2, 3-5

winipcfg utility 3-5

WinPOET 3-9

Wired Equivalent Privacy. *See* WEP

Wireless Ethernet B-12

World Wide Web iii