

Reference Manual for the ProSafe Dual Band Wireless VPN Firewall FWAG114

NETGEAR

NETGEAR, Inc.
4500 Great America Parkway
Santa Clara, CA 95054 USA

SM-FWAG114NA-0
Version 1.0
June 2003

Trademarks

NETGEAR is a trademark 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.

FCC Caution

1. FCC RF Radiation Exposure Statement: The equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
2. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. 3. Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.

EN 55 022 Declaration of Conformance

This is to certify that the ProSafe Dual Band Wireless VPN Firewall FWAG114 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 ProSafe Dual Band Wireless VPN Firewall FWAG114 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 ProSafe Dual Band Wireless VPN Firewall FWAG114 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.

Contents

Chapter 1

About This Manual

Audience	1-1
Typographical Conventions	1-1
Special Message Formats	1-1
Features of the HTML Version of this Manual	1-2

Chapter 2

Introduction

Key Features of the VPN Firewall	2-1
802.11g and 802.11b Wireless Networking	2-2
A Powerful, True Firewall with Content Filtering	2-2
Security	2-3
Autosensing Ethernet Connections with Auto Uplink	2-3
Extensive Protocol Support	2-3
Easy Installation and Management	2-4
Maintenance and Support	2-5
Package Contents	2-5
The FWAG114's Front Panel	2-6
The FWAG114's Rear Panel	2-7

Chapter 3

Connecting the FWAG114 to the Internet

What You Will Need Before You Begin	3-1
Cabling and Computer Hardware Requirements	3-1
Computer Network Configuration Requirements	3-1
Internet Configuration Requirements	3-2
Where Do I Get the Internet Configuration Parameters?	3-2
Record Your Internet Connection Information	3-3
Connecting the ProSafe Dual Band Wireless VPN Firewall FWAG114 to Your LAN	3-4
PPPoE Wizard-Detected Option	3-8

Dynamic IP Wizard-Detected Option	3-10
Fixed IP Account Wizard-Detected Option	3-11
Manually Configuring Your Internet Connection	3-12

Chapter 4

Wireless Configuration

Observe Performance, Placement, and Range Guidelines	4-1
Implement Appropriate Wireless Security	4-2
Understanding Wireless Settings	4-4
Common Wireless Settings	4-5
Understanding WEP Authentication and Encryption	4-6
Authentication Type	4-6
WEP	4-7
Default Factory Settings	4-7
Before You Change the SSID and WEP Settings	4-8
How to Set Up and Test Basic Wireless Connectivity	4-9
How to Restrict Wireless Access by MAC Address	4-10
How to Configure WEP	4-12

Chapter 5

Firewall Protection and Content Filtering

Firewall Protection and Content Filtering Overview	5-1
Block Sites	5-2
Using Rules to Block or Allow Specific Kinds of Traffic	5-3
Inbound Rules (Port Forwarding)	5-5
Inbound Rule Example: A Local Public Web Server	5-5
Inbound Rule Example: Allowing Videoconference from Restricted Addresses	5-6
Considerations for Inbound Rules	5-6
Outbound Rules (Service Blocking)	5-7
Following is an application example of outbound rules:	5-7
Outbound Rule Example: Blocking Instant Messenger	5-7
Order of Precedence for Rules	5-8
Default DMZ Server	5-8
Respond to Ping on Internet WAN Port	5-9
Services	5-10
Using a Schedule to Block or Allow Specific Traffic	5-12
Time Zone	5-13

Getting E-Mail Notifications of Event Logs and Alerts	5-14
Viewing Logs of Web Access or Attempted Web Access	5-16
Syslog	5-17
Chapter 6	
Maintenance	
Viewing VPN Firewall Status Information	5-1
Viewing a List of Attached Devices	5-5
Upgrading the Router Software	5-5
Configuration File Management	5-6
Restoring and Backing Up the Configuration	5-7
Erasing the Configuration	5-8
Changing the Administrator Password	5-8
Chapter 7	
Virtual Private Networking	
Overview of FWAG114 Policy-Based VPN Configuration	6-1
Using Policies to Manage VPN Traffic	6-2
Using Automatic Key Management	6-2
IKE Policies' Automatic Key and Authentication Management	6-3
VPN Policy Configuration for Auto Key Negotiation	6-6
VPN Policy Configuration for Manual Key Exchange	6-9
Using Digital Certificates for IKE Auto-Policy Authentication	6-14
Certificate Revocation List (CRL)	6-14
Walk-Through of Configuration Scenarios on the FWAG114	6-15
VPN Consortium Scenario 1:	
Gateway-to-Gateway with Preshared Secrets	6-16
FWAG114 Scenario 1: FWAG114 to Gateway B IKE and VPN Policies	6-17
How to Check VPN Connections	6-20
FWAG114 Scenario 2: FWAG114 to FWAG114 with RSA Certificates	6-22
Chapter 8	
Advanced Configuration	
How to Configure Dynamic DNS	6-1
Using the LAN IP Setup Options	6-3
Configuring LAN TCP/IP Setup Parameters	6-3
Using the Router as a DHCP server	6-4
Using Address Reservation	6-5
Configuring Static Routes	6-6

Enabling Remote Management Access	6-8
Chapter 9	
Troubleshooting	
Basic Functioning	7-1
Power LED Not On	7-1
LEDs Never Turn Off	7-2
LAN or Internet Port LEDs Not On	7-2
Troubleshooting the Web Configuration Interface	7-3
Troubleshooting the ISP Connection	7-4
Troubleshooting a TCP/IP Network Using a Ping Utility	7-5
Testing the LAN Path to Your Router	7-5
Testing the Path from Your PC to a Remote Device	7-6
Restoring the Default Configuration and Password	7-7
Problems with Date and Time	7-7
Appendix A	
Technical Specifications	
Appendix B	
Network, Routing, Firewall, and Basics	
Related Publications	B-1
Basic Router Concepts	B-1
What is a Router?	B-2
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
Related Documents	B-9
Domain Name Server	B-10
IP Configuration by DHCP	B-10
Internet Security and Firewalls	B-10
What is a Firewall?	B-11
Stateful Packet Inspection	B-11
Denial of Service Attack	B-11

Ethernet Cabling	B-12
Uplink Switches, Crossover Cables, and MDI/MDIX Switching	B-12
Cable Quality	B-13

Appendix C

Preparing Your Network

Preparing Your Computers for TCP/IP Networking	C-1
Configuring Windows 95, 98, and Me for TCP/IP Networking	C-2
Install or Verify Windows Networking Components	C-2
Enabling DHCP to Automatically Configure TCP/IP Settings	C-4
Selecting Windows' Internet Access Method	C-6
Verifying TCP/IP Properties	C-6
Configuring Windows NT4, 2000 or XP for IP Networking	C-7
Install or Verify Windows Networking Components	C-7
Enabling DHCP to Automatically Configure TCP/IP Settings	C-8
DHCP Configuration of TCP/IP in Windows XP	C-8
DHCP Configuration of TCP/IP in Windows 2000	C-10
DHCP Configuration of TCP/IP in Windows NT4	C-13
Verifying TCP/IP Properties for Windows XP, 2000, and NT4	C-15
Configuring the Macintosh for TCP/IP Networking	C-16
MacOS 8.6 or 9.x	C-16
MacOS X	C-16
Verifying TCP/IP Properties for Macintosh Computers	C-17
Verifying the Readiness of Your Internet Account	C-18
Are Login Protocols Used?	C-18
What Is Your Configuration Information?	C-18
Obtaining ISP Configuration Information for Windows Computers	C-19
Obtaining ISP Configuration Information for Macintosh Computers	C-20
Restarting the Network	C-21

Appendix D

Wireless Networking Basics

Wireless Networking Overview	D-1
Infrastructure Mode	D-2
Ad Hoc Mode (Peer-to-Peer Workgroup)	D-2
Network Name: Extended Service Set Identification (ESSID)	D-2
Authentication and WEP Data Encryption	D-3

802.11 Authentication	D-3
Open System Authentication	D-4
Shared Key Authentication	D-4
Overview of WEP Parameters	D-5
Key Size	D-6
WEP Configuration Options	D-7
Wireless Channels	D-7
802/11b/g Wireless Channels	D-8
802/11a Legal Power Output and Wireless Channels	D-9

Appendix E

Virtual Private Networking

What is a VPN?	E-1
What Is IPsec and How Does It Work?	E-2
IPsec Security Features	E-2
IPsec Components	E-3
Encapsulating Security Payload (ESP)	E-3
Authentication Header (AH)	E-4
IKE Security Association	E-5
Mode	E-5
Key Management	E-6
Understand the Process Before You Begin	E-7
VPN Process Overview	E-7
Network Interfaces and Addresses	E-8
Interface Addressing	E-8
Firewalls	E-9
Setting Up a VPN Tunnel Between Gateways	E-9
VPNC IKE Security Parameters	E-11
VPNC IKE Phase I Parameters	E-11
VPNC IKE Phase II Parameters	E-12
Testing and Troubleshooting	E-12
Additional Reading	E-12

Glossary

List of Glossary Terms	G-1
------------------------------	-----

Index

Chapter 1

About This Manual

Congratulations on your purchase of the NETGEAR® ProSafe Dual Band Wireless VPN Firewall FWAG114. The FWAG114 wireless firewall provides connection for multiple personal computers (PCs) to the Internet through an external broadband access device (such as a cable modem or DSL modem) that is normally intended for use by a single PC.

Audience

This reference manual assumes that the reader has basic to intermediate computer and Internet skills. However, basic computer network, Internet, firewall, and VPN technologies tutorial information is provided in the Appendices and on the Netgear website.

Typographical Conventions

This guide uses the following typographical conventions:

Table 1. Typographical conventions

<i>italics</i>	Emphasis.
bold times roman	User input.
[Enter]	Named keys in text are shown enclosed in square brackets. The notation [Enter] is used for the Enter key and the Return key.
SMALL CAPS	DOS file and directory names.

Special Message Formats

This guide uses the following formats to highlight special messages:

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

Features of the HTML Version of this Manual

The HTML version of this manual includes these features.

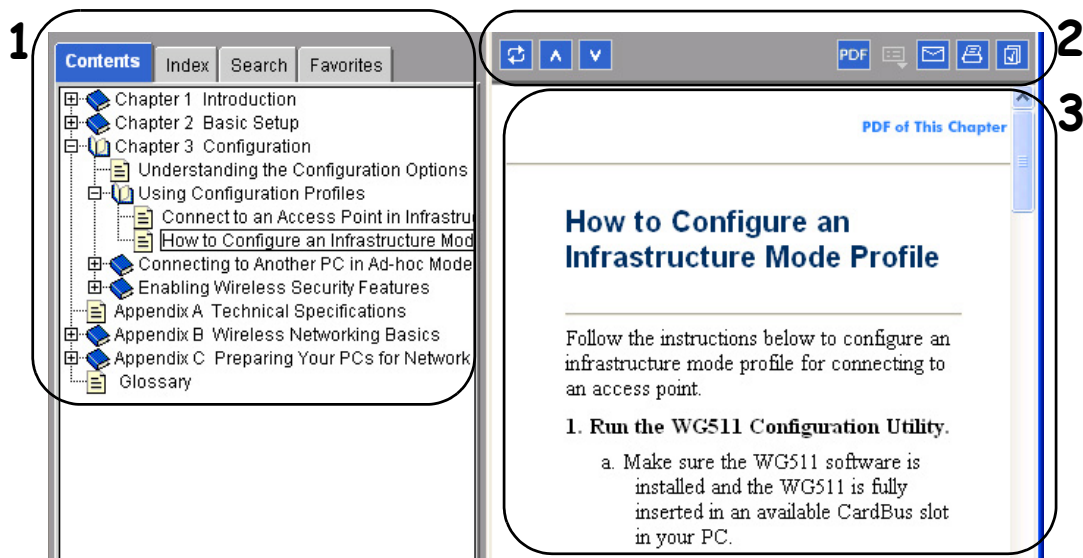


Figure Preface -2: HTML version of this manual

- 1. Left pane.** Use the left pane to view the Contents, Index, Search, and Favorites tabs.

To view the HTML version of the manual, you must have a version 4 or later browser with Java or JavaScript enabled. To use the Favorites feature, your browser must be set to accept cookies. You can record a list of favorite pages in the manual for easy later retrieval.

- 2. Toolbar buttons.** Use the toolbar buttons across the top to navigate, print pages, and more.
 - The *Show in Contents* button locates the currently displayed topic in the Contents tab.
 - *Previous/Next* buttons display the topic that precedes or follows the current topic.
 - The *PDF* button links to a PDF version of the full manual.
 - The *E-mail* button enables you to send feedback by e-mail to Netgear support.
 - The *Print* button prints the currently displayed topic. Using this button when a step-by-step procedure is displayed will send the entire procedure to your printer--you do not have to worry about specifying the correct range of pages.
 - The *Bookmark* button bookmarks the currently displayed page in your browser.
- 3. Right pane.** Use the right pane to view the contents of the manual. Also, each page of the manual includes a “PDF of This Chapter” link at the top right which links to a PDF file containing just the currently selected chapter of the manual.

Chapter 2

Introduction

This chapter describes the features of the NETGEAR ProSafe Dual Band Wireless VPN Firewall FWAG114.

Key Features of the VPN Firewall

The ProSafe Dual Band Wireless VPN Firewall FWAG114 with 4-port switch connects your local area network (LAN) to the Internet through an external access device such as a cable modem or DSL modem.

The FWAG114 is a complete security solution that protects your network from attacks and intrusions. Unlike simple Internet sharing routers that rely on Network Address Translation (NAT) for security, the FWAG114 uses Stateful Packet Inspection for Denial of Service attack (DoS) attack protection and intrusion detection. The FWAG114 allows Internet access for up to 253 users. The FWAG114 wireless firewall provides you with multiple Web content filtering options, plus browsing activity reporting and instant alerts -- both via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, Website addresses and address keywords, and share high-speed cable/DSL Internet access for up to 253 personal computers. In addition to NAT, the built-in firewall protects you from hackers.

With minimum setup, you can install and use the router within minutes.

The FWAG114 wireless firewall provides the following features:

- 802.11g and 802.11b standards-based wireless networking.
- Easy, web-based setup for installation and management.
- Content Filtering and Site Blocking Security.
- Built in 4-port 10/100 Mbps Switch.
- Ethernet connection to a WAN device, such as a cable modem or DSL modem.
- Extensive Protocol Support.
- Login capability.
- Front panel LEDs for easy monitoring of status and activity.

- Flash memory for firmware upgrade.

802.11g and 802.11b Wireless Networking

The FWAG114 wireless firewall includes an 802.11b-compliant wireless access point, providing 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.
- 802.11g wireless networking at up to 54 Mbps, which will conform to the 802.11g standard when ratified.
- 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.
- Wireless network name broadcast can be turned off so that only devices that have the network name (SSID) can connect.

A Powerful, True Firewall with Content Filtering

Unlike simple Internet sharing NAT routers, the FWAG114 is a true firewall, using stateful packet inspection to defend against hacker attacks. Its firewall features include:

- DoS protection.
Automatically detects and thwarts 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 FWAG114 will log security events such as blocked incoming traffic, port scans, attacks, and administrator logins. You can configure the router to email the log to you at specified intervals. You can also configure the router to send immediate alert messages to your email address or email pager whenever a significant event occurs.

- With its content filtering feature, the FWAG114 prevents objectionable content from reaching your PCs. The router allows you to control access to Internet content by screening for keywords within Web addresses. You can configure the router to log and report attempts to access objectionable Internet sites.

Security

The FWAG114 wireless firewall is equipped with several features designed to maintain security, as described in this section.

- **PCs Hidden by NAT**
NAT opens a temporary path to the Internet for requests originating from the local network. Requests originating from outside the LAN are discarded, preventing users outside the LAN from finding and directly accessing the PCs on the LAN.
- **Port Forwarding with NAT**
Although NAT prevents Internet locations from directly accessing the PCs on the LAN, the router allows you to direct incoming traffic to specific PCs based on the service port number of the incoming request, or to one designated “DNS” host computer. You can specify forwarding of single ports or ranges of ports.

Autosensing Ethernet Connections with Auto Uplink

With its internal 8-port 10/100 switch, the FWAG114 can connect to either a 10 Mbps standard Ethernet network or a 100 Mbps Fast Ethernet network. Both the LAN and WAN interfaces are autosensing and capable of full-duplex or half-duplex operation.

The router incorporates Auto Uplink™ technology. Each Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a ‘normal’ connection such as to a PC or an ‘uplink’ connection such as to a switch or hub. That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink will accommodate either type of cable to make the right connection.

Extensive Protocol Support

The FWAG114 wireless 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, “Network, Routing, Firewall, and Basics.”](#)

- **IP Address Sharing by NAT**
The FWAG114 wireless 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 NAT, allows the use of an inexpensive single-user ISP account.
- **Automatic Configuration of Attached PCs by DHCP**
The FWAG114 wireless 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 router provides its own address as a DNS server to the attached PCs. The router obtains actual DNS addresses from the ISP during connection setup and forwards DNS requests from the LAN.
- **PPP over Ethernet (PPPoE)**
PPPoE 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 Entersys or WinPOET on your PC.

Easy Installation and Management

You can install, configure, and operate the ProSafe Dual Band Wireless VPN Firewall FWAG114 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 router 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 FWAG114 wireless firewall automatically senses the type of Internet connection, asking you only for the information required for your type of ISP account.
- **Diagnostic functions**
The firewall incorporates built-in diagnostic functions such as Ping, DNS lookup, and remote reboot.

- 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.
- Visual monitoring
The FWAG114 wireless 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 FWAG114 wireless firewall:

- Flash memory for firmware upgrade
- Free technical support seven days a week, twenty-four hours a day

Package Contents

The product package should contain the following items:

- ProSafe Dual Band Wireless VPN Firewall FWAG114.
- AC power adapter.
- Category 5 (Cat 5) Ethernet cable.
- *Resource CD for ProSafe Dual Band Wireless VPN Firewall*, including:
 - This guide.
 - Application Notes and other helpful information.
- Registration and Warranty 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 router for repair.

The FWAG114's Front Panel

The front panel of the FWAG114 wireless firewall contains the status LEDs described below.

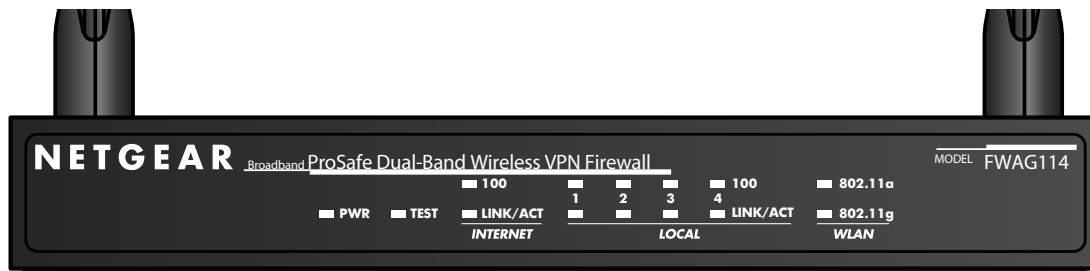


Figure 2-1: FWAG114 Front Panel

You can use some of the LEDs to verify connections. Viewed from left to right, [Table 2-1](#) describes the LEDs on the front panel of the router. These LEDs are green when lit.

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.
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.

The FWAG114's Rear Panel

The rear panel of the FWAG114 wireless firewall contains the port connections listed below.



Figure 1-2: FWAG114 Rear Panel

Viewed from left to right, the rear panel contains the following features:

- Wireless antenna
- AC power adapter outlet
- Factory Default Reset push button
- Internet (WAN) Ethernet port for connecting the router to a cable or DSL modem
- Four LAN Ethernet ports
- Wireless antenna

Chapter 3

Connecting the FWAG114 to the Internet

This chapter describes how to set up the router on your local area network (LAN) and connect to the Internet. You find out how to configure your ProSafe Dual Band Wireless VPN Firewall FWAG114 for Internet access using the Setup Wizard, or how to manually configure your Internet connection.

What You Will Need Before You Begin

You need to prepare these three things before you begin:

1. Have active Internet service such as that provided by a cable or DSL broadband account.
2. Locate the Internet Service Provider (ISP) configuration information for your DSL account.
3. Connect the router to a cable or DSL modem and a computer as explained below.

Cabling and Computer Hardware Requirements

To use the FWAG114 wireless firewall on your network, each computer must have an installed Ethernet Network Interface Card (NIC) and an Ethernet cable. If the computer will connect to your network at 100 Mbps, you must use a Category 5 (CAT5) cable such as the one provided with your router.

Computer Network Configuration Requirements

The FWAG114 includes a built-in Web Configuration Manager. To access the configuration menus on the FWAG114, you must use a Java-enabled web browser program which supports HTTP uploads such as Microsoft Internet Explorer or Netscape Navigator. NETGEAR recommends using Internet Explorer or Netscape Navigator 4.0 or above. Free browser programs are readily available for Windows, Macintosh, or UNIX/Linux.

For the initial connection to the Internet and configuration of your router, you will need to connect a computer to the router which is set to automatically get its TCP/IP configuration from the router via DHCP.

Note: For help with DHCP configuration, please refer to [Appendix C, “Preparing Your Network.”](#)

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

Internet Configuration Requirements

Depending on how your ISP set up your Internet account, you will need one or more of these configuration parameters to connect your router to the Internet:

- Host and Domain Names
- ISP Login Name and Password
- ISP Domain Name Server (DNS) Addresses
- Fixed IP Address which is also known as Static IP Address

Where Do I Get the Internet Configuration Parameters?

There are several ways you can gather the required Internet connection information.

- Your ISP provides all the information needed to connect to the Internet. If you cannot locate this information, you can ask your ISP to provide it or you can try one of the options below.
- If you have a computer already connected using the active Internet access account, you can gather the configuration information from that computer.
 - For Windows 95/98/ME, open the Network control panel, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
 - For Windows 2000/XP, open the Local Area Network Connection, select the TCP/IP entry for the Ethernet adapter, and click Properties. Record all the settings for each tab page.
 - For Macintosh computers, open the TCP/IP or Network control panel. Record all the settings for each section.
- You may also refer to the *FWAG114 Resource CD* for the NETGEAR Router ISP Guide which provides Internet connection information for many ISPs.

Once you locate your Internet configuration parameters, you may want to record them on the page below.

Record Your Internet Connection Information

Print this page. Fill in the configuration parameters from your Internet Service Provider (ISP).

ISP Login Name: The login name and password are case sensitive and must be entered exactly as given by your ISP. For AOL customers, the login name is their primary screen name. Some ISPs use your full e-mail address as the login name. The Service Name is not required by all ISPs. If you connect using a login name and password, then fill in the following:

Login Name: _____ Password: _____

Service Name: _____

Fixed or Static IP Address: If you have a static IP address, record the following information. For example, 169.254.141.148 could be a valid IP address.

Fixed or Static Internet IP Address: _____ . _____ . _____ . _____

Gateway IP Address: _____ . _____ . _____ . _____

Subnet Mask: _____ . _____ . _____ . _____

ISP DNS Server Addresses: If you were given DNS server addresses, fill in the following:

Primary DNS Server IP Address: _____ . _____ . _____ . _____

Secondary DNS Server IP Address: _____ . _____ . _____ . _____

Host and Domain Names: Some ISPs use a specific host or domain name like **CCA7324-A** or **home**. If you haven't been given host or domain names, you can use the following examples as a guide:

- If your main e-mail account with your ISP is **aaa@yyy.com**, then use **aaa** as your host name. Your ISP might call this your account, user, host, computer, or system name.
- If your ISP's mail server is **mail.xxx.yyy.com**, then use **xxx.yyy.com** as the domain name.

ISP Host Name: _____ ISP Domain Name: _____

Connecting the ProSafe Dual Band Wireless VPN Firewall FWAG114 to Your LAN

This section provides instructions for connecting the FWAG114 wireless firewall. Also, the *Resource CD for ProSafe Dual Band Wireless VPN Firewall* included with your router contains an animated Installation Assistant to help you through this procedure.

Procedure: Connecting the VPN Firewall

There are three steps to connecting your router:

1. Connect the router to your network
2. Log in to the router
3. Connect to the Internet

Follow the steps below to connect your router to your network. You can also refer to the Resource CD included with your router which contains an animated Installation Assistant to help you through this procedure.

1. Connect the VPN firewall to your network.

- a. Turn off your computer and Cable or DSL Modem.
- b. Disconnect the Ethernet cable (A) from your computer which connects to your cable or DSL modem.

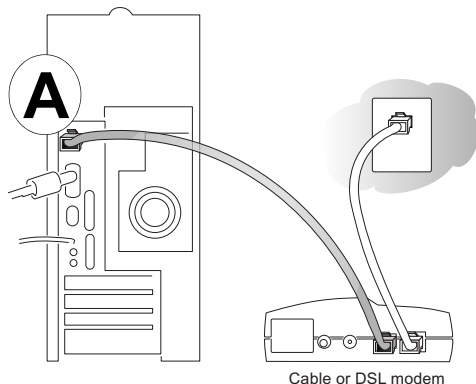


Figure 3-1: Disconnect the cable or DSL Modem

- c. Connect the Ethernet cable from your cable or DSL modem to the Internet port (A) on the FWAG114.

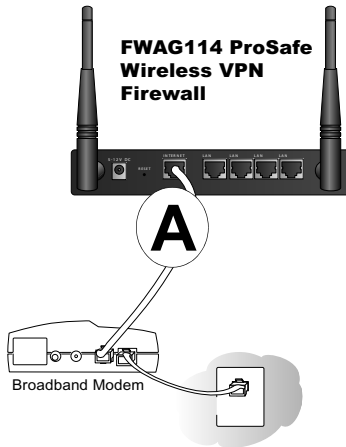


Figure 3-2: Connect the cable or DSL Modem to the router

- d. Connect the Ethernet cable which came with the router from a Local port on the router (B) to your computer.

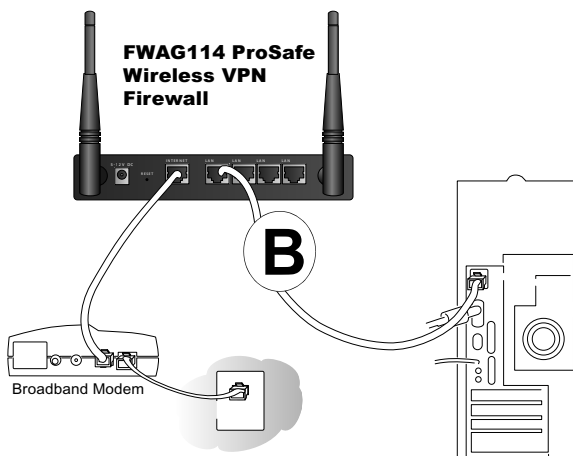


Figure 3-3: Connect the computers on your network to the router

Note: The FWAG114 wireless firewall incorporates Auto Uplink™ technology. Each LOCAL Ethernet port will automatically sense if the cable should have a normal connection or an uplink connection. This feature eliminates the need to worry about crossover cables because Auto Uplink will make the right connection either type of cable.

- e. Now, turn on your computer. If software usually logs you in to your Internet connection, do not run that software or cancel it if it starts automatically.
- f. Verify the following:
 - When you turn the router on, the power light goes on.
 - The router's local lights are lit for any computers that are connected to it.
 - The router's Internet light is lit, indicating a link has been established to the cable or DSL modem.

Note: For wireless placement and range guidelines, and wireless configuration instructions, please see [Chapter 4, "Wireless Configuration."](#)

2. Log in to the VPN firewall .

Note: To connect to the router, your computer needs to be configured to obtain an IP address automatically via DHCP. If you need instructions on how to do this, please refer to [Appendix C, "Preparing Your Network."](#)

- a. Connect to the router by typing <http://192.168.0.1> in the address field of Internet Explorer or Netscape® Navigator.

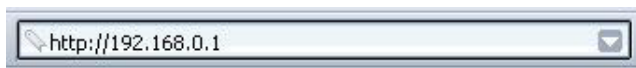


Figure 3-4: Log in to the router

- b. For security reasons, the router has its own user name and password. When prompted, enter **admin** for the router user name and **password** for the router password, both in lower case letters. The router user name and password are not the same as any user name or password you may use to log in to your Internet connection.

A login window shown below opens:

Figure 3-5: Login window

3. Connect to the Internet

Figure 3-6: Setup Wizard

- a. You are now connected to the router. If you do not see the menu above, click the Setup Wizard link on the upper left of the main menu.
- b. Click Next and follow the steps in the Setup Wizard for inputting the configuration parameters from your ISP to connect to the Internet.

Note: If you choose not to use the Setup Wizard, you can manually configure your Internet connection settings by following the procedure [“Manually Configuring Your Internet Connection” on page 3-12.](#)

Unless your ISP automatically assigns your configuration automatically via DHCP, you will need the configuration parameters from your ISP as you recorded them previously in [“Record Your Internet Connection Information” on page 3-3.](#)

- c. When the router successfully detects an active Internet service, the router's Internet LED goes on. The Setup Wizard reports which connection type it discovered, and displays the appropriate configuration menu. If the Setup Wizard finds no connection, you will be prompted to check the physical connection between your router and the cable or DSL line.
- d. The Setup Wizard will report the type of connection it finds. The options are:
 - Connections which require a login using protocols such as PPPoE, DHCP, or Static IP broadband connections.
 - Connections which use dynamic IP address assignment.
 - Connections which use fixed IP address assignment.

The procedures for filling in the configuration menu for each type of connection follow below.

PPPoE Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses PPPoE, you will see this menu:

Internet Service Provider Name: Other (PPPoE) ▼

Account Name: FWAG114

Domain Name:

Login: guest

Password:

Idle Timeout: 5 Minutes

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 Computer's MAC

☐ Use This MAC Address:

Apply Cancel Test

Figure 3-7: Setup Wizard menu for PPPoE accounts

- Enter the Account Name, Domain Name, Login, and Password as provided by your ISP. These fields are case sensitive. The router will try to discover the domain automatically if you leave the Domain Name blank. Otherwise, you may need to enter it manually.
- To change the login timeout, enter a new value in minutes. This determines how long the router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a timeout value of zero means never log out.

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

- If you know that your ISP does not automatically transmit DNS addresses to the router 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.

Note: If you enter DNS addresses, restart your computers so that these settings take effect.

- If your ISP requires a specific MAC address for the connection, you may need to fill a MAC address. Usually, it is not necessary to change the MAC address setting.
- Click Apply to save your settings.
- Click Test to verify that your Internet connection works. If the NETGEAR website does not appear within one minute, refer to [Chapter 9, "Troubleshooting."](#)

Dynamic IP Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses Dynamic IP assignment, you will see this menu:

The screenshot shows a configuration window for a Dynamic IP account. It has three main sections: Account Information, Internet IP Address, and Domain Name Server (DNS) Address, followed by Router's MAC Address. At the bottom are three buttons: Apply, Cancel, and Test.

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

☒ Get Dynamically From ISP

☐ Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

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 Computer's MAC

☐ Use This MAC Address

Figure 3-8: Setup Wizard menu for Dynamic IP address accounts

- 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 router try to discover the domain. Otherwise, you may need to enter it manually.
- If you know that your ISP does not automatically transmit DNS addresses to the router 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.

Note: If you enter DNS addresses, restart your computers so that these settings take effect.

- If your ISP requires a specific MAC address for the connection, you may need to fill a MAC address. Usually, it is not necessary to change the MAC address setting.
- Click Apply to save your settings.
- Click Test to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to [Chapter 9, "Troubleshooting."](#)

Fixed IP Account Wizard-Detected Option

If the Setup Wizard discovers that your ISP uses Fixed IP assignment, you will see this menu:

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

☐ Get Dynamically From ISP

☒ Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

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 Computer's MAC

☐ Use This MAC Address

Figure 3-9: Setup Wizard menu for Fixed IP address accounts

- Fixed IP is also called Static IP. 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. You will need the configuration parameters from your ISP you recorded in [“Record Your Internet Connection Information”](#) on page 3-3.
- Enter the IP address of your ISP's Primary and Secondary DNS Server addresses.

Note: Restart the computers on your network so that these settings take effect.

- If your ISP requires a specific MAC address for the connection, you may need to fill a MAC address. Usually, it is not necessary to change the MAC address setting.
- Click Apply to save the settings.
- Click Test to test your Internet connection. If the NETGEAR website does not appear within one minute, refer to [Chapter 9, “Troubleshooting.”](#)

Manually Configuring Your Internet Connection

You can manually configure your router using the menu below, or you can allow the Setup Wizard to determine your configuration as described in the previous section.

ISP Does Not Require Login

Basic Settings

Does Your Internet Connection Require A Login?

☒ No

☐ Yes

Account Name (If Required)

Domain Name (If Required)

Internet IP Address

☒ Get Dynamically From ISP

☐ Use Static IP Address

IP Address

IP Subnet Mask

Gateway IP Address

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 Computer's MAC

☐ Use This MAC Address

ISP Does Require Login

Basic Settings

Does Your Internet Connection Require A Login?

☐ No

☒ Yes

Internet Service Provider Name

Account Name

Domain Name

Login

Password

Idle Timeout Minutes

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 Computer's MAC

☐ Use This MAC Address

Figure 3-10: Browser-based configuration Basic Settings menus

Procedure: Configuring the Internet Connection Manually

You can manually configure the router using the Basic Settings menu shown in [Figure 3-10](#) using these steps:

1. Click the Basic Settings link on the Setup menu.
2. If your Internet connection does not require a login, click No at the top of the Basic Settings menu and fill in the settings according to the instructions below. If your Internet connection does require a login, click Yes, and skip to step 3.
 - a. 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.
 - b. 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 router will connect.
 - c. Domain Name Server (DNS) Address:
If you know that your ISP does not automatically transmit DNS addresses to the router 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.

Note: If you enter an address here, restart the computers on your network so that these settings take effect.
 - d. Gateway's MAC Address:
This section determines the Ethernet MAC address that will be used by the router 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 router to masquerade as that PC by "cloning" its MAC address.

To change the MAC address, select "Use this Computer's MAC address." The router 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. Or, select "Use this MAC address" and enter it.
 - e. Click Apply to save your settings.
3. If your Internet connection does require a login, fill in the settings according to the instructions below.

Note: After you finish setting up your router, 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 router will automatically log you in.

- a. Select your Internet service provisory from the drop-down list.
- b. The screen will change according to the ISP settings requirements of the ISP you select.
- c. Fill in the parameters for your ISP according to the Wizard-detected procedures starting on [page 3-8](#).
- d. Click Apply to save your settings.

Chapter 4

Wireless Configuration

This chapter describes how to configure the wireless features of your FWAG114 wireless firewall.

Observe Performance, Placement, and Range Guidelines

In planning your wireless network, you should consider the level of security required. You should also select the physical placement of your FWAG114 in order to maximize the network speed. For further information on wireless networking, refer to in [Appendix D, “Wireless Networking Basics.”](#)

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the FWAG114 wireless firewall. The latency, data throughput performance, and notebook power consumption also vary depending on your configuration choices.



Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the VPN firewall . For complete range and performance specifications, please see [Appendix A, “Technical Specifications.”](#)

For best results, place your VPN firewall :

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls). The best location is elevated, such as wall mounted or on the top of a cubicle, and at the center of your wireless coverage area for all the mobile devices.
- Away from sources of interference, such as PCs, microwaves, and 2.4 GHz cordless phones. The 802.11a standard operates at a higher frequency and should be less susceptible to interference from cordless phones. This higher 802.11a frequency may not offer as much range as the lower frequency 802.11b/g in a indoor environment with lots of obstructions.
- Away from large metal surfaces.

Be aware that the time it takes to establish a wireless connection can vary depending on both your security settings and placement. WEP connections can take slightly longer to establish. Also, WEP encryption can consume more battery power on a notebook PC.

Implement Appropriate Wireless Security



Note: Indoors, computers can connect over 802.11 wireless networks at ranges of 300 feet or more. Such distances can allow for others outside of your immediate area to access your network.

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, use the security features of your wireless equipment. The FWAG114 wireless firewall provides highly effective security features which are covered in detail in this chapter. Deploy the security features appropriate to your needs.

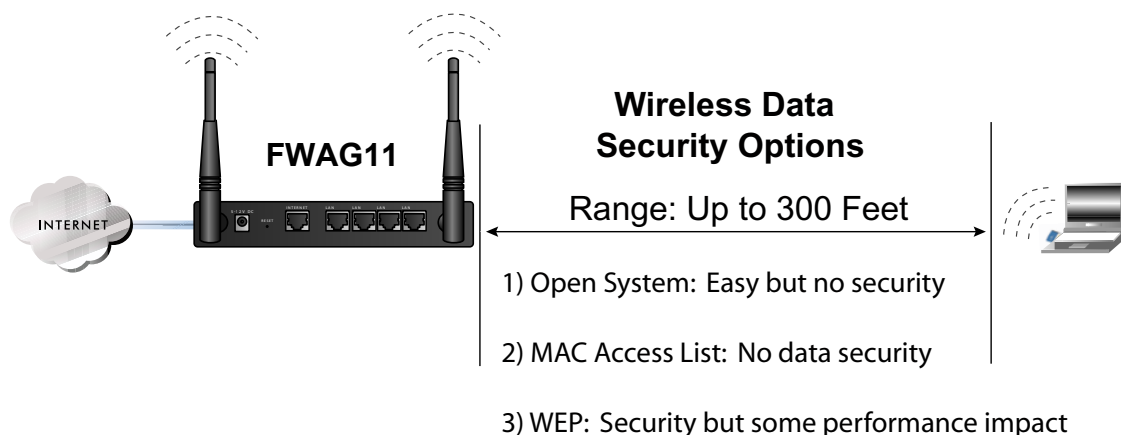


Figure 4-1: FWAG114 wireless data security options

There are several ways you can enhance the security of you wireless network.

- **Restrict Access Based on MAC Address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the FWAG114. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.
- **Turn Off the Broadcast of the Wireless Network Name SSID.** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network ‘discovery’ feature of some products such as Windows XP, but the data is still fully exposed.
- **Turn Off Bridging to the Wired LAN.** If you disable bridging to the LAN, wireless devices cannot communicate with computers on the Ethernet LAN but can still access the Internet. This blocks any access to the computers on the wired LAN but the wireless data routed to the Internet is still fully exposed.
- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP Shared Key authentication and WEP data encryption will block all but the most determined eavesdropper.

Understanding Wireless Settings

To configure the wireless settings of your FWAG114, click the Wireless 11a or Wireless 11b/g link in the Setup section of the main menu. The wireless settings menu will appear, as shown below.

Wireless 11a Settings

Identification
Regulatory Domain:
Station Name:
SSID (Service Set Identifier):

Options
Channel / Frequency:
Turbo Mode: ☒ Disable ☐ Enable
Data Rate:
Transmit Power:
Beacon Interval: ms
DTIM (1 - 255):
WEP Status: no data encryption

Access Point Connections
Allow access by: ☒ All Wireless stations
☐ Trusted PCs only

☒ Enable bridging to wired LAN
☒ Enable SSID broadcast

Wireless 11b/g Settings

Identification
Regulatory Domain:
Station Name:
SSID (Service Set Identifier):

Options
Channel / Frequency:
Data Rate:
Transmit Power:
Beacon Interval: ms
DTIM (1 - 255):
WEP Status: no data encryption

Access Point Connections
Allow access by: ☒ All Wireless stations
☐ Trusted PCs only

☒ Enable bridging to wired LAN
☒ Enable SSID broadcast

Figure 4-2: Wireless 11a and 11b/g Settings menus



Note: The 802.11b and 802.11g wireless networking protocols are configured in exactly the same fashion. The FWAG114 will automatically adjust to the 802.11g or 802.11b protocol as the device requires without compromising the speed of the other connected devices.

Common Wireless Settings

The 802.11a and the 802.11b/g wireless network identification settings are configured separately. However, some types of items you configure in each network are the same. The Wireless Settings menu items which are the same for either type of wireless network are discussed below.

- **Station Name.** The station name of the FWAG114.
- **Regulatory Domain.** For the Wireless 802.11a settings, unless you select a regulatory domain, the 802.11a radio is turned off. This field identifies the region where the FWAG114 can be used. It may not be legal to operate the wireless features of the VPN firewall in a region other than one of those identified in this field.
- **SSID (Service Set Identification).** The SSID is also known as the wireless network name. Enter a value of up to 32 alphanumeric characters. In a setting where there is more than one wireless network, different wireless network names provide a means for separating the traffic. Any device you want to participate in the 11a or the 11b/g wireless network will need to use this SSID for that network. The FWAG114 default SSID is: **NETGEAR**.
- **Options.**
 - **Channel/Frequency.** 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. For more information on the wireless channel frequencies please refer to [“Wireless Channels” on page D-7](#).
 - **Turbo Mode, 802.11a Only.** Enabling turbo mode allows the wireless node to transmit or receive at a higher rate, up to 108 Mbps. Default: Disable.
 - **Data Rate.** Shows the available transmit data rate of the wireless network. The possible data rates supported for 802.11a interface are: 54 Mbps, 48 Mbps, 36 Mbps, 24 Mbps, 18 Mbps, 12 Mbps, 9 Mbps, and 6 Mbps. It can go up to 108 Mbps if the turbo mode is enabled. Default: Best.
 - **Transmit Power.** Set the transmit signal strength of the access point. The options are full, half, quarter, eighth, and min. Decrease the transmit power if more than one AP is co-located using the same channel frequency. Default: Full.

- **Beacon Interval.** Specifies the Beacon Interval value. Enter a value in between 20 to 1000. Default: 100.
- **DTIM.** The Delivery Traffic Indication Message. Specifies the data beacon rate between 1 and 255. Default: 1
- **WEP Status.** If WEP is enabled, this will indicate the current settings.
- **Access Point Connections.** Lets you restrict wireless connections according to a list of Trusted PCs MAC addresses. When the Trusted PCs Only radio button is selected, the FWAG114 checks the MAC address of the wireless station and only allows connections to PCs identified on the trusted PCs list.
- **SSID Broadcast Enable.** The default setting is to enable SSID broadcast. If you disable broadcast of the SSID, only devices that have the correct SSID can connect. Disabling SSID broadcast somewhat hampers the wireless network ‘discovery’ feature of some products.
- **Enable Bridging to the Wired LAN.** The default setting is to enable bridging to the wired LAN. If you disable bridging to the LAN, wireless devices cannot communicate with computers on the Ethernet LAN but can still access the Internet.

Although the types of settings described above are the same for either type of wireless network, the choices you make in each type of network can be different. For example, you can disable the SSID broadcast in you 802.11a wireless network but enable it in your 802.11b/g network.

Understanding WEP Authentication and Encryption

Restricting wireless access to your network prevents intruders from connecting to your network. However, the wireless data transmissions are still vulnerable to snooping. Using the WEB data encryption settings described below will prevent a determined intruder from eavesdropping on your wireless data communications. Also, if you are using the Internet for such activities as purchases or banking, those Internet sites use another level of highly secure encryption called SSL. You can tell if a web site is using SSL because the web address begins with HTTPS rather than HTTP.

Authentication Type

The FWAG114 lets you select the following wireless authentication schemes.

- Open System.
- Shared key.

Be sure to set your wireless adapter according to the authentication scheme you choose for the FWAG114 wireless firewall. Please refer to [“Authentication and WEP Data Encryption” on page D-3](#) for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

WEP

Choose the encryption settings from this menu. Please refer to [“Overview of WEP Parameters” on page D-5](#) for a full explanation of each of these options, as defined by the IEEE 802.11 wireless communication standard.

- **Disable.** No encryption will be applied. This setting is useful for troubleshooting your wireless connection, but leaves your wireless data fully exposed.
- **64-bit, 128-bit, or in the case of 802.11a, 152-bit WEP.** When 64-, 128-, or 152-Bit WEP is selected, WEP encryption will be applied.

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.

There are two methods for creating WEP encryption keys:

- **Passphrase.** Enter a word or group of printable characters in the Passphrase box and click the Generate button.
- **Manual.** 64-bit WEP: Enter 10 hexadecimal digits (any combination of 0-9, a-f, or A-F).
128-bit WEP: Enter 26 hexadecimal digits (any combination of 0-9, a-f, or A-F).

Clicking the radio button selects which of the four keys will be the default.

Default Factory Settings

When you first receive your FWAG114, the default factory settings are shown below. You can restore these defaults with the Factory Default Restore button on the rear panel. After you install the FWAG114 wireless firewall, use the procedures below to customize any of the settings to better meet your networking needs.

FEATURE	DEFAULT FACTORY SETTINGS
SSID for both 802.11a & 802.11b	NETGEAR
11a RF Channel	Off until the Regulatory Domain is selected, then 52 Non-Turbo Mode; 50 Turbo Mode
11b RF Channel	6
WEP	Disabled
Authentication Type	Open System
Access Point Connections for both 802.11a & 802.11b/g	All wireless stations allowed
Bridging to wired LAN for both 802.11a & 802.11b/g	Enabled
SSID broadcast for both 802.11a & 802.11b/g	Enabled

Before You Change the SSID and WEP Settings

Take the following steps:

For a new wireless network, print or copy this form and fill in the configuration parameters. For an existing wireless network, the person who set up or is responsible for the network will be able to provide this information. Be sure to set the Regulatory Domain correctly as the first step.

- **SSID:** The Service Set Identification (SSID) identifies the wireless local area network. **NETGEAR** is the default FWAG114 SSID. However, you may customize it by using up to 32 alphanumeric characters. Write your customized SSID on the line below.

Note: The SSID in the VPN firewall is the SSID you configure in the wireless adapter card. All wireless nodes in the same network must be configured with the same SSID.

802.11a SSID: _____

802.11b SSID: _____

- **Authentication**

The two bands can use different authentication settings. Choose “Shared Key” for more security.

802.11a SSID, circle one: Open System or Shared Key

802.11b SSID, circle one: Open System or Shared Key

Note: If you select shared key, the other devices in the network will not connect unless they are set to Shared Key as well.

- **WEP Encryption**

802.11a and 802.11b differ in their use of WEP encryption keys. See [“Security Configuration” on page 2-21](#) for a description of these differences.

802.11a WEP Encryption Keys

Key 1: _____ Circle Key Size: 64 or 128 or 152 bits

Key 2: _____ Circle Key Size: 64 or 128 or 152 bits

Key 3: _____ Circle Key Size: 64 or 128 or 152 bits

Key 4: _____ Circle Key Size: 64 or 128 or 152 bits

802.11b WEP Encryption Keys

For all four 802.11b keys, choose the Key Size. Circle one: 64 or 128 bits

Key 1: _____

Key 2: _____

Key 3: _____

Key 4: _____

Use the procedures described in the following sections to configure the FWAG114. Store this information in a safe place.

How to Set Up and Test Basic Wireless Connectivity

Follow the instructions below to set up and test basic wireless connectivity. Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs.

1. Log in the default LAN address of <http://192.168.0.1> with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Depending on the types of wireless adapters you have in your computers, click the Wireless 11a or 11b link in the main menu of the FWAG114.
3. Set the Regulatory Domain correctly.
4. Choose a suitable descriptive name for the wireless network name (SSID). In the SSID box, enter a value of up to 32 alphanumeric characters. The default SSID is NETGEAR.

Note: The characters are case sensitive. An access point always functions in infrastructure mode. The SSID for any wireless device communicating with the access point must match the SSID configured in the ProSafe Dual Band Wireless VPN Firewall FWAG114. If they do not match, you will not get a wireless connection to the FWAG114.

5. Set the Channel.

It should not be necessary to change the wireless channel unless you notice interference problems with another nearby wireless router or access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your VPN firewall . For more information on the wireless channel frequencies please refer to [“Wireless Channels” on page D-7](#).

6. For initial configuration and test, leave the Wireless Card Access List set to “All Wireless Stations” and the Encryption Strength set to “Disable.”
7. Click Apply to save your changes.



Note: If you are configuring the FWAG114 from a wireless PC and you change the VPN firewall 's SSID, channel, or security 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 FWAG114's new settings.

8. Configure and test your PCs for wireless connectivity.

Program the wireless adapter of your PCs to have the same SSID that you configured in the FWAG114. Check that they have a wireless link and are able to obtain an IP address by DHCP from the VPN firewall .

Once your PCs have basic wireless connectivity to the VPN firewall , then you can configure the advanced options and wireless security functions.

How to Restrict Wireless Access by MAC Address

To restrict access based on MAC addresses, follow these steps:

1. Log in at the default LAN address of <http://192.168.0.1> with the default user name of **admin** and default password of **password**.
2. Click the Wireless 11a or 11b link in the main menu of the FWAG114.
3. From the Wireless Settings menu, click the Trusted PCs only radio button.

- Click the Trusted PCs button to display the Wireless Access menu shown below.

Wireless 11b Access

Trusted PCs

Delete

Add new Trusted PC

Wireless Adapter

MAC address

Add

Back

Figure 4-3. Wireless Access menu

- Enter the MAC address of a wireless adapter and click the Add button to add a wireless device to the wireless access control list. The Trusted PCs list updates with the new entry.

Note: You can copy and paste the MAC addresses from the FWAG114's Attached Devices menu into the MAC Address box of this menu. To do this, configure each wireless PC to obtain a wireless link to the VPN firewall. The PC should then appear in the Attached Devices menu.

- Click the Back button to return to the Wireless Settings menu.



Note: When configuring the FWAG114 from a wireless PC whose MAC address is not in the Trusted PC list, if you select Turn Access Control On, you will lose your wireless connection when you click on Apply. You must then access the VPN firewall from a wired PC or from a wireless PC which is on the access control list to make any further changes.

- Be sure to click Apply to save your trusted wireless PCs list settings.

Now, only devices on this list will be allowed to wirelessly connect to the FWAG114.

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

How to Configure WEP

To configure WEP data encryption, follow these steps:

1. Log in at the default LAN address of <http://192.168.0.1> with the default user name of **admin** and default password of **password**, or using whatever LAN address and password you have set up.
2. Click the Wireless 11a or 11b link in the main menu of the FWAG114.
3. Click the Configure WEP button.
4. Choose the Authentication Type and WEP option.
5. You can manually or automatically program the four data encryption keys. These values must be identical on all PCs and Access Points in your network.
 - Automatic - Enter a word or group of printable characters in the Passphrase box and click the Generate button. The four key boxes will be automatically populated with key values.
 - Manual - Enter ten hexadecimal digits (any combination of 0-9, a-f, or A-F)
Select which of the four keys will be active.

Please refer to “[Overview of WEP Parameters](#)” on [page D-5](#) for a full explanation of each of these options, as defined by the IEEE 802.11b wireless communication standard.

6. Click Apply to save your settings.



Note: When configuring the VPN firewall from a wireless PC, if you configure WEP settings, you will lose your wireless connection when you click on Apply. You must then either configure your wireless adapter to match the VPN firewall WEP settings or access the VPN firewall from a wired PC to make any further changes.

Chapter 5

Firewall Protection and Content Filtering

This chapter describes how to use the content filtering features of the ProSafe Dual Band Wireless VPN Firewall FWAG114 to protect your network. These features can be found by clicking on the Content Filtering heading in the Main Menu of the browser interface.

Firewall Protection and Content Filtering Overview

The ProSafe Dual Band Wireless VPN Firewall FWAG114 provides you with Web content filtering options, plus browsing activity reporting and instant alerts via e-mail. Parents and network administrators can establish restricted access policies based on time-of-day, web addresses and web address keywords. You can also block Internet access by applications and services, such as chat or games.

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.

To configure these features of your router, click on the subheadings under the Content Filtering heading in the Main Menu of the browser interface. The subheadings are described below:

Block Sites

The FWAG114 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 5-1](#):

Block Sites

☒ Turn Keyword Blocking On

Add Keyword

Block Sites Containing These Keywords Or Domain Names:

yahoo

Delete Keyword Clear List

☐ Allow Trusted IP Address To Visit Blocked Sites

Trusted IP address

Apply Cancel

Figure 5-1: 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, as is the newsgroup alt.pictures.XXX.
- 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.

Using Rules to Block or Allow Specific Kinds of Traffic

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 FWAG114 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 5-2](#):

Rules

Outbound Services

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

Add

Edit

Move

Delete

Inbound Services

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

Add

Edit

Move

Delete

☐ Default DMZ Server...☒ Respond to Ping on Internet WAN Port

Apply

Cancel

Figure 5-2: 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 5-3](#). 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.
 - **Match** - traffic of this type which matches the parameters and action will be logged.

Inbound Rules (Port Forwarding)

Because the FWAG114 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 router 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 FWAG114 wireless 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 5-3](#):

Inbound Services

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

Figure 5-3: 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 5-4](#), 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 'Inbound Services' configuration window. It has several fields and buttons:

- Service:** A dropdown menu set to 'CU-SEEME(TCP/UDP:7648)'.
- Action:** A dropdown menu set to 'ALLOW always'.
- Send to LAN Server:** Four input boxes containing '192', '168', '0', and '11'.
- WAN Users:** A dropdown menu set to 'Address Range'.
- start:** Four input boxes containing '134', '177', '88', and '1'.
- finish:** Four input boxes containing '134', '177', '88', and '254'.
- Log:** A dropdown menu set to 'Not Match'.
- Buttons:** 'Back', 'Apply', and 'Cancel' at the bottom.

Figure 5-4: 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 menus 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 FWAG114 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:

- IP address of the local PC (source address)
- IP address of the Internet site being contacted (destination address)
- Time of day
- 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 router log any attempt to use Instant Messenger during that blocked period.

Outbound Services

The screenshot shows the 'Outbound Services' configuration page. It includes the following fields and options:

- Service:** A dropdown menu with 'AIM(TCP:5190)' selected.
- Action:** A dropdown menu with 'BLOCK by schedule, otherwise allow' selected.
- LAN users:** A dropdown menu with 'Any' selected. Below it are 'start' and 'finish' time fields, each with four input boxes for HH:MM:SS (all set to 0).
- WAN Users:** A dropdown menu with 'Any' selected. Below it are 'start' and 'finish' time fields, each with four input boxes for HH:MM:SS (all set to 0).
- Log:** A dropdown menu with 'Match' selected.
- At the bottom are three buttons: 'Back', 'Apply', and 'Cancel'.

Figure 5-5: 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 5-6](#):

Rules

Outbound Services

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

Add Edit Move Delete

Inbound Services

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

Add Edit Move Delete

☐ Default DMZ Server

192.168.0.0

☒ Respond to Ping on Internet/WAN Port

Apply Cancel

Figure 5-6: 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 router 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 router 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 router 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 router 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 FWAG114 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 5-7](#):

Services

Service Table


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

Figure 5-7: 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 the Services menu and click on the Add Custom Service button. The Add Services menu will appear, as shown in [Figure 5-8](#):

Services

Service Definition

Name:

Type:

Start Port: (TCP or UDP)

Finish Port: (TCP or UDP)

Figure 5-8: 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.

Using a Schedule to Block or Allow Specific Traffic

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 router allows you to specify when blocking will be enforced by configuring the Schedule tab shown below:

Schedule

☐ Use this schedule for rules

Days:

☐ Every Day

☐ Sunday

☐ Monday

☐ Tuesday

☐ Wednesday

☐ Thursday

☐ Friday

☐ Saturday

Time of day: (use 24-hour clock)

☐ All Day

Start Time hour minute

End Time hour minute

Time Zone

(GMT-12:00) Eniwetok,Kwajalein

☐ Adjust for daylight savings time

☐ Use this NTP Server . . .

Current time:

Figure 5-9: Schedule menu

To block keywords or Internet domains based on a schedule, select Every Day or select one or more days. 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.

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

Time Zone

The FWAG114 wireless 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 specify your Time Zone:

- Time Zone. Select your local time zone. This setting will be used for the blocking schedule and for time-stamping log entries.
- Daylight Savings Time. Check this box for daylight savings time.

Note: If your region uses Daylight Savings Time, you must manually select Adjust for Daylight Savings Time on the first day of Daylight Savings Time, and unselect it at the end. Enabling Daylight Savings Time will add one hour to the standard time.

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

Getting E-Mail Notifications of Event Logs and Alerts

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.

Figure 5-10: E-mail menu

- **Turn e-mail notification on.** Check this box if you wish to receive e-mail logs and alerts from the router.
- **Send alerts and logs by e-mail.** If you enable e-mail notification, these boxes cannot be blank. 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. 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.
- **Send E-mail alerts immediately.** 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.
- **Send logs according to this schedule.** You can specify that logs are sent to you according to a schedule. Select whether you would like to receive the logs None, 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 router's memory. If the router cannot e-mail the log file, the log buffer may fill up. In this case, the router overwrites the log and discards its contents.

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

Viewing Logs of Web Access or Attempted Web Access

The router 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 5-11](#):

Logs

Date: 2000-01-01 00:25:34

```
Destination: 217.207.63.122 - [Unable to determine route to destination,
dropping packet Src 1075 Dst 161 from CORP n/w]
Sat, 2000-01-01 00:24:50 - UDP packet - Source: 192.168.0.2 -
Destination: 217.207.63.122 - [Unable to determine route to destination,
dropping packet Src 1075 Dst 161 from CORP n/w]
Sat, 2000-01-01 00:25:01 - [Send out NTP Request to 133.100.9.2]
Sat, 2000-01-01 00:25:01 - [NTP Reply Invalid]
Sat, 2000-01-01 00:25:27 - UDP packet - Source: 192.168.0.2 -
Destination: 217.207.63.122 - [Unable to determine route to destination,
dropping packet Src 1075 Dst 161 from CORP n/w]
Sat, 2000-01-01 00:25:31 - [Send out NTP Request to 133.100.9.2]
Sat, 2000-01-01 00:25:31 - [NTP Reply Invalid]
Sat, 2000-01-01 00:25:33 - UDP packet - Source: 192.168.0.2 -
Destination: 217.207.63.122 - [Unable to determine route to destination,
dropping packet Src 1075 Dst 161 from CORP n/w]
```

Refresh Clear Log Send Log

Include in Log

- ☒ Known DoS attacks and port scans
- ☒ Attempted access to blocked sites
- ☒ Router administration (startup, time sync, logins, etc)
- ☐ All websites and newsgroups visited
- ☐ Local activity
- ☐ All incoming and outgoing traffic

☐ **Enable Syslog**

- ☐ Broadcast on LAN
- ☐ Send to this Syslog Server IP Address

Apply Cancel

Figure 5-11: 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.

Syslog

You can configure the router to send system logs to an external PC that is running a syslog logging program. Enter the IP address of the logging PC and click the Enable Syslog checkbox.

Logging programs are available for Windows, Macintosh, and Linux computers.

Chapter 6

Maintenance

This chapter describes how to use the maintenance features of your ProSafe Dual Band Wireless VPN Firewall FWAG114. These features can be found by clicking on the Maintenance heading in the Main Menu of the browser interface.

Viewing VPN Firewall Status Information

The Router Status menu provides status and usage information. From the main menu of the browser interface, click on Maintenance, then select Router Status to view this screen.

Router Status

System Name	FWAG114
Firmware Version	U12H00500_V1.0.8
WAN Port	
MAC Address	00:90:4c:22:00:04
IP Address	0.0.0.0
DHCP	DHCPClient
IP Subnet Mask	0.0.0.0
Domain Name Server	0.0.0.0
LAN Port	
MAC Address	00:90:4c:21:00:04
IP Address	192.168.0.1
DHCP	ON
IP Subnet Mask	255.255.255.0
IEEE802.11a Interface	
SSID	wireless 11a
BSSID	00:03:7F:BE:F4:20
Channel/Frequency	52/5.260GHz
WEP Status	Disabled
IEEE802.11b/g Interface	
SSID	wireless 11g
BSSID	00:03:7F:00:15:39
Channel/Frequency	11/2.462GHz
WEP Status	Disabled
Show Statistics	
Show WAN Status	

Figure 6-1: Router Status screen

This screen shows the following parameters:

Table 6-1. Menu 3.2 - FWAG114 Status Fields

Field	Description
System Name	This field displays the System Name assigned to the router.
Firmware Version	This field displays the router firmware version.
WAN Port	These parameters apply to the Internet (WAN) port of the router.
MAC Address	This field displays the MAC address being used by the Internet (WAN) port of the router.
IP Address	This field displays the IP address being used by the Internet (WAN) port of the router. If no address is shown, the router cannot connect to the Internet.
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Internet (WAN) port of the router.
DHCP	This field shows the protocol on the WAN port used to obtain the WAN IP address. This field can show DHCP Client, Fixed IP, PPPoE, BPA or PPTP. For example, if set to Client, the router is configured to obtain an IP address dynamically from the ISP.
LAN Port	These parameters apply to the Local (WAN) port of the router.
MAC Address	This field displays the Media Access Control address being used by the LAN port of the router.
IP Address	This field displays the IP address being used by the Local (LAN) port of the router. The default is 192.168.0.1
IP Subnet Mask	This field displays the IP Subnet Mask being used by the Local (LAN) port of the router. The default is 255.255.255.0
DHCP	Identifies if the router's built-in DHCP server is active for the LAN attached devices.
IEEE802.11a/b/g Interface	These parameters apply to the 802.11a Wireless port of the router.
SSID	This field displays the wireless network name (SSID) being used by the wireless port of the router. The default is Wireless.
MAC Address	This field displays the MAC address being used by the wireless port of the router.
Channel/Frequency	Identifies if the channel the wireless port is using. See "Wireless Channels" on page D-7 for the frequencies used on each channel.
WEP Status	Identifies the current WEP configuration of this interface.

Click “Show WAN Status” to display the WAN connection status.

Connection Time	00:00:00
Connection Method	DynamicIP
IP Address	0.0.0.0
Network Mask	0.0.0.0
Default Gateway	0.0.0.0

Figure 6-2: Connection Status screen

This screen shows the following statistics:.

Table 6-1. Connection Status Fields

Field	Description
Connection Time	The length of time the router has been connected to your Internet service provider's network.
Connection Method	The method used to obtain an IP address from your Internet service provider.
IP Address	The WAN (Internet) IP Address assigned to the router.
Network Mask	The WAN (Internet) Subnet Mask assigned to the router.
Default Gateway	The WAN (Internet) default gateway the router communicates with.

Log action buttons are described in [Table 6-2](#)

Table 6-2. Connection Status action buttons

Field	Description
Renew	Click the Renew button to renew the DHCP lease.

Click “Show Statistics” to display router usage statistics.

System Up Time 01:09:13

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	Link Down	556	0	0	944	0	01:09:13
LAN	100M/Full	2926	2432	0	16417	3756	01:09:13
802.11a		920	0		96	0	01:09:13
802.11b/g		920	0		96	0	01:09:13

Poll Interval: (secs)

Figure 6-3: Router Statistics screen

This screen shows the following statistics:

Table 6-1. Router Statistics Fields

Field	Description
interface	The statistics for the WAN (Internet), LAN (local), 802.11a, and 802.11b/g interfaces. For each interface, the screen displays:
Status	The link status of the interface.
TxPkts	The number of packets transmitted on this interface since reset or manual clear.
RxPkts	The number of packets received on this interface since reset or manual clear.
Collisions	The number of collisions on this interface since reset or manual clear.
Tx B/s	The current transmission (outbound) bandwidth used on the interfaces.
Rx B/s	The current reception (inbound) bandwidth used on the interfaces.
Up Time	The amount of time since the router was last restarted.
Up Time	The time elapsed since this port acquired the link.
Poll Interval	Specifies the intervals at which the statistics are updated in this window. Click on Stop to freeze the display.

WAN Status action buttons are described in [Table 6-2](#)

Table 6-2. Connection Status action buttons

Field	Description
Set Interval	Enter a time and click the button to set the polling frequency.
Stop	Click the Stop button to freeze the polling information.

Viewing a List of Attached Devices

The Attached Devices menu contains a table of all IP devices that the router 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 below.

Attached Devices

#	IP Address	Device Name	MAC Address
1	192.168.0.2	emachine	00:48:54:8d:d7:d3

Refresh

Figure 6-4: 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 router is rebooted, the table data is lost until the router rediscovers the devices. To force the router to look for attached devices, click the Refresh button.

Upgrading the Router Software

The routing software of the FWAG114 wireless 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 (.TRX) file before sending it to the router. The upgrade file can be sent to the router using your browser.

Note: The Web browser used to upload new firmware into the FWAG114 wireless firewall must support HTTP uploads. NETGEAR recommends using Microsoft Internet Explorer or Netscape Navigator 3.0 or above.

From the Main Menu of the browser interface, under the Maintenance heading, select the Router Upgrade heading to display the menu shown below.

Router Upgrade

Locate and select the upgrade file from your hard disk:



The screenshot shows a web interface for the Router Upgrade menu. At the top, the title 'Router Upgrade' is displayed in blue. Below it, a text prompt reads 'Locate and select the upgrade file from your hard disk:'. This is followed by a text input field and a 'Browse...' button. At the bottom of the form, there are two buttons: 'Upload' and 'Cancel'.

Figure 6-5: 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) upgrade file
3. Click Upload.

Note: When uploading software to the FWAG114 wireless 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 router will automatically restart. The upgrade process will typically take about one minute.

In some cases, you may need to reconfigure the router after upgrading.

Configuration File Management

The configuration settings of the FWAG114 wireless firewall are stored within the router 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 below.

Settings Backup

Save a copy of current settings

Back Up

Restore saved settings from file

Browse...

Restore

Revert to factory default settings

Erase

Figure 6-6: Settings Backup menu

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

Restoring and Backing Up the Configuration

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

To save your settings, select the Backup tab. Click the Backup button. Your browser will extract the configuration file from the router 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 router. The router will then reboot automatically.

Erasing the Configuration

It is sometimes desirable to restore the router to a known blank condition. This can be done by using the Erase function, which will restore all factory settings. After an erase, the router's password will be **password**, the LAN IP address will be 192.168.0.1, and the router'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 router. See [“Restoring the Default Configuration and Password” on page 7-7](#).

Changing the Administrator Password

The default password for the router's Web Configuration Manager is **password**. Netgear recommends that you change this password to a more secure password.

From the main menu of the browser interface, under the Maintenance heading, select Set Password to bring up this menu.

Set Password

Old Password

Set Password

Repeat New Password

Administrator login times out after idle for minutes.

Figure 6-7: Set Password menu

To change the password, first enter the old password, and then enter the new password twice. Click Apply. To change the login idle timeout, change the number of minutes and click Apply.

Chapter 7

Virtual Private Networking

This chapter describes how to use the virtual private networking (VPN) features of the FWAG114 wireless firewall. VPN tunnels provide secure, encrypted communications between your local network and a remote network or computer.

Overview of FWAG114 Policy-Based VPN Configuration

The FWAG114 uses state-of-the-art firewall and security technology to facilitate controlled and actively monitored VPN connectivity. Since the FWAG114 strictly conforms to IETF standards, it is interoperable with devices from major network equipment vendors.

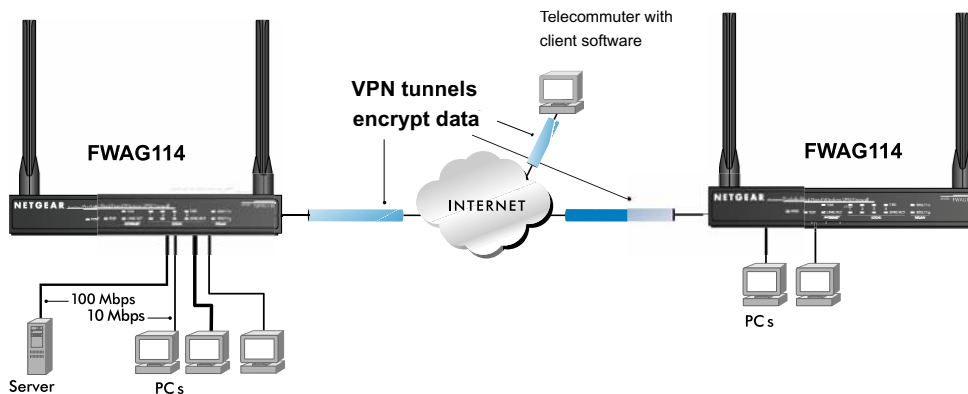


Figure 7-1: Secure access through FWAG114 VPN routers

Using Policies to Manage VPN Traffic

You create policy definitions to manage VPN traffic on the FWAG114. There are two kinds of policies:

- **IKE Policies:** Define the authentication scheme and automatically generate the encryption keys. As an alternative option, to further automate the process, you can create an IKE policy which uses a trusted certificate authority to provide the authentication while the IKE policy still handles the encryption.
- **VPN Policies:** Apply the IKE policy to specific traffic which requires a VPN tunnel. Or, you can create a VPN policy which does not use an IKE policy but in which you manually enter all the authentication and key parameters.

Since the VPN policies use the IKE policies, you define the IKE policy first. The FWAG114 also allows you to manually input the authentication scheme and encryption key values. In the case of manual key management there will not be any IKE policies.

In order to establish secure communication over the Internet with the remote site you need to configure matching VPN policies on both the local and remote FWAG114 wireless firewalls. The outbound VPN policy on one end must match to the inbound VPN policy on other end, and vice versa.

When the network traffic enters into the FWAG114 from the LAN network interface, if there is no VPN policy found for a type of network traffic, then that traffic passes through without any change. However, if the traffic is selected by a VPN policy, then the IPSec authentication and encryption rules will be applied to it as defined in the VPN policy.

By default, a new VPN policy is added with the least priority, that is, at the end of the VPN policy table.

Using Automatic Key Management

The most common configuration scenarios will use IKE policies to automatically manage the authentication and encryption keys. Based on the IKE policy, some parameters for the VPN tunnel are generated automatically. The IKE protocols perform negotiations between the two VPN endpoints to automatically generate required parameters.

Some organizations will use an IKE policy with a Certificate Authority (CA) to perform authentication. Typically, CA authentication is used in large organizations which maintain their own internal CA server. This requires that each VPN gateway has a certificate from the CA. Using CAs reduces the amount of data entry required on each VPN endpoint.

IKE Policies' Automatic Key and Authentication Management

Click the IKE Policies link from the VPN section of the main menu, and then click the Add button of the IKE Policies screen to display the IKE Policy Configuration menu shown in [Figure 7-2](#).

IKE Policies

Policy Table				
#	Name	Mode	Local ID	Remote ID
<div><div>Add</div><div>Edit</div><div>Move</div></div>				

IKE Policy Configuration

General

Policy Name

Direction/Type

Initiator

Exchange Mode

Main Mode

Local

Local Identity Type

WAN IP Address

Local Identity Data

Remote

Remote Identity Type

Remote WAN IP

Remote Identity Data

IKE SA Parameters

Encryption Algorithm

3DES

Authentication Algorithm

MD5

Authentication Method

Pre-shared Key

RSA Signature (requires Certificate)

Diffie-Hellman (DH) Group

Group 1 (768 Bit)

SA Life Time

180 (secs)

Back

Apply

Cancel

Figure 7-2: IKE - Policy Configuration Menu

The IKE Policy Configuration fields are defined in the following table.

Table 7-1. IKE Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the IKE policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify IKE policies.
Direction/Type	This setting is used when determining if the IKE policy matches the current traffic. The drop-down menu includes the following: <ul style="list-style-type: none">• Initiator – Outgoing connections are allowed, but incoming are blocked.• Responder – Incoming connections are allowed, but outgoing are blocked.• Both Directions – Both outgoing and incoming connections are allowed.• Remote Access – This is to allow only incoming client connections, where the IP address of the remote client is unknown.
Exchange Mode	<p>If Remote Access is selected, the “Exchange Mode” MUST be “Aggressive,” and the ‘Identities’ below (both Local and Remote) MUST be “Name.” On the matching VPN Policy, the IP address of the remote VPN endpoint should be set to 0.0.0.0.</p> <p>Main Mode or Aggressive Mode. This setting must match the setting used on the remote VPN endpoint.</p> <ul style="list-style-type: none">• Main Mode is slower but more secure. Also, the “Identity” below must be established by IP address.• Aggressive Mode is faster but less secure. The “Identity” below can be by name (host name, domain name, email address, etc.) instead of by IP address.
Local	These parameters apply to the Local FWAG114 wireless firewall.
Local Identity Type	Use this field to identify the local FWAG114. You can choose one of the following four options from the drop-down list: <ul style="list-style-type: none">• By its Internet (WAN) port IP address.• By its Fully Qualified Domain Name (FQDN) -- your domain name.• By a Fully Qualified User Name -- your name, E-mail address, or other ID.• By DER ASN.1 DN -- the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Local Identity Data	This field lets you identify the local FWAG114 by name.

Table 7-1. IKE Policy Configuration Fields

Field	Description
Remote	These parameters apply to the target remote FWAG114, VPN gateway, or VPN client.
Remote Identity Type	Use this field to identify the remote FWAG114. You can choose one of the following four options from the drop-down list: <ul style="list-style-type: none"> • By its Internet (WAN) port IP address. • By its Fully Qualified Domain Name (FQDN) -- your domain name. • By a Fully Qualified User Name -- your name, E-mail address, or other ID. • By DER ASN.1 DN -- the binary DER encoding of your ASN.1 X.500 Distinguished Name.
Remote Identity Data	This field lets you identify the target remote FWAG114 by name.
IKE SA Parameters	These parameters determine the properties of the IKE Security Association.
Encryption Algorithm	Choose the encryption algorithm for this IKE policy: <ul style="list-style-type: none"> • DES is the default • 3DES is more secure
Authentication Algorithm	If you enable Authentication Header (AH), this menu lets you to select from these authentication algorithms: <ul style="list-style-type: none"> • MD5 - the default • SHA-1 - more secure
Authentication Method	You may select Pre-Shared Key or RSA Signature.
Pre-Shared Key	Specify the key according to the requirements of the Authentication Algorithm you selected. <ul style="list-style-type: none"> • For MD5, the key length should be 16 bytes. • For SHA-1, the key length should be 20 bytes.
RSA Signature	RSA Signature requires a certificate.
Diffie-Hellman (D-H) Group	The DH Group setting determines the bit size used in the key exchange. This must match the value used on the remote VPN gateway or client.
SA Life Time	The amount of time in seconds before the Security Association expires; over an hour (3600) is common.

VPN Policy Configuration for Auto Key Negotiation

An already defined IKE policy is required for VPN - Auto Policy configuration. From the VPN Policies section of the main menu, you can navigate to the VPN - Auto Policy configuration menu.

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote
<div> <div>Edit</div> <div>Move</div> <div>Delete</div> </div> <div> <div>Apply</div> <div>Cancel</div> </div> <div> <div>Add Auto Policy</div> <div>Add Manual</div> </div>					

VPN - Auto Policy

General

Policy Name:

IKE policy:

Remote VPN Endpoint: Address Type: Address Data:

SA Life Time: (Seconds) (Kbytes)

☐ IPSec PFS PFS Key Group:

Traffic Selector

Local IP:

Start IP address:

Finish IP address:

Subnet Mask:

Remote IP:

Start IP address:

Finish IP address:

Subnet Mask:

AH Configuration

☐ Enable Authentication Authentication Algorithm:

ESP Configuration

☐ Enable Encryption Encryption Algorithm:

☐ Enable Authentication Authentication Algorithm:

☐ NETBIOS Enable

Figure 7-3: VPN - Auto Policy Menu

The VPN Auto Policy fields are defined in the following table.

Table 7-1. VPN Auto Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The descriptive name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN endpoint. It is only used to help you identify VPN policies.
IKE Policy	The existing IKE policies are presented in a drop-down list. Note: Create the IKE policy BEFORE creating a VPN - Auto policy.
Remote VPN Endpoint	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FWAG114's Local IP values entered as its "Remote VPN Endpoint." <ul style="list-style-type: none"> • By its Fully Qualified Domain Name (FQDN) -- your domain name. • By its IP Address.
Address Type	The address type used to locate the remote VPN firewall or client to which you wish to connect. <ul style="list-style-type: none"> • By its Fully Qualified Domain Name (FQDN) -- your domain name. • By its IP Address.
Address Data	The address used to locate the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FWAG114's Local Identity Data entered as its "Remote VPN Endpoint." <ul style="list-style-type: none"> • By its Fully Qualified Domain Name (FQDN) -- your domain name. • By its IP Address.
SA Life Time	The duration of the Security Association before it expires. <ul style="list-style-type: none"> • Seconds - the amount of time before the SA expires. Over an hour is common (3600). • Kbytes - the amount of traffic before the SA expires. One of these can be set without setting the other.
IPSec PFS	If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. Each key has no relationship to the previous key.
PFS Key Group	If PFS is enabled, this setting determines the DH group bit size used in the key exchange. This must match the value used on the remote gateway.

Table 7-1. VPN Auto Policy Configuration Fields

Field	Description
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets <i>all</i> criteria, then a VPN tunnel will be created.
Local IP	The drop-down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from your network address space. The choices are: <ul style="list-style-type: none"> • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Remote IP	The drop-down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from the remote site's corporate network address space. The choices are: <ul style="list-style-type: none"> • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint.
Enable Authentication	Use this checkbox to enable or disable AH for this VPN policy.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: <ul style="list-style-type: none"> • MD5 - the default • SHA1 - more secure
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both Encryption and Authentication. Two ESP modes are available: <ul style="list-style-type: none"> • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
Enable Encryption	Use this checkbox to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP encryption, then select the encryption algorithm: <ul style="list-style-type: none"> • DES - the default • 3DES - more secure

Table 7-1. VPN Auto Policy Configuration Fields

Field	Description
Enable Authentication	Use this checkbox to enable or disable ESP transform for this VPN policy. You can select the ESP mode also with this menu. Two ESP modes are available: <ul style="list-style-type: none">• Plain ESP• ESP with authentication
Authentication Algorithm	If you enable AH, then use this menu to select which authentication algorithm will be employed. The choices are: <ul style="list-style-type: none">• MD5 - the default• SHA1 - more secure
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

VPN Policy Configuration for Manual Key Exchange

With Manual Key Management, you will not use an IKE policy. You must manually type in all the required key information. Click the VPN Policies link from the VPN section of the main menu to display the menu shown below.

VPN Policies

Policy Table

#	Enable	Name	Type	Local	Remote	AH	ESP
<div><div>Edit</div><div>Move</div><div>Delete</div></div> <div><div>Apply</div><div>Cancel</div></div>							

Add Auto Policy

Add Manual Policy

VPN - Manual Policy

General

Policy Name

Remote VPN Endpoint

Address Type: IP Address

Address Data:

Traffic Selector

Local IP

- Select -

Start IP address:

0

0

0

0

Finish IP address:

0

0

0

0

Subnet Mask:

0

0

0

0

Remote IP

- Select -

Start IP address:

0

0

0

0

Finish IP address:

0

0

0

0

Subnet Mask:

0

0

0

0

AH Configuration

SPI - Incoming (Hex, 3 - 8 Characters)

SPI - Outgoing (Hex, 3 - 8 Characters)

☐ Enable Authentication

Authentication Algorithm: MD5

Key - In:

Key - Out:

(MD5 - 16 chars; SHA-1 - 20 chars)

ESP Configuration

SPI - Incoming (Hex, 3 - 8 Characters)

SPI - Outgoing (Hex, 3 - 8 Characters)

☐ Enable Encryption

Encryption Algorithm: DES

Key - In:

Key - Out:

(DES - 8 chars; 3DES - 24 chars)

☐ Enable Authentication

Authentication Algorithm: MD5

Key - In:

Key - Out:

(MD5 - 16 chars; SHA-1 - 20 chars)

☐ NETBIOS Enable

Figure 7-4: VPN - Manual Policy Menu

The VPN Manual Policy fields are defined in the following table.

Table 7-1. VPN Manual Policy Configuration Fields

Field	Description
General	These settings identify this policy and determine its major characteristics.
Policy Name	The name of the VPN policy. Each policy should have a unique policy name. This name is not supplied to the remote VPN Endpoint. It is used to help you identify VPN policies.
Remote VPN Endpoint	The WAN Internet IP address of the remote VPN firewall or client to which you wish to connect. The remote VPN endpoint must have this FWAG114's WAN Internet IP address entered as its "Remote VPN Endpoint."
Traffic Selector	These settings determine if and when a VPN tunnel will be established. If network traffic meets <i>all</i> criteria, then a VPN tunnel will be created.
Local IP	The drop down menu allows you to configure the source IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from your network address space. The choices are: <ul style="list-style-type: none"> • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Remote IP	The drop down menu allows you to configure the destination IP address of the outbound network traffic for which this VPN policy will provide security. Usually, this address will be from the remote site's corporate network address space. The choices are: <ul style="list-style-type: none"> • ANY for all valid IP addresses in the Internet address space • Single IP Address • Range of IP Addresses • Subnet Address
Authenticating Header (AH) Configuration	AH specifies the authentication protocol for the VPN header. These settings must match the remote VPN endpoint. Note: The "Incoming" settings here must match the "Outgoing" settings on the remote VPN endpoint, and the "Outgoing" settings here must match the "Incoming" settings on the remote VPN endpoint.
SPI - Incoming	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Outgoing SPI" field.

Table 7-1. VPN Manual Policy Configuration Fields

Field	Description
SPI - Outgoing	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Incoming SPI" field.
Enable Authentication	Use this checkbox to enable or disable AH. Authentication is often not used. In this case, leave the checkbox unchecked.
Authentication Algorithm	If you enable AH, then select the authentication algorithm: <ul style="list-style-type: none"> • MD5 - the default • SHA1 - more secure Enter the keys in the fields provided. For MD5, the keys should be 16 characters. For SHA-1, the keys should be 20 characters.
Key - In	Enter the keys. <ul style="list-style-type: none"> • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - Out" field.
Key - Out	Enter the keys in the fields provided. <ul style="list-style-type: none"> • For MD5, the keys should be 16 characters. • For SHA-1, the keys should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - In" field.
Encapsulated Security Payload (ESP) Configuration	ESP provides security for the payload (data) sent through the VPN tunnel. Generally, you will want to enable both encryption and authentication when you use ESP. Two ESP modes are available: <ul style="list-style-type: none"> • Plain ESP encryption • ESP encryption with authentication These settings must match the remote VPN endpoint.
SPI - Incoming	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Outgoing SPI" field.
SPI - Outgoing	Enter a Hex value (3 - 8 chars). Any value is acceptable, provided the remote VPN endpoint has the same value in its "Incoming SPI" field.
Enable Encryption	Use this checkbox to enable or disable ESP Encryption.
Encryption Algorithm	If you enable ESP Encryption, then select the Encryption Algorithm: <ul style="list-style-type: none"> • DES - the default • 3DES - more secure

Table 7-1. VPN Manual Policy Configuration Fields

Field	Description
Key - In	Enter the key in the fields provided. <ul style="list-style-type: none"> • For DES, the key should be 8 characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm "Key - Out" field.
Key - Out	Enter the key in the fields provided. <ul style="list-style-type: none"> • For DES, the key should be 8 characters. • For 3DES, the key should be 24 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Encryption Algorithm "Key - In" field.
Enable Authentication	Use this checkbox to enable or disable ESP authentication for this VPN policy.
Authentication Algorithm	If you enable authentication, then use this menu to select the algorithm: <ul style="list-style-type: none"> • MD5 - the default • SHA1 - more secure
Key - In	Enter the key. <ul style="list-style-type: none"> • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - Out" field.
Key - Out	Enter the key in the fields provided. <ul style="list-style-type: none"> • For MD5, the key should be 16 characters. • For SHA-1, the key should be 20 characters. Any value is acceptable, provided the remote VPN endpoint has the same value in its Authentication Algorithm "Key - In" field.
NETBIOS Enable	Check this if you wish NETBIOS traffic to be forwarded over the VPN tunnel. The NETBIOS protocol is used by Microsoft Networking for such features as Network Neighborhood.

Using Digital Certificates for IKE Auto-Policy Authentication

Digital certificates are strings generated using encryption and authentication schemes which cannot be duplicated by anyone without access to the different values used in the production of the string. They are issued by Certification Authorities (CAs) to authenticate a person or a workstation uniquely. The CAs are authorized to issue these certificates by Policy Certification Authorities (PCAs), who are in turn certified by the Internet Policy Registration Authority (IPRA). The FWAG114 is able to use certificates to authenticate users at the end points during the IKE key exchange process.

The certificates can be obtained from a certificate server an organization might maintain internally or from the established public CAs. The certificates are produced by providing the particulars of the user being identified to the CA. The information provided may include the user's name, e-mail ID, domain name, etc.

Each CA has its own certificate. The certificates of a CA are added to the FWAG114 and can then be used to form IKE policies for the user. Once a CA certificate is added to the FWAG114 and a certificate is created for a user, the corresponding IKE policy is added to the FWAG114. Whenever the user tries to send traffic through the FWAG114, the certificates are used in place of pre-shared keys during initial key exchange as the authentication and key generation mechanism. Once the keys are established and the tunnel is set up the connection proceeds according to the VPN policy.

Certificate Revocation List (CRL)

Each Certification Authority (CA) maintains a list of the revoked certificates. The list of these revoked certificates is known as the Certificate Revocation List (CRL).

Whenever an IKE policy receives the certificate from a peer, it checks for this certificate in the CRL on the FWAG114 obtained from the corresponding CA. If the certificate is not present in the CRL it means that the certificate is not revoked. IKE can then use this certificate for authentication. If the certificate is present in the CRL it means that the certificate is revoked, and the IKE will not authenticate the client.

You must manually update the FWAG114 CRL regularly in order for the CA-based authentication process to remain valid.

Walk-Through of Configuration Scenarios on the FWAG114

There are a variety of configurations you might implement with the FWAG114. The scenarios listed below illustrate typical configurations you might use in your organization.

In order to help make it easier to set up an IPsec system, the following two scenarios are provided. These scenarios were developed by the VPN Consortium (<http://www.vpnc.org>). The goal is to make it easier to get the systems from different vendors to interoperate. NETGEAR is providing you with both of these scenarios in the following two formats:

- VPN Consortium Scenarios without Any Product Implementation Details
- VPN Consortium Scenarios Based on the FWAG114 User Interface

The purpose of providing these two versions of the same scenarios is to help you determine where the two vendors use different vocabulary. Seeing the examples presented in these different ways will reveal how systems from different vendors do the same thing.



Note: NETGEAR will publish additional interoperability scenarios with various gateway and client software products. Look on the NETGEAR web site at www.netgear.com for the HTML version of this manual. The scenarios will be published as an additional section of the on-line version of this reference manual.

VPN Consortium Scenario 1: Gateway-to-Gateway with Preshared Secrets

The following is a typical gateway-to-gateway VPN that uses a preshared secret for authentication.

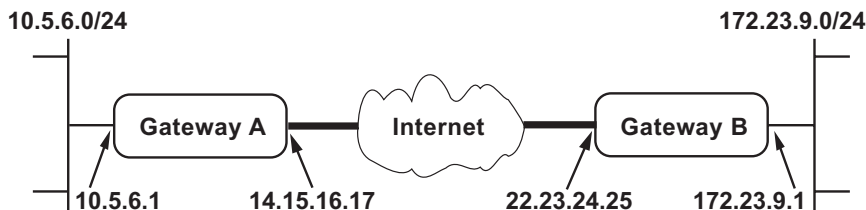


Figure 7-5: VPN Consortium Scenario 1

Gateway A connects the internal LAN 10.5.6.0/24 to the Internet. Gateway A's LAN interface has the address 10.5.6.1, and its WAN (Internet) interface has the address 14.15.16.17.

Gateway B connects the internal LAN 172.23.9.0/24 to the Internet. Gateway B's WAN (Internet) interface has the address 22.23.24.25. Gateway B's LAN interface address, 172.23.9.1, can be used for testing IPsec but is not needed for configuring Gateway A.

The IKE Phase 1 parameters used in Scenario 1 are:

- Main mode
- TripleDES
- SHA-1
- MODP group 2 (1024 bits)
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours) with no kbytes rekeying

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 2 (1024 bits)
- Perfect forward secrecy for rekeying
- SA lifetime of 3600 seconds (one hour) with no kbytes rekeying
- Selectors for all IP protocols, all ports, between 10.5.6.0/24 and 172.23.9.0/24, using IPv4 subnets

FWAG114 Scenario 1: FWAG114 to Gateway B IKE and VPN Policies

Note: This scenario assumes all ports are open on the FWAG114. You can verify this by reviewing the security settings as seen in the “Rules menu” on page 3-6.

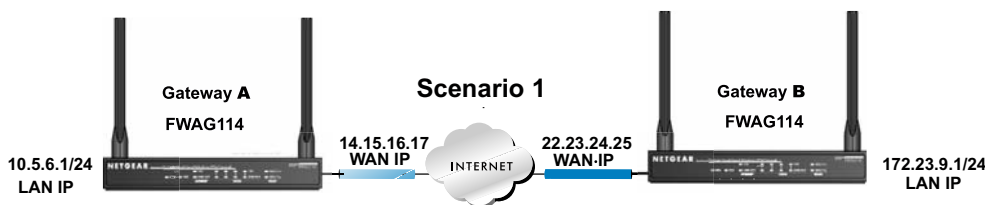


Figure 7-6: LAN to LAN VPN access from an FWAG114 to an FWAG114

Use this scenario illustration and configuration screens as a model to build your configuration.

1. Log in to the FWAG114 labeled Gateway A as in the illustration.

Log in at the default address of <http://192.168.0.1> with the default user name of **admin** and default password of **password**, or using whatever password and LAN address you have chosen.

2. Configure the WAN (Internet) and LAN IP addresses of the FWAG114.

- a. From the main menu Setup section, click on the Basic Setup link.

Basic Settings

Does Your Internet Connection Require A Login?

- ☒ No
☐ Yes

Account Name (if Required)
Domain Name (if Required)

FVL328

Internet IP Address

- ☐ Get Dynamically From ISP
☒ Use Static IP Address

IP Address

14 . 15 . 16 . 17

IP Subnet Mask

255 . 255 . 255 . 0

Gateway IP Address

10 . 1 . 1 . 13

WAN IP addresses

ISP provides these addresses

Figure 7-7: FWAG114 Internet IP Address menu

- b. Configure the WAN Internet Address according to the settings above and click Apply to save your settings. For more information on configuring the WAN IP settings in the Basic Setup topics, please see [“How to Complete a Manual Configuration”](#) on page 2-14.
- c. From the main menu Advanced section, click on the LAN IP Setup link.

LAN IP Setup

LAN TCP/IP Setup

IP Address

10

5

6

1

IP Subnet Mask

255

255

255

0

RIP Direction

None ▾

RIP Version

Disabled ▾

MTU Size

☒ Default (1500)

☐ Custom

1500

☒ **Use router as DHCP server**

Starting IP Address

10

5

6

2

Ending IP Address

10

5

6

254

Reserved IP Table

	#	IP Address	Mac Address	Device Name
<div><div>Add</div><div>Edit</div><div>Delete</div></div>				

Apply

Cancel

Figure 7-8: LAN IP configuration menu

- d. Configure the LAN IP address according to the settings above and click Apply to save your settings. For more information on LAN TCP/IP setup topics, please see [“How to Configure LAN TCP/IP Setup Settings”](#) on page 6-5.

Note: After you click Apply to change the LAN IP address settings, your workstation will be disconnected from the FWAG114. You will have to log on with *http://10.5.6.1* which is now the address you use to connect to the built-in web-based configuration manager of the FWAG114.

3. Set up the IKE Policy illustrated below on the FWAG114.

- a. From the main menu VPN section, click on the IKE Policies link, and then click the Add button to display the screen below.

IKE Policy Configuration

General

Policy Name	<input type="text" value="Scenario_1"/>
Direction/Type	<input type="button" value="Both Directions"/>
Exchange Mode	<input type="button" value="Main Mode"/>

Local

Local Identity Type	<input type="button" value="WAN IP Address"/>
Local Identity Data	<input type="text"/>

Remote

Remote Identity Type	<input type="button" value="Remote WAN IP"/>
Remote Identity Data	<input type="text"/>

IKE SA Parameters

Encryption Algorithm	<input type="button" value="3DES"/>
Authentication Algorithm	<input type="button" value="SHA-1"/>
Authentication Method	<input checked="" type="radio"/> Pre-shared Key <input type="text" value="hr5xb84l6aa9r6"/> <input type="radio"/> RSA Signature (requires Certificate)
Diffie-Hellman (DH) Group	<input type="button" value="Group 2 (1024 Bit)"/>
SA Life Time	<input type="text" value="2300"/> (secs)

<input type="button" value="Back"/>	<input type="button" value="Apply"/>	<input type="button" value="Cancel"/>
-------------------------------------	--------------------------------------	---------------------------------------

Figure 7-9: Scenario 1 IKE Policy

- b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings. For more information on IKE Policy topics, please see [“IKE Policies’ Automatic Key and Authentication Management”](#) on page 7-3.

4. Set up the FWAG114 VPN -Auto Policy illustrated below.

- a. From the main menu VPN section, click on the VPN Policies link, and then click on the Add Auto Policy button.

VPN - Auto Policy

General

Policy Name: scenario1a

IKE policy: Scenario_1

Remote VPN Endpoint: Address Type: IP Address, Address Data: 22.23.24.25 (WAN IP address)

SA Life Time: 3600 (Seconds), 0 (Kbytes)

☒ IPsec PFS, PFS Key Group: Group 2 (1024 Bit)

Traffic Selector

Local IP: Subnet address, Start IP address: 10.5.6.0, Finish IP address: 0.0.0.0, Subnet Mask: 255.255.255.0 (LAN IP addresses)

Remote IP: Subnet address, Start IP address: 172.23.9.0, Finish IP address: 0.0.0.0, Subnet Mask: 255.255.255.0 (LAN IP addresses)

AH Configuration

☐ Enable Authentication Authentication Algorithm: MD5

ESP Configuration

☒ Enable Encryption Encryption Algorithm: 3DES

☒ Enable Authentication Authentication Algorithm: SHA-1

☐ NETBIOS Enable

Back Apply Cancel

Figure 7-10: Scenario 1 VPN - Auto Policy

- b. Configure the IKE Policy according to the settings in the illustration above and click Apply to save your settings. For more information on IKE Policy topics, please see [“IKE Policies’ Automatic Key and Authentication Management”](#) on page 7-3.
5. After applying these changes, all traffic from the range of LAN IP addresses specified on FWAG114 A and FWAG114 B will flow over a secure VPN tunnel.

How to Check VPN Connections

You can test connectivity and view VPN status information on the FWAG114.

1. To test connectivity between the Gateway A FWAG114 LAN and the Gateway B LAN, follow these steps:
 - a. Using our example, from a PC attached to the FWAG114 on LAN A, on a Windows PC click the Start button on the taskbar and then click Run.
 - b. Type `ping -t 172.23.9.1`, and then click OK.
 - c. This will cause a continuous ping to be sent to the LAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.”
 - d. At this point the connection is established.
2. To test connectivity between the FWAG114 Gateway A and Gateway B WAN ports, follow these steps:
 - a. Using our example, log in to the FWAG114 on LAN A, go to the main menu Maintenance section and click the Diagnostics link.
 - b. To test connectivity to the WAN port of Gateway B, enter `22.23.24.25`, and then click Ping.
 - c. This will cause a ping to be sent to the WAN interface of Gateway B. After between several seconds and two minutes, the ping response should change from “timed out” to “reply.” You may have to run this test several times before you get the “reply” message back from the target FWAG114.
 - d. At this point the connection is established.

Note: If you want to ping the FWAG114 as a test of network connectivity, be sure the FWAG114 is configured to respond to a ping on the Internet WAN port by checking the checkbox seen in [“Rules menu” on page 3-6](#). However, to preserve a high degree of security, you should turn off this feature when you are finished with testing.
3. To view the FWAG114 event log and status of Security Associations, follow these steps:
 - a. Go to the FWAG114 main menu VPN section and click the VPN Status link.
 - b. The log screen will display a history of the VPN connections, and the IPSec SA and IKE SA tables will report the status and data transmission statistics of the VPN tunnels for each policy.

FWAG114 Scenario 2: FWAG114 to FWAG114 with RSA Certificates

The following is a typical gateway-to-gateway VPN that uses Public Key Infrastructure x.509 (PKIX) certificates for authentication. The network setup is identical to the one given in scenario 1. The IKE Phase 1 and Phase 2 parameters are identical to the ones given in scenario 1, with the exception that the identification is done with signatures authenticated by PKIX certificates.

Note: Before completing this configuration scenario, make sure the correct Time Zone is set on the FWAG114. For instructions on this topic, please see, [“How to Set Your Time Zone” on page 3-14](#).

1. Obtain a root certificate.

- a. Obtain the root certificate (which includes the public key) from a Certificate Authority (CA)

Note: The procedure for obtaining certificates differs from a CA like Verisign and a CA such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. For example, an administrator of a Windows 2000 certificate server might provide it to you via e-mail.

- b. Save the certificate as a text file called *trust.txt*.

2. Install the trusted CA certificate for the Trusted Root CA.

- a. Log in to the FWAG114.
- b. From the main menu VPN section, click on the CAs link.
- c. Click Add to add a CA.
- d. Click Browse to locate the *trust.txt* file.
- e. Click Upload.

3. Create a certificate request for the FWAG114.

- a. From the main menu VPN section, click the Certificates link.

- b. Click the Generate Request button to display the screen illustrated in [Figure 7-11](#) below.

Generate Self Certificate Request

Required	
Name	<input type="text" value="FWAG114"/>
Subject	<input type="text" value="test"/>
Hash Algorithm	<input type="button" value="SHA1"/>
Signature Algorithm	<input type="button" value="RSA"/>
Signature Key Length	<input type="button" value="1024"/>
Optional	
IP Address	<input type="text"/>
Domain Name	<input type="text"/>
E-mail Address	<input type="text"/>

Figure 7-11: Generate Self Certificate Request menu

- c. Fill in the fields on the Add Self Certificate screen.
- Required
 - Name. Enter a name to identify this certificate.
 - Subject. This is the name which other organizations will see as the holder (owner) of this certificate. This should be your registered business name or official company name. Generally, all certificates should have the same value in the Subject field.
 - Hash Algorithm. Select the desired option: MD5 or SHA1.
 - Signature Algorithm. Select the desired option: DSS or RSA.
 - Signature Key Length. Select the desired option: 512, 1024, or 2048.
 - Optional
 - IP Address. If you use “IP type” in the IKE policy, you should input the IP Address here. Otherwise, you should leave this blank.
 - Domain Name. If you have a domain name, you can enter it here. Otherwise, you should leave this blank.
 - E-mail Address. You can enter you e-mail address here.

- d. Click the Next button to continue. The FWAG114 generates a Self Certificate Request as shown below.

Self Certificate Request

Certificate Details

Subject Name	test
Hash Algorithm	SHA1
Signature Algorithm	RSA
Key Length	1024

Data to supply to CA

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBTjCBuAIBAIAjAPMQowCwYDVQQDEwROZXMOMIGfMA0GCSqGSIb3DQEBAQUAA4GN
ADCBiQKBgQC5cI30M9NZyJ2Hpvj83JEmBo+xbkjc0YVCPDop7ud+b6EYbQd0o4v
bt6pCChZTmZCk1p8yE94IB25wjcR8ntJotZP2MhEL1ItehXT11U09sUWtMwp7T1
T3Q6Q/1Jr37extkgdtHw17rhxo0wt0IJYUACvIgZ872HSp4ZT0er8wIDAQABAAAw
DQYJKoZIhvcNAQEFBQADgYEAtmMmKz0zrZeR68BieAV6FddG4WcljA840ldRdkdi
bx1TrMgYzfHv8e0simPtQML5aVXFd6iFYHOF4aXQpCitv/FLce80Gv15wqe0FIGA
c1j18mRGa70MiJtTY+Ro+PevIbs1T3B1AewTj4qWYRYk0vJ9yFIAYcRnggf+NPS/
cfU=
-----END CERTIFICATE REQUEST-----

```

Back Done Cancel

Highlight, copy and paste this data into a text file.

Figure 7-12: Self Certificate Request data

4. Transmit the Self Certificate Request data to the Trusted Root CA.

- a. Highlight the text in the Data to supply to CA area, copy it, and paste it into a text file.
- b. Give the certificate request data to the CA. In the case of a Windows 2000 internal CA, you might simply e-mail it to the CA administrator. The procedures of a CA like Verisign and a CA such as a Windows 2000 certificate server administrator will differ. Follow the procedures of your CA.

- c. When you have finished gathering the Self Certificate Request data, click the Done button. You will return to the Certificates screen where your pending “FWAG114” Self Certificate Request will be listed, as illustrated in Figure 7-13 below.

Certificates

Active Self Certificates

#	Name	Subject Name	Issuer Name	Expiry Time
<input checked="" type="radio"/> 1	Netgear	FQDN: netgear.com	/O=VPNC/OU=Conformance testing root 1	Mar 26 22:53:29 2011 GMT

Self Certificate Requests

#	Name	Status
<input checked="" type="radio"/> 1	FWAG114	Waiting for Certificate upload

Figure 7-13: Self Certificate Requests table

5. Receive the certificate back from the Trusted Root CA and save it as a text file.

Note: In the case of a Windows 2000 internal CA, the CA administrator might simply email it to back to you. Follow the procedures of your CA. Save the certificate you get back from the CA as a text file called *final.txt*.

6. Upload the new certificate.

- a. From the main menu VPN section, click on the Certificates link.
- b. Click the radio button of the Self Certificate Request you want to upload.
- c. Click the Upload Certificate button.
- d. Browse to the location of the file you saved in step 5 above which contains the certificate from the CA.
- e. Click the Upload button.

- f. You will now see the “FWAG114” entry in the Active Self Certificates table and the pending “FWAG114” Self Certificate Request is gone, as illustrated below.

Certificates

Active Self Certificates

#	Name	Subject Name	Issuer Name	Expiry Time
1	Netgear	FQDN: netgear.com	/O=VPNC/OU=Conformance testing root 1	Mar 26 22:53:29 2011 GMT
2	FWAG	/CN=test	/C=FI/O=SSH Communications Security/OU=Web test/CN=Test CA 1	Dec 1 00:00:00 2003 GMT

Self Certificate Requests

#	Name	Status
---	------	--------

Figure 7-14: Self Certificates table

7. Associate the new certificate and the Trusted Root CA certificate on the FWAG114.

- a. Create a new IKE policy called **Scenario_2** with all the same properties of **Scenario_1** (see “[Scenario 1 IKE Policy](#)” on page 6-19) except now use the RSA Signature instead of the shared key.

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Authentication Method: ☐ Pre-shared Key ☒ RSA Signature (requires Certificate)

Diffie-Hellman (DH) Group:

SA Life Time: (secs)

Figure 7-15: IKE policy using RSA Signature

- b. Create a new VPN Auto Policy called **scenario2a** with all the same properties as **scenario1a** except that it uses the IKE policy called Scenario_2.

Now, the traffic from devices within the range of the LAN subnet addresses on FWAG114 A and Gateway B will be authenticated using the certificates rather than via a shared key.

8. Set up Certificate Revocation List (CRL) checking.

- a. Get a copy of the CRL from the CA and save it as a text file.

Note: The procedure for obtaining a CRL differs from a CA like Verisign and a CA such as a Windows 2000 certificate server, which an organization operates for providing certificates for its members. Follow the procedures of your CA.

- b. From the main menu VPN section, click on the CRL link.
- c. Click Add to add a CRL.
- d. Click Browse to locate the CRL file.
- e. Click Upload.

Now expired or revoked certificates will not be allowed to use the VPN tunnels managed by IKE policies which use this CA.

Note: You must update the CRLs regularly in order to maintain the validity of the certificate-based VPN policies.

Chapter 8

Advanced Configuration

This chapter describes how to configure the advanced features of your ProSafe Dual Band Wireless VPN Firewall FWAG114. These features can be found under the Advanced heading in the Main Menu of the browser interface.

How to Configure 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, which will allow you to register your domain to their IP address, and will forward traffic directed to your domain to your frequently-changing IP address.

The router 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 router, whenever your ISP-assigned IP address changes, your router will automatically contact your dynamic DNS service provider, log in to your account, and register your new IP address.

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



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

Using the LAN IP Setup Options

The second feature category under the Advanced heading is LAN IP Setup. This 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 below.

LAN IP Setup

LAN TCP/IP Setup

IP Address: 192 . 168 . 0 . 1

IP Subnet Mask: 255 . 255 . 255 . 0

RIP Direction: Both ▼

RIP Version: RIP-1 ▼

☒ **Use Router As DHCP Server**

Starting IP Address: 192 . 168 . 0 . 2

Ending IP Address: 192 . 168 . 0 . 50

Address Reservation

#	IP Address	Device Name	MAC Address

Add Edit Delete

Apply Cancel

Figure 8-1: LAN IP Setup Menu

Configuring LAN TCP/IP Setup Parameters

The router is shipped preconfigured to use private IP addresses on the LAN side, and to act as a DHCP server. The router'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 router.
- **IP Subnet Mask**
This is the LAN Subnet Mask of the router. 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 router sends and receives RIP packets. Both is the default.
 - When set to Both or Out Only, the router 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. RIP-2B uses subnet broadcasting.



Note: If you change the LAN IP address of the router 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.

Using the Router as a DHCP server

By default, the router 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 router. 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 router 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.

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 router’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 router 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 router’s LAN IP address)
- Primary DNS Server (if you entered a Primary DNS address in the Basic Settings menu; otherwise, the router’s LAN IP address)
- Secondary DNS Server (if you entered a Secondary DNS address in the Basic Settings menu)

Using Address Reservation

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 router’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.

Configuring Static Routes

Static Routes provide additional routing information to your router. Under normal circumstances, the router 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 Route menu, shown below.

IP Static Routes

#	Name	Destination	Gateway
1	isdn_rtr	134.177.0.0	192.168.0.100
2	-
3	-
4	-
5	-
6	-
7	-
8	-

Edit

Figure 8-2. Static Route Summary Table

To add or edit a Static Route:

1. Click the Add button to open the Add/Edit Menu, shown below.

Static Routes

Route Name	<input type="text" value="isdn_rtr"/>			
<input checked="" type="checkbox"/> Active	<input checked="" type="checkbox"/> Private			
Destination IP Address	<input type="text" value="134"/>	<input type="text" value="177"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
IP Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Gateway IP Address	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="0"/>	<input type="text" value="100"/>
Metric	<input type="text" value="2"/>			

Figure 8-3. Static Route Entry and Edit Menu

2. Type a route name for this static route in the Route Name box under the table.
(This is for identification purpose only.)
3. Select Private if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Select Active to make this route effective.
5. Type the Destination IP Address of the final destination.
6. Type the IP Subnet Mask for this destination.
If the destination is a single host, type 255.255.255.255.
7. Type the Gateway IP Address, which must be a router on the same LAN segment as the router.
8. Type a number between 1 and 15 as the Metric value.
This represents the number of routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click Apply to have the static route entered into the table.

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 router, 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 router 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 router that 134.177.0.0 should be accessed through the ISDN router at 192.168.0.100. The static route would look like [Figure 8-3](#).

In this example:

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

Enabling Remote Management Access

Using the Remote Management page, you can allow a user or users on the Internet to configure, upgrade and check the status of your FWAG114 wireless 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 router for Remote Management:

1. Select the Turn Remote Management On check box.
2. Specify what external addresses will be allowed to access the router's remote management.

Note: For enhanced security, 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.

Note: 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, you must enter in your browser:

`http://134.177.0.123:8080`

Chapter 9

Troubleshooting

This chapter gives information about troubleshooting your ProSafe Dual Band Wireless VPN Firewall FWAG114. After each problem description, instructions are provided to help you diagnose and solve the problem.

Basic Functioning

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

1. When power is first applied, verify that the PWR LED is on.
2. After approximately 10 seconds, verify that:
 - a. The TEST LED is not lit.
 - b. The LAN port LEDs are lit for any local ports that are connected.
 - c. The Internet port LED is lit.
 - d. The Wireless 802.11a is off and the LED is *not* lit until the country selection has been set.

If a port's LED is lit, a link has been established to the connected device. If a LAN port is connected to a 100 Mbps device, verify that the port's LED is green. If the port is 10 Mbps, the LED will be amber.

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 router is turned on:

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

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

LEDs Never Turn Off

When the router is turned on, the LEDs turn on for about 10 seconds and then turn off. If all the LEDs stay on, there is a fault within the router.

If all LEDs are still on one minute after power up:

- Cycle the power to see if the router recovers.
- Clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in [“Restoring the Default Configuration and Password” on page 7-7](#).

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

LAN or Internet Port LEDs Not On

If either the LAN LEDs or Internet LED do not light when the Ethernet connection is made, check the following:

- Make sure that the Ethernet cable connections are secure at the router and at the hub or workstation.
- Make sure that power is turned on to the connected hub or workstation.
- Be sure you are using the correct cable:

When connecting the router'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 router's Web Configuration interface from a PC on your local network, check the following:

- Check the Ethernet connection between the PC and the router as described in the previous section.
- Make sure your PC's IP address is on the same subnet as the router. 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 4](#) 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 router and reboot your PC.

- If your router's IP address has been changed and you don't know the current IP address, clear the router's configuration to factory defaults. This will set the router's IP address to 192.168.0.1. This procedure is explained in [“Restoring the Default Configuration and Password” on page 7-7](#).
- 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 router 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 router is unable to access the Internet, you should first determine whether the router is able to obtain a WAN IP address from the ISP. Unless you have been assigned a static IP address, your router must request an IP address from the ISP. You can determine whether the request was successful using the Web Configuration Manager.

To check the WAN IP address:

1. Launch your browser and select an external site such as www.netgear.com
2. Access the Main Menu of the router'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 router has not obtained an IP address from your ISP.

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

1. Turn off power to the cable or DSL modem.
2. Turn off power to your router.
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 router.

If your router 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 router's MAC address.

OR

Configure your router to spoof your PC's MAC address. This can be done in the Basic Settings menu. Refer to [“Manually Configuring Your Internet Connection” on page 3-12](#).

If your router 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 router'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 router configured as its TCP/IP gateway.

If your PC obtains its information from the router 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 your PC or workstation.

Testing the LAN Path to Your Router

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

To ping the router 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 router, 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 [“LAN or Internet Port LEDs Not On”](#) on [page 9-2](#).
 - 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 router.
- 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 router 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 router 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 router 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 router to “clone” or “spoof” the MAC address from the authorized PC. Refer to [“Manually Configuring Your Internet Connection” on page 3-12](#).

Restoring the Default Configuration and Password

This section explains how to restore the factory default configuration settings, changing the router’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 router (see [“Erasing the Configuration” on page 5-8](#)).
- Use the Default Reset button on the rear panel of the router. Use this method for cases when the administration password or IP address is not known.

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 router.

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 router 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 FWAG114 wireless 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 router 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 router, wait at least five minutes and check the date and time again.
- Time is off by one hour. Cause: The router 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 ProSafe Dual Band Wireless VPN Firewall FWAG114.

Network Protocol and Standards Compatibility

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

Power Adapter

North America: 120V, 60 Hz, input
United Kingdom, Australia: 240V, 50 Hz, input
Europe: 230V, 50 Hz, input
Japan: 100V, 50/60 Hz, input
All regions (output): 12 V DC @ 1.2 A output, 18W maximum

Physical Specifications

Dimensions: 28 x 175 x 118 mm (1.1 x 6.89 x 4.65 in.)
Weight: 0.3 kg (0.66 lb)

Environmental Specifications

Operating temperature: 0° to 40° C (32° to 104° F)
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

LAN: 10BASE-T or 100BASE-Tx, RJ-45
 WAN: 10BASE-T or 100BASE-Tx

Wireless

Data Encoding:	Direct Sequence Spread Spectrum (DSSS)		
Maximum Computers Per Wireless Network:	Limited by the amount of wireless network traffic generated by each node. Typically 30-70 nodes.		
802.11b and g Radio Data Rate	1, 2, 5.5, & 11 Mbps (Auto-rate capable)		
802.11b and g Operating Frequencies	2.412 ~ 2.462 GHz (US) 2.412 ~ 2.484 GHz (Japan) 2.412 ~ 2.472 GHz (Europe ETSI)	2.457 ~ 2.462 GHz (Spain) 2.457 ~ 2.472 GHz (France)	
802.11b and g Operating Range		Outdoor environment	Indoor environment
	@ 11 Mbps	398 ft (120 m)	198 ft (60 m)
	@ 5.5 Mbps	561 ft (170 m)	264 ft (80 m)
	@ 2 Mbps	890 ft (270 m)	430 ft (130 m)
	@ 1 Mbps	1485 ft (450 m)	660 ft (200 m)
802.11b and g Encryption	40-bits (also called 64-bits), 128-bits WEP data encryption		
802.11a Radio Data Rate	6, 9, 12, 18, 24, 36, 48, 54, & 108 Mbps turbo mode (Turbo mode is available only for models shipped in the United States, Canada, and Australia)		
802.11a Operating Frequency	5.15 ~ 5.25 GHz (lower band) 5.25 ~ 5.35 GHz (middle band) 5.725 ~ 5.825 GHz (hi-band)		
802.11a Operating Range		Outdoor environment	Indoor environment
	@ 54 Mbps	100 ft (30.5 m)	60 ft (18.3 m)
	@ 6 Mbps	1200 ft (366 m)	300 ft (91.4 m)
802.11a Encryption	40-bits (also called 64-bits), 128-bits, 152-bits WEP data encryption		

Appendix B

Network, Routing, Firewall, and Basics

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

Related Publications

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

Basic Router Concepts

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

What is a Router?

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

Routers vary in performance and scale, number of routing protocols supported, and types of physical WAN connection they support. The ProSafe Dual Band Wireless VPN Firewall FWAG114 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 FWAG114 wireless firewall supports both the older RIP-1 and the newer RIP-2 protocols. Among other improvements, RIP-2 supports subnet and multicast protocols. RIP is not required for most home applications.

IP Addresses and the Internet

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

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

For example, the following binary address:

```
11000011 00100010 00001100 00000111
```

is normally written as:

195.34.12.7

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

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

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

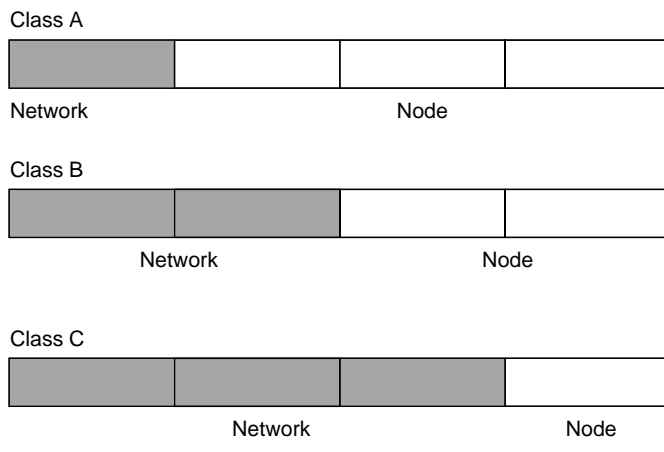


Figure 9-1: Three Main Address Classes

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 9-2: 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 192.68.135.126, 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 9-1. 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 9-2. Netmask Formats

Dotted-Decimal	Masklength
255.0.0.0	/8
255.255.0.0	/16

Table 9-2. Netmask Formats

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

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

Choose your private network number from this range. The DHCP server of the FWAG114 wireless firewall is preconfigured to automatically assign private addresses.

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

Single IP Address Operation Using NAT

In the past, if multiple PCs on a LAN needed to access the Internet simultaneously, you had to obtain a range of IP addresses from the ISP. This type of Internet account is more costly than a single-address account typically used by a single user with a modem, rather than a router. The FWAG114 wireless 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.

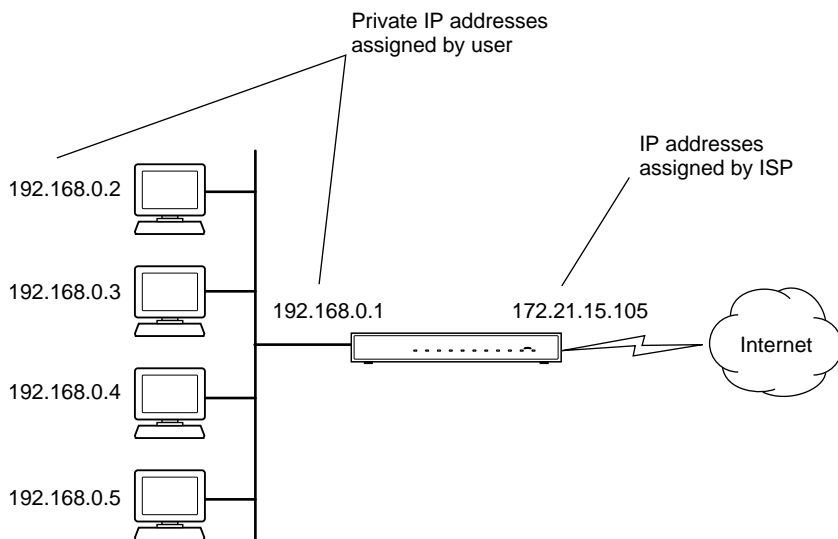


Figure 9-3: Single IP Address Operation Using NAT

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.

Related Documents

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

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

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

Domain Name Server

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

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

IP Configuration by DHCP

When an IP-based local area network is installed, each PC must be configured with an IP address. If the PCs need to access the Internet, they should also be configured with a gateway address and one or more DNS server addresses. As an alternative to manual configuration, there is a method by which each PC on the network can automatically obtain this configuration information. A device on the network may act as a Dynamic Host Configuration Protocol (DHCP) server. The DHCP server stores a list or pool of IP addresses, along with other information (such as gateway and DNS addresses) that it may assign to the other devices on the network. The FWAG114 wireless firewall has the capacity to act as a DHCP server.

The FWAG114 wireless 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 process, the network behind the 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.

Ethernet Cabling

Although Ethernet networks originally used thick or thin coaxial cable, most installations currently use unshielded twisted pair (UTP) cabling. The UTP cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. A normal straight-through UTP Ethernet cable follows the EIA568B standard wiring and pinout as described in [Table 9-1](#).

Table 9-1. UTP Ethernet cable wiring, straight-through

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

Uplink Switches, Crossover Cables, and MDI/MDIX Switching

In the wiring table above, the concept of transmit and receive are from the perspective of the PC, which is wired as Media Dependant Interface (MDI). In this wiring, the PC transmits on pins 1 and 2. At the hub, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X).

When connecting a PC to a PC, or a hub port to another hub port, the transmit pair must be exchanged with the receive pair. This exchange is done by one of two mechanisms. 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.

The FWAG114 wireless firewall incorporates Auto Uplink™ technology (also called MDI/MDIX). Each LOCAL Ethernet port will automatically sense whether the Ethernet cable plugged into the port should have a normal connection (e.g. connecting to a PC) or an uplink connection (e.g. connecting to a router, switch, or hub). That port will then configure itself to the correct configuration. This feature also eliminates the need to worry about crossover cables, as Auto Uplink™ will accommodate either type of cable to make the right connection.

Cable Quality

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

Appendix C

Preparing Your Network

This appendix describes how to prepare your network to connect to the Internet through the ProSafe Dual Band Wireless VPN Firewall FWAG114 and how to verify the readiness of broadband Internet service from an Internet service provider (ISP).



Note: If an ISP technician configured your computer during the installation of a broadband modem, or if you configured it using instructions provided by your ISP, you may need to copy the current configuration information for use in the configuration of your firewall. Write down this information before reconfiguring your computers. Refer to [“Obtaining ISP Configuration Information for Windows Computers”](#) on [page C-19](#) or [“Obtaining ISP Configuration Information for Macintosh Computers”](#) on [page C-20](#) for further information.

Preparing Your Computers for TCP/IP Networking

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

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

- Windows® 95 or later includes the software components for establishing a TCP/IP network.
- Windows 3.1 does not include a TCP/IP component. You need to purchase a third-party TCP/IP application package such as NetManage Chameleon.
- Macintosh Operating System 7 or later includes the software components for establishing a TCP/IP network.
- All versions of UNIX or Linux include TCP/IP components. Follow the instructions provided with your operating system or networking software to install TCP/IP on your computer.

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

The FWAG114 wireless firewall is shipped preconfigured as a DHCP server. The firewall assigns the following TCP/IP configuration information automatically when the PCs are rebooted:

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

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

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

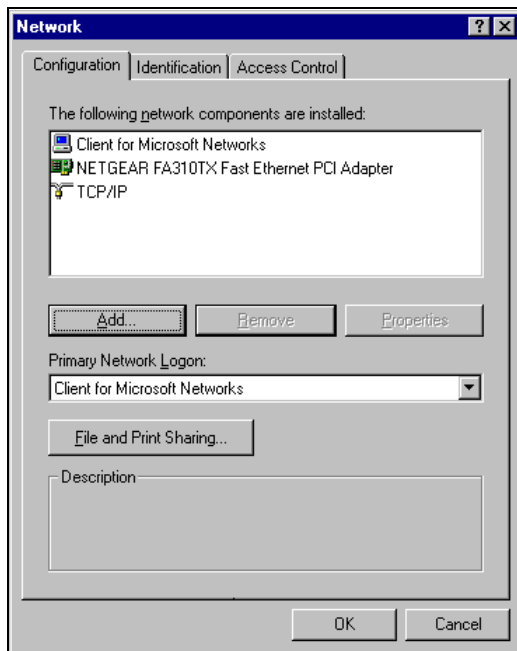
As part of the PC preparation process, you need to manually install and configure TCP/IP on each networked PC. Before starting, locate your Windows CD; you may need to insert it during the TCP/IP installation process.

Install or Verify Windows Networking Components

To install or verify the necessary components for IP networking:

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

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



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



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

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

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

If you need TCP/IP:

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

If you need Client for Microsoft Networks:

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

Enabling DHCP to Automatically Configure TCP/IP Settings

After the TCP/IP protocol components are installed, each PC must be assigned specific information about itself and resources that are available on its network. The simplest way to configure this information is to allow the PC to obtain the information from a DHCP server in the network.

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

1

Locate your **Network Neighborhood** icon.

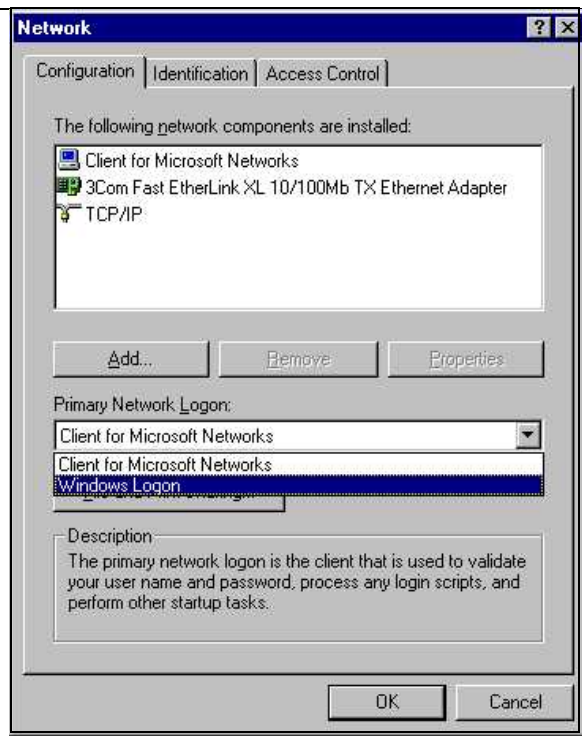
- If the Network Neighborhood icon is on the Windows desktop, position your mouse pointer over it and right-click your mouse button.
- If the icon is not on the desktop,
 - Click **Start** on the task bar located at the bottom left of the window.
 - Choose **Settings**, and then **Control Panel**.
 - Locate the **Network Neighborhood** icon and click on it. This will open the Network panel as shown below.

2

Verify the following settings as shown:

- Client for Microsoft Network exists
- Ethernet adapter is present
- TCP/IP is present
- **Primary Network Logon** is set to Windows logon

Click on the **Properties** button. The following TCP/IP Properties window will display.

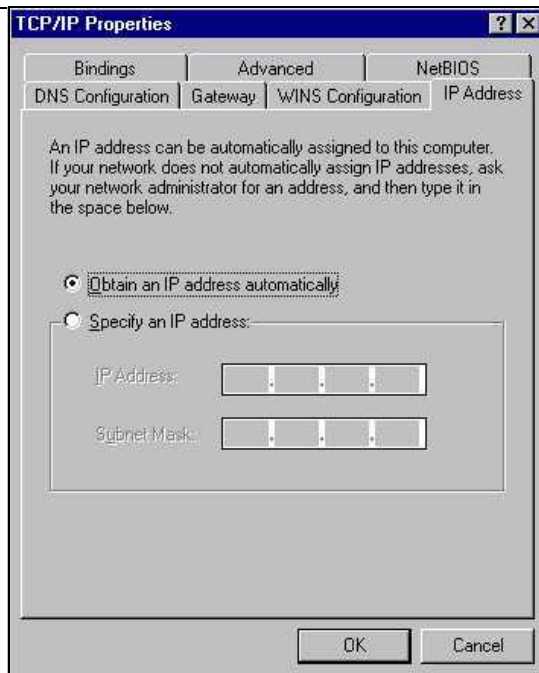


3

- By default, the **IP Address** tab is open on this window.
- Verify the following:
 - Obtain an IP address automatically** is selected. If not selected, click in the radio button to the left of it to select it. This setting is required to enable the DHCP server to automatically assign an IP address.
 - Click **OK** to continue.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Selecting Windows' Internet Access Method

1. On the Windows taskbar, click the Start button, point to Settings, and then click Control Panel.
2. Double-click the Internet Options icon.
3. Select "I want to set up my Internet connection manually" or "I want to connect through a Local Area Network" and click Next.
4. Select "I want to connect through a Local Area Network" and click Next.
5. Uncheck all boxes in the LAN Internet Configuration screen and click Next.
6. Proceed to the end of the Wizard.

Verifying TCP/IP Properties

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

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

2. Type **winipcfg**, and then click OK.

The IP Configuration window opens, which lists (among other things), your IP address, subnet mask, and default gateway.

3. From the drop-down box, select your Ethernet adapter.

The window is updated to show your settings, which should match the values below if you are using the default TCP/IP settings that NETGEAR recommends for connecting through a router or gateway:

- 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 NT4, 2000 or XP for IP Networking

As part of the PC preparation process, you may need to 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. Then, restart your PC.

Enabling DHCP to Automatically Configure TCP/IP Settings

You will find there are many similarities in the procedures for different Windows systems when using DHCP to configure TCP/IP.

The following steps will walk you through the configuration process for each of these versions of Windows.

DHCP Configuration of TCP/IP in Windows XP

1

Locate your **Network Neighborhood** icon.

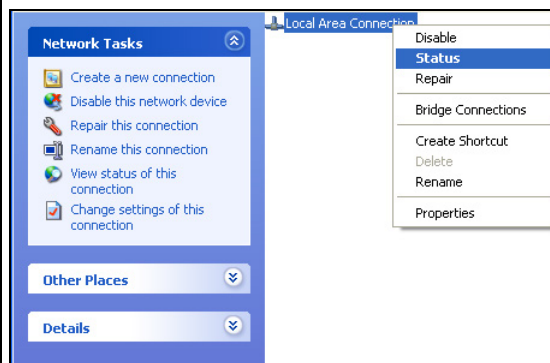
- Select **Control Panel** from the Windows XP new Start Menu.
- Select the **Network Connections** icon on the Control Panel. This will take you to the next step.

2

- Now the Network Connection window displays.

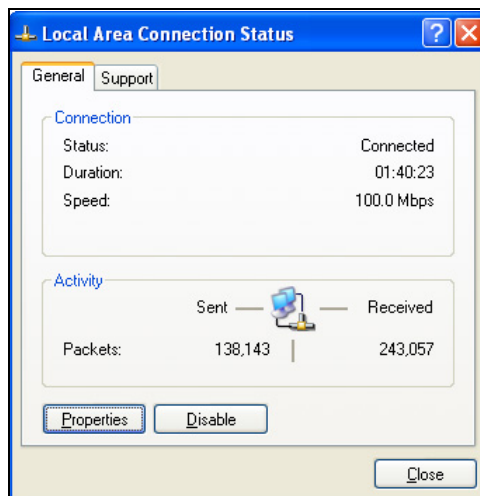
The Connections List that shows all the network connections set up on the PC, located to the right of the window.

- Right-click on the **Connection** you will use and choose **Status**.



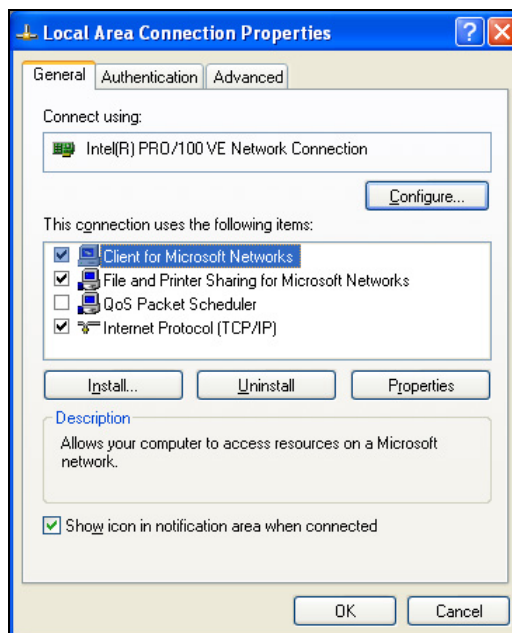
3

- Now you should be at the Local Area Network Connection Status window. This box displays the connection status, duration, speed, and activity statistics.
- Administrator logon access rights are needed to use this window.
- Click the **Properties** button to view details about the connection.



4

- The TCP/IP details are presented on the Support tab page.
- Select **Internet Protocol**, and click **Properties** to view the configuration information.

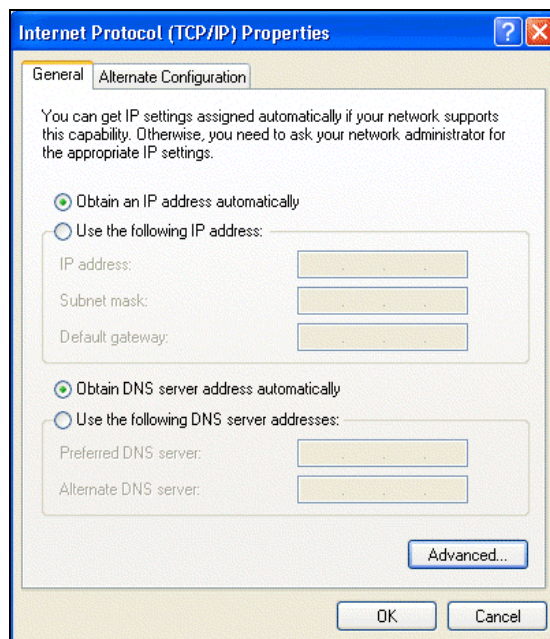


5

- Verify that the **Obtain an IP address automatically** radio button is selected.
- Verify that **Obtain DNS server address automatically** radio button is selected.
- Click the **OK** button.

This completes the DHCP configuration of TCP/IP in Windows XP.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows 2000

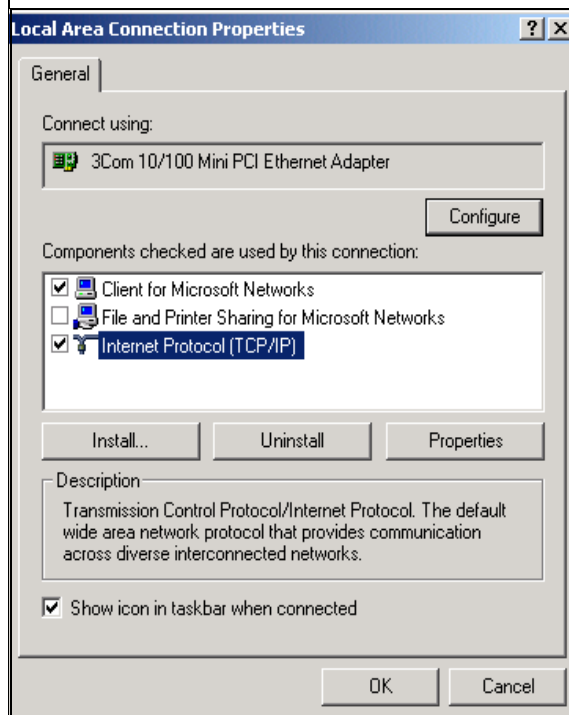
Once again, after you have installed the network card, TCP/IP for Windows 2000 is configured. TCP/IP should be added by default and set to DHCP without your having to configure it. However, if there are problems, follow these steps to configure TCP/IP with DHCP for Windows 2000.

1

- Click on the **My Network Places** icon on the Windows desktop. This will bring up a window called Network and Dial-up Connections.
- Right click on **Local Area Connection** and select **Properties**.

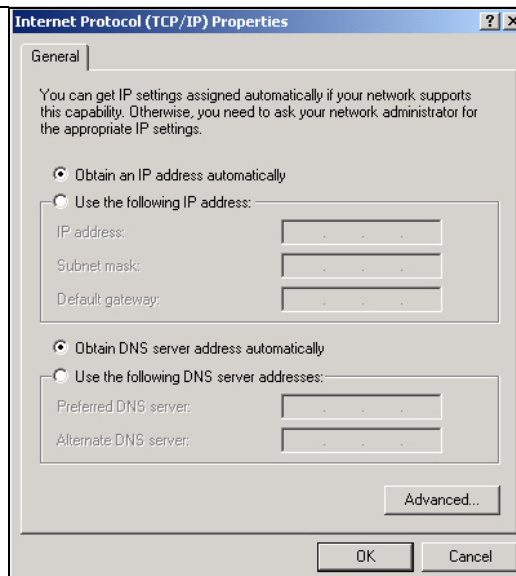
2

- The **Local Area Connection Properties** dialog box appears.
- Verify that you have the correct Ethernet card selected in the **Connect using:** box.
- Verify that at least the following two items are displayed and selected in the box of “Components checked are used by this connection:”
 - Client for Microsoft Networks and
 - Internet Protocol (TCP/IP)
- Click **OK**.



3

- With Internet Protocol (TCP/IP) selected, click on **Properties** to open the Internet Protocol (TCP/IP) Properties dialogue box.
- Verify that
 - **Obtain an IP address automatically** is selected.
 - **Obtain DNS server address automatically** is selected.
- Click **OK** to return to Local Area Connection Properties.

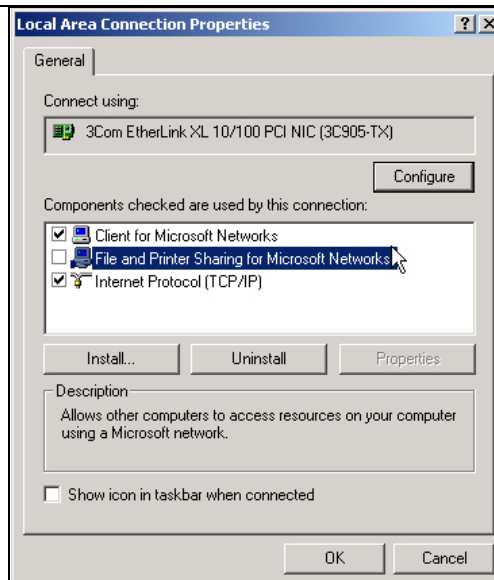


4

- Click **OK** again to complete the configuration process for Windows 2000.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



DHCP Configuration of TCP/IP in Windows NT4

Once you have installed the network card, you need to configure the TCP/IP environment for Windows NT 4.0. Follow this procedure to configure TCP/IP with DHCP in Windows NT 4.0.

1

- Choose **Settings** from the Start Menu, and then select **Control Panel**. This will display Control Panel window.

2

- Double-click the **Network** icon in the Control Panel window.

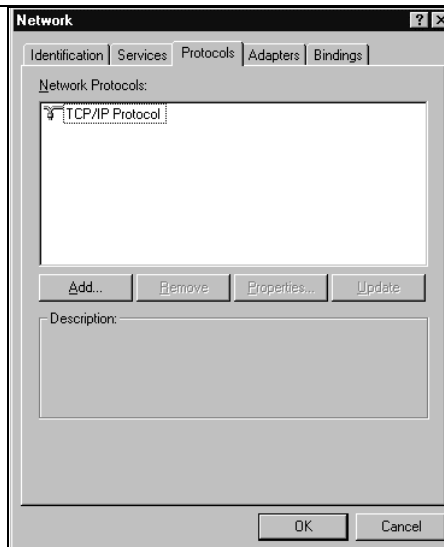
The Network panel will display.

- Select the **Protocols** tab to continue.



3

- Highlight the **TCP/IP Protocol** in the **Network Protocols** box, and click on the **Properties** button.

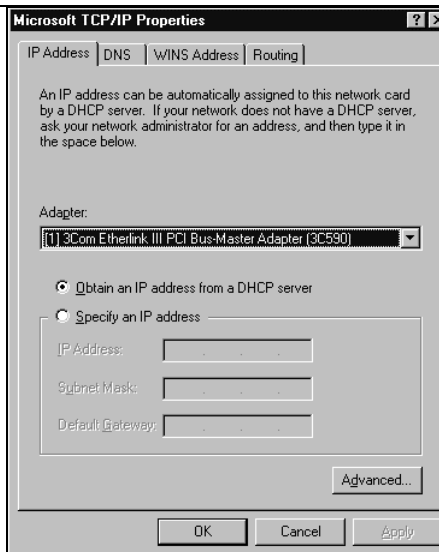


4

- The **TCP/IP Properties** dialog box now displays.
- Click the **IP Address** tab.
- Select the radio button marked **Obtain an IP address from a DHCP server**.
- Click **OK**. This completes the configuration of TCP/IP in Windows NT.

Restart the PC.

Repeat these steps for each PC with this version of Windows on your network.



Verifying TCP/IP Properties for Windows XP, 2000, and NT4

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 for connecting through a router or gateway:

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

- The default gateway is 192.168.0.1

4. Type **exit**

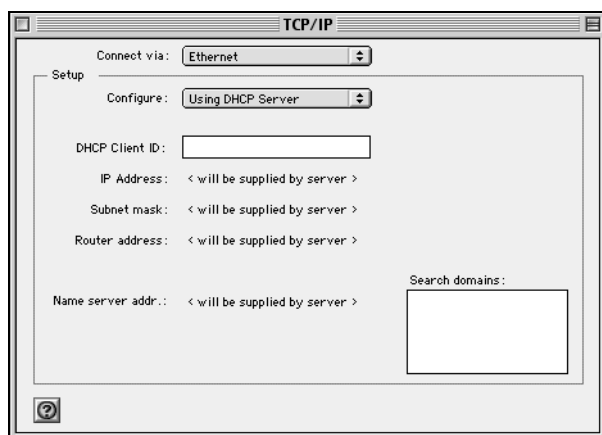
Configuring the Macintosh for TCP/IP Networking

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

MacOS 8.6 or 9.x

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

The TCP/IP Control Panel opens:



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

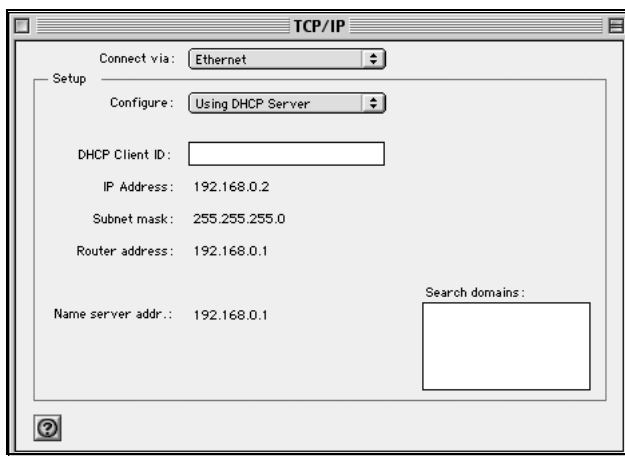
MacOS X

1. From the Apple menu, choose System Preferences, then Network.

2. If not already selected, select Built-in Ethernet in the Configure list.
3. If not already selected, Select Using DHCP in the TCP/IP tab.
4. Click Save.

Verifying TCP/IP Properties for Macintosh Computers

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



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

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

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

Verifying the Readiness of Your Internet Account

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

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

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

Are Login Protocols Used?

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

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

What Is Your Configuration Information?

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

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

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

`mail.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 the configuration information from your PC's Network TCP/IP Properties window or Macintosh TCP/IP Control Panel before reconfiguring your PC for use with the firewall. These procedures are described next.

Obtaining ISP Configuration Information for Windows Computers

As mentioned above, you may need to collect configuration information from your PC so that you can use this information when you configure the FWAG114 wireless firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

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

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

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

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

The TCP/IP Properties dialog box opens.

4. Select the IP Address tab.

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

5. Select the Gateway tab.

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

6. Select the DNS Configuration tab.

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

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

You are returned to the Network window.

8. Click OK.

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

Obtaining ISP Configuration Information for Macintosh Computers

As mentioned above, you may need to collect configuration information from your Macintosh so that you can use this information when you configure the FWAG114 wireless firewall. Following this procedure is only necessary when your ISP does not dynamically supply the account information.

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

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

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

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

Restarting the Network

Once you've set up your computers to work with the firewall, you must reset the network for the devices to be able to communicate correctly. Restart any computer that is connected to the FWAG114 wireless firewall.

After configuring all of your computers for TCP/IP networking and restarting them, and connecting them to the local network of your FWAG114 wireless firewall, you are ready to access and configure the firewall.

Appendix D

Wireless Networking Basics

This chapter provides an overview of Wireless networking.

Wireless Networking Overview

The FWAG114 wireless firewall conforms to the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard for wireless LANs (WLANs) and a product update will bring the FWAG114 into conformance to the 802.11g standard when it is ratified. On an 802.11b or g 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 802.11b 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 802.11g auto rate sensing rates are 1, 2, 5.5, 6, 9, 12, 18, 24, 36, 48, and 54 Mbps. Likewise, the 802.11a wireless link offers a maximum data rate of 54 Mbps, but will automatically back down to rates 48, 36, 24, 18, 12, 9, and 6 Mbps.

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

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.

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.

Network Name: 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 ESSID is used, but may still be referred to as SSID.

An SSID is a thirty-two character (maximum) alphanumeric key identifying the name of 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.

The ESSID is usually broadcast in the air from an access point. The wireless station sometimes can be configured with the ESSID **ANY**. This means the wireless station will try to associate with whichever access point has the stronger radio frequency (RF) signal, providing that both the access point and wireless station use Open System authentication.

Authentication and WEP Data 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 these two types of authentication methods:

- **Open System.** With Open System authentication, a wireless PC can join any network and receive any messages that are not encrypted.
- **Shared Key.** 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 used when the wireless devices are configured to operate in Shared Key authentication mode.

802.11 Authentication

The 802.11 standard defines several services that govern how two 802.11 devices communicate. The following events must occur before an 802.11 Station can communicate with an Ethernet network through an access point such as the one built in to the FWAG114:

1. Turn on the wireless station.
2. The station listens for messages from any access points that are in range.
3. The station finds a message from an access point that has a matching SSID.
4. The station sends an authentication request to the access point.
5. The access point authenticates the station.
6. The station sends an association request to the access point.
7. The access point associates with the station.
8. The station can now communicate with the Ethernet network through the access point.

An access point must authenticate a station before the station can associate with the access point or communicate with the network. The IEEE 802.11 standard defines two types of authentication: Open System and Shared Key.

- Open System Authentication allows any device to join the network, assuming that the device SSID matches the access point SSID. Alternatively, the device can use the “ANY” SSID option to associate with any available Access Point within range, regardless of its SSID.
- Shared Key Authentication requires that the station and the access point have the same WEP Key to authenticate. These two authentication procedures are described below.

Open System Authentication

The following steps occur when two devices use Open System Authentication:

1. The station sends an authentication request to the access point.
2. The access point authenticates the station.
3. The station associates with the access point and joins the network.

This process is illustrated in below.

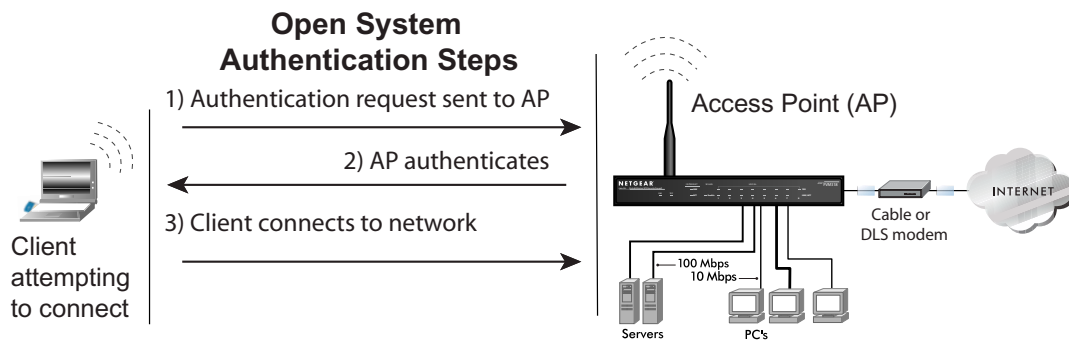


Figure 9-4: Open system authentication

Shared Key Authentication

The following steps occur when two devices use Shared Key Authentication:

1. The station sends an authentication request to the access point.
2. The access point sends challenge text to the station.

3. The station uses its configured 64-bit or 128-bit default key to encrypt the challenge text, and sends the encrypted text to the access point.
4. The access point decrypts the encrypted text using its configured WEP Key that corresponds to the station's default key. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, then the access point and the station share the same WEP Key and the access point authenticates the station.
5. The station connects to the network.

If the decrypted text does not match the original challenge text (i.e., the access point and station do not share the same WEP Key), then the access point will refuse to authenticate the station and the station will be unable to communicate with either the 802.11 network or Ethernet network.

This process is illustrated in below.

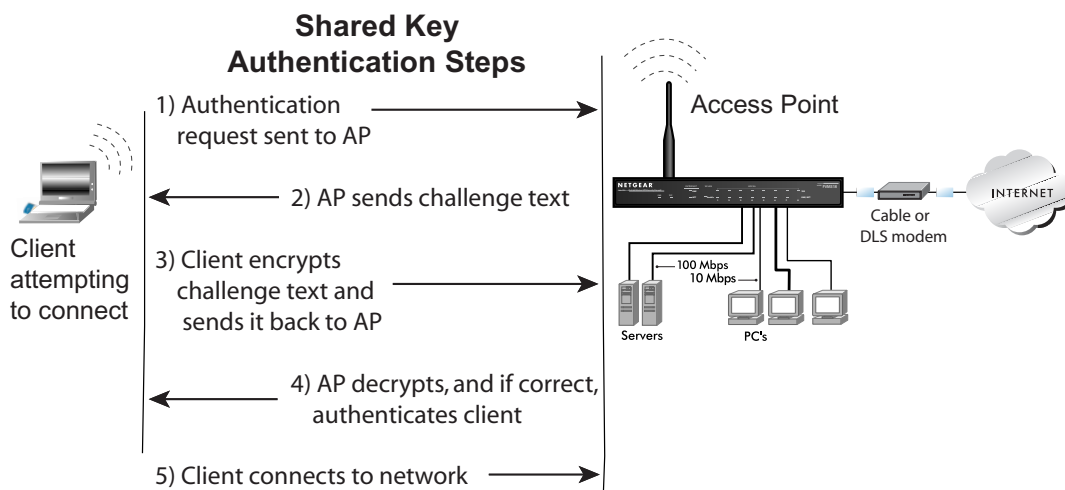


Figure 9-5: Shared key authentication

Overview of WEP Parameters

Before enabling WEP on an 802.11 network, you must first consider what type of encryption you require and the key size you want to use. Typically, there are three WEP Encryption options available for 802.11 products:

1. **Do Not Use WEP:** The 802.11 network does not encrypt data. For authentication purposes, the network uses Open System Authentication.

2. Use WEP for Encryption: A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the network uses Open System Authentication.

3. Use WEP for Authentication and Encryption: A transmitting 802.11 device encrypts the data portion of every packet it sends using a configured WEP Key. The receiving device decrypts the data using the same WEP Key. For authentication purposes, the wireless network uses Shared Key Authentication.

Note: Some 802.11 access points also support **Use WEP for Authentication Only** (Shared Key Authentication without data encryption).

Key Size

The IEEE 802.11 standard supports two types of WEP encryption: 40-bit and 128-bit.

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.

128-bit encryption is stronger than 40-bit encryption, but 128-bit encryption may not be available outside of the United States due to U.S. export regulations.

In NETGEAR's 802.11a solutions, there are three shared key methods implemented: the standards based 40-bit and 128-bit WEP data encryption; and an extended 152-bit WEP data encryption.

When configured for 40-bit encryption, 802.11 products typically support up to four WEP Keys. Each 40-bit WEP Key is expressed as 5 sets of two hexadecimal digits (0-9 and A-F). For example, "12 34 56 78 90" is a 40-bit WEP Key.

When configured for 128-bit encryption, 802.11 products typically support four WEP Keys but some manufacturers support only one 128-bit key. The 128-bit WEP Key is expressed as 13 sets of two hexadecimal digits (0-9 and A-F). For example, “12 34 56 78 90 AB CD EF 12 34 56 78 90” is a 128-bit WEP Key.

Table D-1: Encryption Key Sizes

Encryption Key Size	# of Hexadecimal Digits	Example of Hexadecimal Key Content
64-bit (24+40)	10	4C72F08AE1
128-bit (24+104)	26	4C72F08AE19D57A3FF6B260037
152-bit (24+128)	32	4C72F08AE19D57A3FF6B26003715DAC2

Note: Typically, 802.11 access points can store up to four 128-bit WEP Keys but some 802.11 client adapters can only store one. Therefore, make sure that your 802.11 access and client adapters configurations match.

WEP Configuration Options

The WEP settings must match on all 802.11 devices that are within the same wireless network as identified by the SSID. In general, if your mobile clients will roam between access points, then all of the 802.11 access points and all of the 802.11 client adapters on the network must have the same WEP settings.

Note: Whatever keys you enter for an AP, you must also enter the same keys for the client adapter in the same order. In other words, WEP key 1 on the AP must match WEP key 1 on the client adapter, WEP key 2 on the AP must match WEP key 2 on the client adapter, etc.

Note: The AP and the client adapters can have different default WEP Keys as long as the keys are in the same order. In other words, the AP can use WEP key 2 as its default key to transmit while a client adapter can use WEP key 3 as its default key to transmit. The two devices will communicate as long as the AP’s WEP key 2 is the same as the client’s WEP key 2 and the AP’s WEP key 3 is the same as the client’s WEP key 3.

Wireless Channels

The wireless frequencies used by 802.11a and 802.11b/g networks are different. These channel frequency options are discussed below.

802/11b/g Wireless Channels

IEEE 802.11b/g wireless nodes communicate with each other using radio frequency signals in the ISM (Industrial, Scientific, and Medical) band between 2.4 GHz and 2.5 GHz. Neighboring channels are 5 MHz apart. However, due to spread spectrum effect of the signals, a node sending signals using a particular channel will utilize frequency spectrum 12.5 MHz 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 in 802.11b/g networks are listed in [Table D-2](#):

Table D-2: 802.11b/g Radio Frequency Channels

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

Note: The available channels supported by the wireless products in various countries are different. For example, Channels 1 to 11 are supported in the U.S. and Canada, and Channels 1 to 13 are supported in Europe and Australia.

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.

802/11a Legal Power Output and Wireless Channels

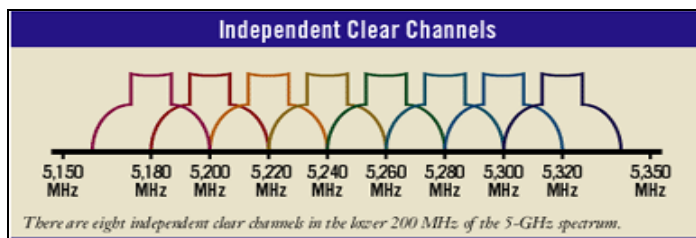
IEEE 802.11a utilizes 300 MHz of bandwidth in the 5 GHz Unlicensed National Information Infrastructure (U-NII) band. Though the lower 200 MHz is physically contiguous, the FCC has divided the total 300 MHz into three distinct domains, each with a different legal maximum power output. Below is a table of summary for different regulatory domains.

Table D-3: 802.11a Radio Frequency Channels

U-NII Band	Low	Middle	High
Frequency (GHz)	5.15 – 5.25	5.25 – 5.35	5.725 – 5.825
Max. Power Output	50 mW for US 200 mW for Canada, Europe, and Australia	250 mW for US 200 mW for Europe and Australia 1 W for Canada	1 W for US and Australia 4 W for Canada 25 mW for Europe

Note: Please check your local Authority for updated information on the available frequency and maximum power output.

IEEE 802.11a uses Orthogonal Frequency Division Multiplexing (OFDM), a new encoding scheme that offers certain benefits over a spread spectrum in channel availability and data rate. The 802.11a uses OFDM to define a total of 8 non-overlapping 20 MHz channels across the 2 lower bands; each of these is divided into 52 sub carriers and each carrier is approximately 300 KHz wide.



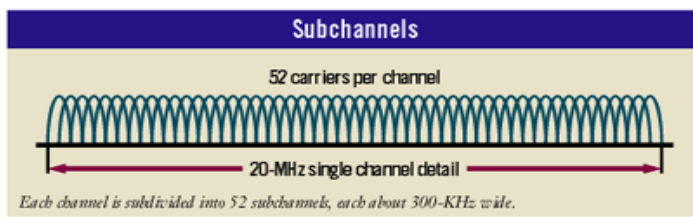


Figure 4-6: IEEE 802.11a Channel Allocations

The FWAG114 user can use thirteen channels in **non-turbo** mode.

Table D-1: 802.11a Turbo Mode Off Radio Frequency Channels

Turbo Mode OFF	
Channel	Frequency
36	
40	
44	
48	
52	
56	
60	
64	
149	5.745 GHz
153	5.765 GHz
157	5.785 GHz
161	5.805 GHz
165	5.825 GHz

The FWAG114 user can use five channels in turbo mode.

Turbo Mode ON	
Channel	Frequency
42	5.21 GHz
50	5.25 GHz
58	5.29 GHz
152	5.76 GHz
160	5.8 GHz

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

Appendix E

Virtual Private Networking

There have been many improvements in the Internet including Quality of Service, network performance, and inexpensive technologies, such as DSL. But one of the most important advances has been in Virtual Private Networking (VPN) Internet Protocol security (IPSec). IPSec is one of the most complete, secure, and commercially available, standards-based protocols developed for transporting data.

What is a VPN?

A VPN is a shared network where private data is segmented from other traffic so that only the intended recipient has access. The term VPN was originally used to describe a secure connection over the Internet. Today, however, VPN is also used to describe private networks, such as Frame Relay, Asynchronous Transfer Mode (ATM), and Multiprotocol Label Switching (MPLS).

A key aspect of data security is that the data flowing across the network is protected by encryption technologies. Private networks lack data security, which allows data attackers to tap directly into the network and read the data. IPSec-based VPNs use encryption to provide data security, which increases the network's resistance to data tampering or theft.

IPSec-based VPNs can be created over any type of IP network, including the Internet, Frame Relay, ATM, and MPLS, but only the Internet is ubiquitous and inexpensive.

VPNs are traditionally used for:

- **Intranets:** Intranets connect an organization's locations. These locations range from the headquarters offices, to branch offices, to a remote employee's home. Often this connectivity is used for e-mail and for sharing applications and files. While Frame Relay, ATM, and MPLS accomplish these tasks, the shortcomings of each limits connectivity. The cost of connecting home users is also very expensive compared to Internet-access technologies, such as DSL or cable. Because of this, organizations are moving their networks to the Internet, which is inexpensive, and using IPSec to create these networks.
- **Remote Access:** Remote access enables telecommuters and mobile workers to access e-mail and business applications. A dial-up connection to an organization's modem pool is one method of access for remote workers, but is expensive because the organization must pay the associated long distance telephone and service costs. Remote access VPNs greatly reduce expenses by enabling mobile workers to dial a local Internet connection and then set up a secure IPSec-based VPN communications to their organization.
- **Extranets:** Extranets are secure connections between two or more organizations. Common uses for extranets include supply-chain management, development partnerships, and subscription services. These undertakings can be difficult using legacy network technologies due to connection costs, time delays, and access availability. IPSec-based VPNs are ideal for extranet connections. IPSec-capable devices can be quickly and inexpensively installed on existing Internet connections.

What Is IPSec and How Does It Work?

IPSec is an Internet Engineering Task Force (IETF) standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks. IPSec provides data security at the IP packet level. A packet is a data bundle that is organized for transmission across a network, and includes a header and payload (the data in the packet). IPSec emerged as a viable network security standard because enterprises wanted to ensure that data could be securely transmitted over the Internet. IPSec protects against possible security exposures by protecting data while in transit.

IPSec Security Features

IPSec is the most secure method commercially available for connecting network sites. IPSec was designed to provide the following security features when transferring packets across networks:

- **Authentication:** Verifies that the packet received is actually from the claimed sender.
- **Integrity:** Ensures that the contents of the packet did not change in transit.

- **Confidentiality:** Conceals the message content through encryption.

IPSec Components

IPSec contains the following elements:

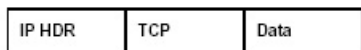
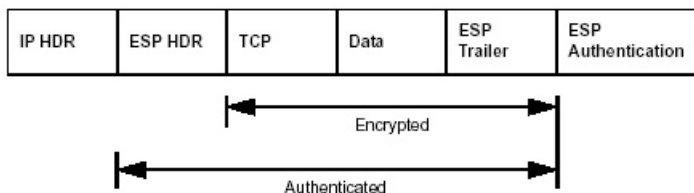
- **Encapsulating Security Payload (ESP):** Provides confidentiality, authentication, and integrity.
- **Authentication Header (AH):** Provides authentication and integrity.
- **Internet Key Exchange (IKE):** Provides key management and Security Association (SA) management.

Encapsulating Security Payload (ESP)

ESP provides authentication, integrity, and confidentiality, which protect against data tampering and, most importantly, provide message content protection.

IPSec provides an open framework for implementing industry standard algorithms, such as SHA and MD5. The algorithms IPSec uses produce a unique and unforgeable identifier for each packet, which is a data equivalent of a fingerprint. This fingerprint allows the device to determine if a packet has been tampered with. Furthermore, packets that are not authenticated are discarded and not delivered to the intended receiver.

ESP also provides all encryption services in IPSec. Encryption translates a readable message into an unreadable format to hide the message content. The opposite process, called decryption, translates the message content from an unreadable format to a readable message. Encryption/decryption allows only the sender and the authorized receiver to read the data. In addition, ESP has an option to perform authentication, called ESP authentication. Using ESP authentication, ESP provides authentication and integrity for the payload and not for the IP header.

Original Packet*Packet with IPSec Encapsulating Security Payload (ESP)***Figure 4-7: Original packet and packet with IPSec Encapsulated Security Payload**

The ESP header is inserted into the packet between the IP header and any subsequent packet contents. However, because ESP encrypts the data, the payload is changed. ESP does not encrypt the ESP header, nor does it encrypt the ESP authentication.

Authentication Header (AH)

AH provides authentication and integrity, which protect against data tampering, using the same algorithms as ESP. AH also provides optional anti-replay protection, which protects against unauthorized retransmission of packets. The authentication header is inserted into the packet between the IP header and any subsequent packet contents. The payload is not touched.

Although AH protects the packet's origin, destination, and contents from being tampered with, the identity of the sender and receiver is known. In addition, AH does not protect the data's confidentiality. If data is intercepted and only AH is used, the message contents can be read. ESP protects data confidentiality. For added protection in certain cases, AH and ESP can be used together. In the following table, IP HDR represents the IP header and includes both source and destination IP addresses.

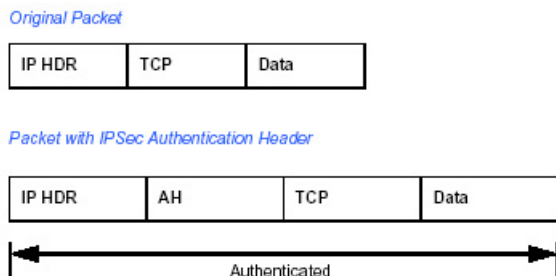


Figure 4-8: Original packet and packet with IPSec Authentication Header

IKE Security Association

IPSec introduces the concept of the Security Association (SA). An SA is a logical connection between two devices transferring data. An SA provides data protection for unidirectional traffic by using the defined IPSec protocols. An IPSec tunnel typically consists of two unidirectional SAs, which together provide a protected, full-duplex data channel.

The SAs allow an enterprise to control exactly what resources may communicate securely, according to security policy. To do this an enterprise can set up multiple SAs to enable multiple secure VPNs, as well as define SAs within the VPN to support different departments and business partners.

Mode

SAs operate using modes. A mode is the method in which the IPSec protocol is applied to the packet. IPSec can be used in tunnel mode or transport mode. Typically, the tunnel mode is used for gateway-to-gateway IPSec tunnel protection, while transport mode is used for host-to-host IPSec tunnel protection. A gateway is a device that monitors and manages incoming and outgoing network traffic and routes the traffic accordingly. A host is a device that sends and receives network traffic.

- **Transport Mode:** The transport mode IPSec implementation encapsulates only the packet's payload. The IP header is not changed. After the packet is processed with IPSec, the new IP packet contains the old IP header (with the source and destination IP addresses unchanged) and the processed packet payload. Transport mode does not shield the information in the IP header; therefore, an attacker can learn where the packet is coming from and where it is going to. The previous packet diagrams show a packet in transport mode.

- **Tunnel Mode:** The tunnel mode IPSec implementation encapsulates the entire IP packet. The entire packet becomes the payload of the packet that is processed with IPSec. A new IP header is created that contains the two IPSec gateway addresses. The gateways perform the encapsulation/decapsulation on behalf of the hosts. Tunnel mode ESP prevents an attacker from analyzing the data and deciphering it, as well as knowing who the packet is from and where it is going.

Note: AH and ESP can be used in both transport mode or tunnel mode.

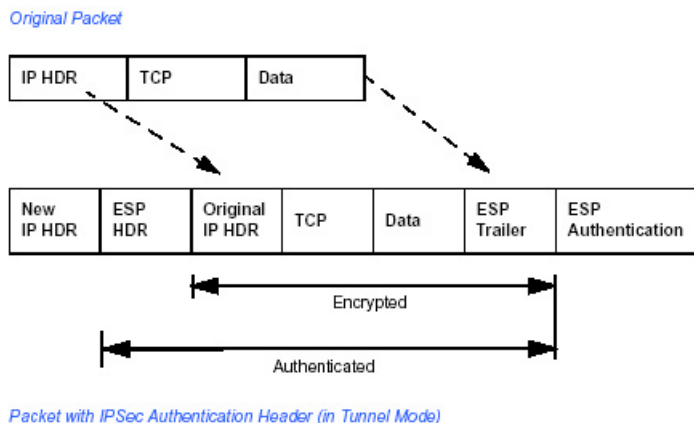


Figure 4-9: Original packet and packet with IPSec ESP in Tunnel mode

Key Management

IPSec uses the Internet Key Exchange (IKE) protocol to facilitate and automate the SA setup and the exchange of keys between parties transferring data. Using keys ensures that only the sender and receiver of a message can access it.

IPSec requires that keys be re-created, or refreshed, frequently so that the parties can communicate securely with each other. IKE manages the process of refreshing keys; however, a user can control the key strength and the refresh frequency. Refreshing keys on a regular basis ensures data confidentiality between sender and receiver.

Understand the Process Before You Begin

This TechNote provides case studies on how to configure a secure IPSec VPN tunnels. This document assumes the reader has a working knowledge of NETGEAR management systems.

NETGEAR is a member of the VPN Consortium, a group formed to facilitate IPSec VPN vendor interoperability. The VPN Consortium has developed specific scenarios to aid system administrators in the often confusing process of connecting two different vendor implementations of the IPSec standard. The case studies in this TechNote follow the addressing and configuration mechanics defined by the VPN Consortium. Additional information regarding inter-vendor interoperability may be found at <http://www.vpnc.org/interop.html>.

It is a good idea to gather all the necessary information required to establish a VPN before you begin the configuration process. You should understand whether the firmware is up to date, all of the addresses that will be necessary, and all of the parameters that need to be set on both sides. Try to understand any incompatibilities before you begin, so that you minimize any potential complications which may arise from normal firewall or WAN processes.

If you are not a full-time system administrator, it is a good idea to familiarize yourself with the mechanics of a VPN. The brief description in this TechNote will help. Other good sources include:

- The NETGEAR VPN Tutorial – http://www.netgear.com/planetvpn/pvpn_2.html
- The VPN Consortium – <http://www.vpnc.org/>
- The VPN bibliography in “Additional Reading“ on page E-12.

VPN Process Overview

Even though IPSec is standards-based, each vendor has its own set of terms and procedures for implementing the standard. Because of these differences, it may be a good idea to review some of the terms and the generic processes for connecting two gateways before diving into to the specifics.

Network Interfaces and Addresses

The VPN gateway is aptly named because it functions as a “gatekeeper” for each of the computers connected on the Local Area Network behind it.

In most cases, each Gateway will have a “public” facing address (WAN side) and a “private” facing address (LAN side). These addresses are referred to as the “network interface” in documentation regarding the construction of VPN communication. Please note that the addresses used in the example.

Interface Addressing

This TechNote uses example addresses provided the VPN Consortium. It is important to understand that you will be using addresses specific to the devices that you are attempting to connect via IPSec VPN.

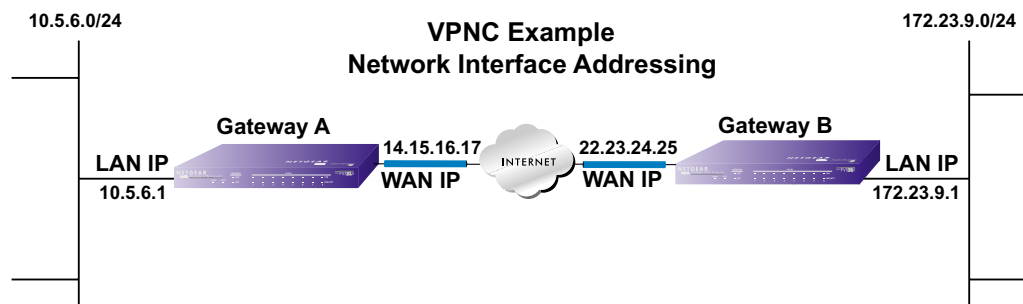


Figure 4-10: VPNC Example Network Interface Addressing

It is also important to make sure the addresses do not overlap or conflict. That is, each set of addresses should be separate and distinct.

Table 4-1. WAN (Internet/Public) and LAN (Internal/Private) Addressing

Gateway	LAN or WAN	VPNC Example Address
Gateway A	LAN (Private)	10.5.6.1
Gateway A	WAN (Public)	14.15.16.17

Table 4-1. WAN (Internet/Public) and LAN (Internal/Private) Addressing

Gateway	LAN or WAN	VPNC Example Address
Gateway B	LAN (Private)	22.23.24.25
Gateway B	WAN (Public)	172.23.9.1

It will also be important to know the subnet mask of both gateway LAN Connections. Use the worksheet in Appendix A to gather the necessary address and subnet mask information to aid in the configuration and troubleshooting process.

Table 4-2. Subnet Addressing

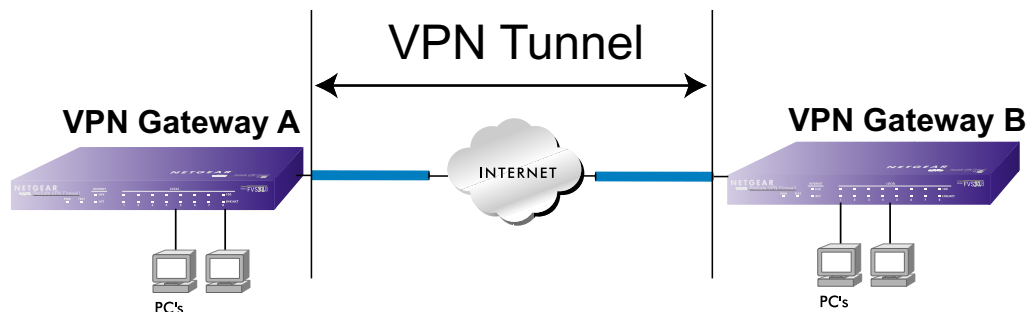
Gateway	LAN or WAN	Interface Name	Example Subnet Mask
Gateway A	LAN (Private)	Subnet Mask A	255.255.255.0
Gateway B	LAN (Private)	Subnet Mask B	255.255.255.0

Firewalls

It is important to understand that many gateways are also firewalls. VPN tunnels cannot function properly if firewall settings disallow all incoming traffic. Please refer to the firewall instructions for both gateways to understand how to open specific protocols, ports, and addresses that you intend to allow.

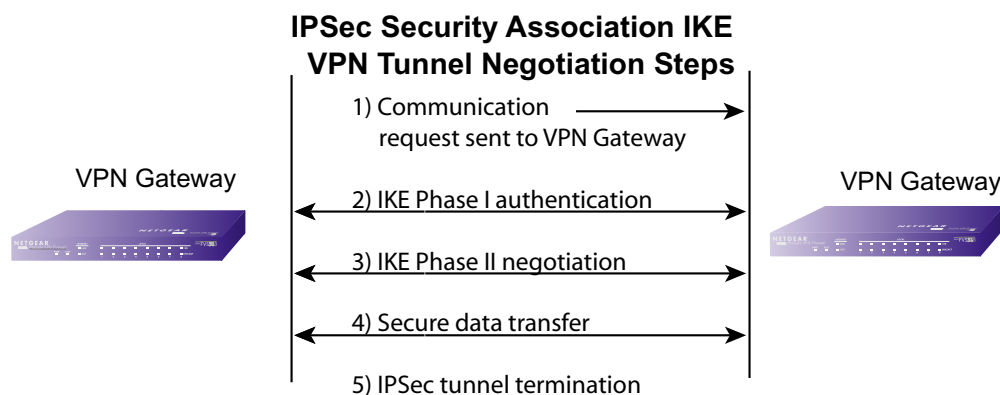
Setting Up a VPN Tunnel Between Gateways

A SA, frequently called a tunnel, is the set of information that allows two entities (networks, PCs, routers, firewalls, gateways) to “trust each other” and communicate securely as they pass information over the Internet.

**Figure 4-11: VPN Tunnel SA**

The SA contains all the information necessary for gateway A to negotiate a secure and encrypted communication stream with gateway B. This communication is often referred to as a “tunnel.” The gateways contain this information so that it does not have to be loaded onto every computer connected to the gateways.

Each gateway must negotiate its Security Association with another gateway using the parameters and processes established by IPSec. As illustrated below, the most common method of accomplishing this process is via the Internet Key Exchange (IKE) protocol which automates some of the negotiation procedures. Alternatively, you can configure your gateways using manual key exchange, which involves manually configuring each parameter on both gateways.

**Figure 4-12: IPSec SA negotiation**

1. **The IPSec software on Host A initiates the IPSec process in an attempt to communicate with Host B.** The two computers then begin the Internet Key Exchange (IKE) process.

2. IKE Phase I.

- a. The two parties negotiate the encryption and authentication algorithms to use in the IKE SAs.
- b. The two parties authenticate each other using a predetermined mechanism, such as preshared keys or digital certificates.
- c. A shared master key is generated by the Diffie-Hellman Public key algorithm within the IKE framework for the two parties. The master key is also used in the second phase to derive IPSec keys for the SAs.

3. IKE Phase II.

- a. The two parties negotiate the encryption and authentication algorithms to use in the IPSec SAs.
 - b. The master key is used to derive the IPSec keys for the SAs. Once the SA keys are created and exchanged, the IPSec SAs are ready to protect user data between the two VPN gateways.
4. **Data transfer.** Data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.
5. **IPSec tunnel termination.** IPSec SAs terminate through deletion or by timing out.

VPNC IKE Security Parameters

It is important to remember that both gateways must have the identical parameters set for the process to work correctly. The settings in these TechNote examples follow the examples given for Scenario 1 of the VPN Consortium.

VPNC IKE Phase I Parameters

The IKE Phase 1 parameters used:

- Main mode
- TripleDES
- SHA-1
- MODP group 1
- pre-shared secret of "hr5xb84l6aa9r6"
- SA lifetime of 28800 seconds (eight hours)

VPNC IKE Phase II Parameters

The IKE Phase 2 parameters used in Scenario 1 are:

- TripleDES
- SHA-1
- ESP tunnel mode
- MODP group 1
- Perfect forward secrecy for rekeying
- SA lifetime of 28800 seconds (one hour)

Testing and Troubleshooting

Once you have completed the VPN configuration steps you can use PCs, located behind each of the gateways, to ping various addresses on the LAN-side of the other gateway.

You can troubleshoot connections using the VPN status and log details on the Netgear gateway to determine if IKE negotiation is working. Common problems encountered in setting up VPNs include:

- Parameters may be configured differently on Gateway A vs. Gateway B.
- Two LANs set up with similar or overlapping addressing schemes.
- So many required configuration parameters mean errors such as mistyped information or mismatched parameter selections on either side are more likely to happen.

Additional Reading

- *Building and Managing Virtual Private Networks*, Dave Kosiur, Wiley & Sons; ISBN: 0471295264
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick and Steven M. Bellovin, Addison-Wesley; ISBN: 0201633574
- *VPNs A Beginners Guide*, John Mains, McGraw Hill; ISBN: 0072191813
- [FF98] Floyd, S., and Fall, K., Promoting the Use of End-to-End Congestion Control in the Internet. IEEE/ACM Transactions on Networking, August 1999.

Relevant RFCs listed numerically:

- [RFC 791] *Internet Protocol DARPA Internet Program Protocol Specification*, Information Sciences Institute, USC, September 1981.
- [RFC 1058] *Routing Information Protocol*, C Hedrick, Rutgers University, June 1988.
- [RFC 1483] *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, Juha Heinanen, Telecom Finland, July 1993.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol, RFC 2401, November 1998.
- [RFC 2407] D. Piper, The Internet IP Security Domain of Interpretation for ISAKMP, November 1998.
- [RFC 2474] K. Nichols, S. Blake, F. Baker, D. Black, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers, December 1998.
- [RFC 2475] S. Blake, D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, An Architecture for Differentiated Services, December 1998.
- [RFC 2481] K. Ramakrishnan, S. Floyd, A Proposal to Add Explicit Congestion Notification (ECN) to IP, January 1999.
- [RFC 2408] D. Maughan, M. Schertler, M. Schneider, J. Turner, Internet Security Association and Key Management Protocol (ISAKMP).
- [RFC 2409] D. Harkins, D. Carrel, Internet Key Exchange (IKE) protocol.
- [RFC 2401] S. Kent, R. Atkinson, Security Architecture for the Internet Protocol.

List of Glossary Terms

Use the list below to find definitions for technical terms used in this manual.

10BASE-T

IEEE 802.3 specification for 10 Mbps Ethernet over twisted pair wiring.

100BASE-Tx

IEEE 802.3 specification for 100 Mbps Ethernet over twisted pair wiring.

802.1x

802.1x defines port-based, network access control used to provide authenticated network access and automated data encryption key management.

The IEEE 802.1x draft standard offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1x uses a protocol called EAP (Extensible Authentication Protocol) and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. For details on EAP specifically, refer to IETF's RFC 2284.

802.11b

IEEE specification for wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz.

802.11g

A soon to be ratified IEEE specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.5GHz. 802.11g is backwards compatible with 802.11b.

ADSL

Short for asymmetric digital subscriber line, a technology that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

ARP

Address Resolution Protocol, a TCP/IP protocol used to convert an IP address into a physical address (called a DLC address), such as an Ethernet address.

A host wishing to obtain a physical address broadcasts an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address. There is also Reverse ARP (RARP) which can be used by a host to discover its IP address. In this case, the host broadcasts its physical address and a RARP server replies with the host's IP address.

Auto Uplink

Auto Uplink™ technology (also called MDI/MDIX) eliminates the need to worry about crossover vs. straight-through Ethernet cables. Auto Uplink™ will accommodate either type of cable to make the right connection.

CA

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

Cat 5

Category 5 unshielded twisted pair (UTP) cabling. An Ethernet network operating at 10 Mb/s (10BASE-T) will often tolerate low quality cables, but at 100 Mb/s (10BASE-Tx) the cable must be rated as Category 5, or Cat 5 or Cat V, by the Electronic Industry Association (EIA).

This rating will be printed on the cable jacket. Cat 5 cable contains eight conductors, arranged in four twisted pairs, and terminated with an RJ45 type connector. In addition, there are restrictions on maximum cable length for both 10 and 100 Mb/s networks.

Certificate Authority

A Certificate Authority is a trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs.

The role of the CA in this process is to guarantee that the individual granted the unique certificate is, in fact, who he or she claims to be. Usually, this means that the CA has an arrangement with a financial institution, such as a credit card company, which provides it with information to confirm an individual's claimed identity. CAs are a critical component in data security and electronic commerce because they guarantee that the two parties exchanging information are really who they claim to be.

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.

DMZ

Specifying a Default DMZ Server allows you to set up a computer or server that is available to anyone on the Internet for services that you haven't defined. There are security issues with doing this, so only do this if you'll be willing to risk open access.

DNS

Short for Domain Name System (or Service), an Internet service that translates domain names into IP addresses.

Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name `www.example.com` might translate to `198.105.232.4`. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

Domain Name

A descriptive name for an address or group of addresses on the Internet. Domain names are of the form of a registered entity name plus one of a number of predefined top level suffixes such as `.com`, `.edu`, `.uk`, etc. For example, in the address `mail.NETGEAR.com`, `mail` is a server name and `NETGEAR.com` is the domain.

DSL

Short for digital subscriber line, but is commonly used in reference to the asymmetric version of this technology (ADSL) that allows data to be sent over existing copper telephone lines at data rates of from 1.5 to 9 Mbps when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate).

ADSL requires a special ADSL modem. ADSL is growing in popularity as more areas around the world gain access.

Dynamic Host Configuration Protocol

DHCP. An Ethernet protocol specifying how a centralized DHCP server can assign network configuration information to multiple DHCP clients. The assigned information includes IP addresses, DNS addresses, and gateway (router) addresses.

EAP

Extensible Authentication Protocol is a general protocol for authentication that supports multiple authentication methods.

EAP, an extension to PPP, supports such authentication methods as token cards, Kerberos, one-time passwords, certificates, public key authentication and smart cards. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server such as RADIUS. The server asks the AP for proof of identity, which the AP gets from the user and then sends back to the server to complete the authentication. EAP is defined by RFC 2284.

ESSID

The Extended Service Set Identification (ESSID) is a thirty-two character (maximum) alphanumeric key identifying the wireless local area network.

Gateway

A local device, usually a router, that connects hosts on a local network to other networks.

IP

Internet Protocol is the main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

IP Address

A four-byte number uniquely defining each host on the Internet, usually written in dotted-decimal notation with periods separating the bytes (for example, 134.177.244.57).

Ranges of addresses are assigned by Internic, an organization formed for this purpose.

ISP

Internet service provider.

Internet Protocol

The main internetworking protocol used in the Internet. Used in conjunction with the Transfer Control Protocol (TCP) to form TCP/IP.

LAN

A communications network serving users within a limited area, such as one floor of a building.

local area network

LAN. A communications network serving users within a limited area, such as one floor of a building.

A LAN typically connects multiple personal computers and shared network devices such as storage and printers. Although many technologies exist to implement a LAN, Ethernet is the most common for connecting personal computers.

MAC address

The Media Access Control address is a unique 48-bit hardware address assigned to every network interface card. Usually written in the form 01:23:45:67:89:ab.

Mbps

Megabits per second.

MD5

MD5 creates digital signatures using a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

When using a one-way hash function, one can compare a calculated message digest against the message digest that is decrypted with a public key to verify that the message hasn't been tampered with. This comparison is called a "hashcheck."

MDI/MDIX

In cable wiring, the concept of transmit and receive are from the perspective of the PC, which is wired as a Media Dependant Interface (MDI). In MDI wiring, a PC transmits on pins 1 and 2. At the hub, switch, router, or access point, the perspective is reversed, and the hub receives on pins 1 and 2. This wiring is referred to as Media Dependant Interface - Crossover (MDI-X). See also Auto Uplink.

NAT

A technique by which several hosts share a single IP address for access to the Internet.

NetBIOS

Network Basic Input Output System. An application programming interface (API) for sharing services and information on local-area networks (LANs). Provides for communication between stations of a network where each station is given a name. These names are alphanumeric names, 16 characters in length.

netmask

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.

A number that explains which part of an IP address comprises the network address and which part is the host address on that network. It can be expressed in dotted-decimal notation or as a number appended to the IP address. For example, a 28-bit mask starting from the MSB can be shown as 255.255.255.192 or as /28 appended to the IP address.

Network Address Translation

A technique by which several hosts share a single IP address for access to the Internet.

packet

A block of information sent over a network. A packet typically contains a source and destination network address, some protocol and length information, a block of data, and a checksum.

Point-to-Point Protocol

PPP. A protocol allowing a computer using TCP/IP to connect directly to the Internet.

RADIUS

Short for Remote Authentication Dial-In User Service, RADIUS is an authentication system.

Using RADIUS, you must enter your user name and password before gaining access to a network. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

RIP

A protocol in which routers periodically exchange information with one another so that they can determine minimum distance paths between sources and destinations.

router

A device that forwards data between networks. An IP router forwards data based on IP source and destination addresses.

SSID

A Service Set Identification is a thirty-two character (maximum) alphanumeric key identifying a 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.

This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name. *See also* Wireless Network Name and ESSID.

Subnet Mask

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.

TLS

Short for Transport Layer Security, TLS is a protocol that guarantees privacy and data integrity between client/server applications communicating over the Internet.

The TLS protocol is made up of two layers. The TLS Record Protocol ensures that a connection is private by using symmetric data encryption and ensures that the connection is reliable. The second TLS layer is the TLS Handshake Protocol, which allows authentication between the server and client and the negotiation of an encryption algorithm and cryptographic keys before data is transmitted or received. Based on Netscape's SSL 3.0, TLS supercedes and is an extension of SSL. TLS and SSL are not interoperable.

UTP

Unshielded twisted pair is the cable used by 10BASE-T and 100BASE-Tx Ethernet networks.

WAN

A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

WEP

Wired Equivalent Privacy is a data encryption protocol for 802.11b wireless networks.

All wireless nodes and access points on the network are configured with a 64-bit or 128-bit Shared Key for data encryption.

wide area network

WAN. A long distance link used to extend or connect remotely located local area networks. The Internet is a large WAN.

Wi-Fi

A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see <http://www.wi-fi.net>), an industry standards group promoting interoperability among 802.11b devices.

Windows Internet Naming Service

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

If a remote network contains a WINS server, your Windows PCs can gather information from that WINS server about its local hosts. This allows your PCs to browse that remote network using the Windows Network Neighborhood feature.

WINS

WINS. Windows Internet Naming Service is a server process for resolving Windows-based computer names to IP addresses.

Wireless Network Name (SSID)

Wireless Network Name (SSID) is the name assigned to a wireless network. This is the same as the SSID or ESSID configuration parameter.

Index

Numerics

64 or 128 bit WEP 4-7

802.11b D-1

A

Account Name 3-10, 3-13

Address Resolution Protocol B-9

Addressing E-8

ad-hoc mode D-2

Authentication Header (AH) E-3, E-4

Auto MDI/MDI-X B-13, G-2

Auto Uplink 2-3, B-13, G-2

B

backup configuration 5-7

Basic Wireless Connectivity 4-9

BSSID D-2

C

CA 6-22

cables, pinout B-12

Cabling B-12

Cat5 cable 3-1, B-13, G-2

Certificate Authority 6-22

configuration

 automatic by DHCP 2-4

 backup 5-7

 erasing 5-8

 restore 5-6

 router, initial 3-1

content filtering 2-2, 5-1

conventions

typography 1-1

crossover cable 2-3, 7-2, B-12, B-13, G-2

D

date and time 7-7

Daylight Savings Time 7-7

daylight savings time 5-13

Denial of Service (DoS) protection 2-2

denial of service attack B-11

DHCP B-10

DHCP Client ID C-16

DMZ 2-3

DMZ Server 5-8

DNS Proxy 2-4

DNS server 3-10, 3-13, C-20

domain C-20

Domain Name 3-10, 3-13

domain name server (DNS) B-10

DoS attack B-11

E

Encapsulating Security Payload E-3

Encryption Strength 4-7

EnterNet C-18

erase configuration 5-8

ESP E-3

ESSID 4-9, D-2

Ethernet 2-3

Ethernet cable B-12

exposed host 5-9

F

- factory settings, restoring 5-8
- firewall features 2-2
- Flash memory, for firmware upgrade 2-2
- front panel 2-6, 2-7
- fully qualified domain name (FQDN) 4-6

G

- gateway address C-20
- General 6-4, 6-7, 6-11

H

- host name 3-10, 3-13

I

- IANA
 - contacting B-2
- IETF B-1
 - Web site address B-7
- IKE Security Association E-5
- inbound rules 5-5
- infrastructure mode D-2
- installation 2-4
- Internet account
 - address information C-18
 - establishing C-18
- Internet Key Exchange (IKE) E-3
- Internet Protocol security E-1
- Internet Service Provider 3-1
- Intranets E-2
- IP addresses C-19, C-20
 - and NAT B-8
 - and the Internet B-2
 - assigning B-2, B-9
 - auto-generated 7-3
 - private B-7
 - translating B-9
- IP configuration by DHCP B-10
- IP networking

- for Macintosh C-16
- for Windows C-2, C-7

- IPSec E-1
- IPSec Components E-3
- IPSec SA negotiation E-10
- IPSec Security Features E-2
- ISP 3-1

L

- LAN IP Setup Menu 6-3
- LEDs
 - description 2-6
 - troubleshooting 7-2
- log
 - sending 5-14

M

- MAC address 7-7, B-9
 - spoofing 3-13, 7-5
- Macintosh C-19
 - configuring for IP networking C-16
 - DHCP Client ID C-16
 - Obtaining ISP Configuration Information C-20
- masquerading C-18
- MDI/MDI-X B-13, G-2
- MDI/MDI-X wiring B-12, G-4
- metric 6-7

N

- NAT C-18
- NAT. *See* Network Address Translation
- netmask
 - translation table B-6
- Network Address Translation 2-4, B-8, C-18
- Network Time Protocol 5-13, 7-7
- newsgroup 5-2
- NTP 5-13, 7-7

O

- Open System authentication D-3
- order of precedence 5-8
- outbound rules 5-7

P

- package contents 2-5
- Passphrase 4-7, 4-12
- passphrase 2-2
- password
 - restoring 7-7
- PC, using to configure C-21
- ping 5-9
- pinout, Ethernet cable B-12
- PKIX 6-22
- port filtering 5-7
- port forwarding 5-5
- port forwarding behind NAT B-9
- port numbers 5-10
- PPP over Ethernet 2-4, C-18
- PPPoE 2-4, C-18
- Primary DNS Server 3-9, 3-10, 3-11, 3-13
- protocols
 - Address Resolution B-9
 - DHCP B-10
 - Routing Information 2-3, B-2
 - support 2-1
- publications, related B-1

R

- range 4-1
- rear panel 2-7
- remote management 6-8
- requirements
 - hardware 3-1
- reserved IP addresses 6-5
- restore configuration 5-6
- restore factory settings 5-8

- Restrict Wireless Access by MAC Address 4-10
- RFC

- 1466 B-7, B-9
 - 1597 B-7, B-9
 - 1631 B-8, B-9
 - finding B-7

- RIP (Router Information Protocol) 6-4

- router concepts B-1

- Router Status 5-1

- Routing Information Protocol 2-3, B-2

- rules

- inbound 5-5
 - order of precedence 5-8
 - outbound 5-7

S

- SA E-5

- Secondary DNS Server 3-9, 3-10, 3-11, 3-13

- security 2-1, 2-3

- service blocking 5-7

- service numbers 5-10

- Setup Wizard 3-1

- Shared Key authentication D-3

- SMTP 5-14

- spoof MAC address 7-5

- SSID 4-5, 4-9, 4-10, D-2

- stateful packet inspection 2-2, 5-1, B-11

- subnet addressing B-5

- subnet mask B-6, C-19, C-20

- syslog 5-17

T

- TCP/IP

- configuring C-1, E-1
 - network, troubleshooting 7-5

- TCP/IP properties

- verifying for Macintosh C-17
 - verifying for Windows C-6, C-15

- Testing and Troubleshooting E-12

- time of day 7-7

- time zone 5-13
- time-stamping 5-13
- Transport Mode E-5
- troubleshooting 7-1
- Trusted Host 5-3
- Tunnel Mode E-6
- typographical conventions 1-1

U

- Uplink switch B-12
- USB C-18

V

- VPN E-1
- VPN Consortium E-7
- VPN Process Overview E-7
- VPNC IKE Phase I Parameters E-11
- VPNC IKE Phase II Parameters E-12

W

- WEP D-3
- Wi-Fi D-1
- Windows, configuring for IP routing C-2, C-7
- winipcfg utility C-6
- WinPOET C-18
- Wired Equivalent Privacy. *See* WEP
- Wireless Authentication 4-6
- wireless authentication scheme 4-6
- Wireless Encryption 4-6
- Wireless Ethernet D-1
- Wireless Network Settings 4-5
- Wireless Security 4-2