NETGEAR

ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

Reference Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

October 2012
202-10983-02
v2.0

Support

Thank you for choosing NETGEAR.

After installing your device, locate the serial number on the label of your product and use it to register your product at *https://my.netgear.com*. You must register your product before you can use NETGEAR telephone support. NETGEAR recommends registering your product through the NETGEAR website. For product updates and web support, visit *http://support.netgear.com*.

Phone (US & Canada only): 1-888-NETGEAR.

Phone (Other Countries): Check the list of phone numbers at *http://support.netgear.com/general/contact/default.aspx*.

NETGEAR recommends that you use only the official NETGEAR support resources.

Trademarks

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10983-02	2.0	October 2012	Minor nontechnical revisions
202-10983-02	1.0	September 2012	• Added and refined information (no new features added) • Added *Appendix B, Command-Line Reference* • Added *Index*
202-10983-01	1.0	August 2012	First publication

Contents

Chapter 1 Introduction

Chapter 2 Installation and Basic Configuration

Chapter 3 Wireless Configuration and Security

Chapter 4 Management and Monitoring

Chapter 5 Advanced Configuration

Chapter 6 Troubleshooting

Appendix A Supplemental Information

Appendix B Command-Line Reference

Appendix C Notification of Compliance

Index

Introduction

1

This chapter introduces the NETGEAR® ProSafe® Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620 and describes some of the key features. The chapter includes the following sections:

- *About the ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620*
- *What Is in the Box?*
- *System Requirements*
- *Key Features and Standards*
- *Hardware Description*
- *Register the Wireless Access Point*

Note: For more information about the topics covered in this manual, visit the Support website at *http://support.netgear.com*.

Note: Firmware updates with new features and bug fixes are made available from time to time at *downloadcenter.netgear.com*. Some products can regularly check the site and download new firmware, or you can check for and download new firmware manually. If the features or behavior of your product do not match what is described in this guide, you might need to update your firmware.

About the ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

The ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620, going forward in this manual referred to as the wireless access point, is a powerful building block of a wireless LAN infrastructure. It provides either 2.4 GHz 802.11b/g/n or 5 GHz 802.11a/n connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Support for three transmit radio chains and three receive radio chains, also referred to as 3x3 multiple input, multiple output (MIMO), can increase wireless throughput considerably.

The wireless access point provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) through an antenna. Typically, an individual in-building wireless access point provides a maximum connectivity area with about a 500-foot radius. The wireless access point can support a maximum of 128 clients in a range of several hundred feet. The throughput is shared between all clients. Make sure that you install a sufficient number of wireless access points to meet the required coverage, throughput, and quality of your wireless network.

The wireless access point acts as a bridge between the wired LAN and wireless clients. Connecting multiple wireless access points through a wired Ethernet backbone can further increase the wireless network coverage. As a mobile computing device moves out of the range of one wireless access point, it moves into the range of another. As a result, wireless clients can freely roam from one wireless access point to another and still maintain a seamless connection to the network.

The autosensing capability of the wireless access point allows packet transmission at up to 450 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

Advanced wireless features that are supported on the wireless access point include a wireless intrusion detection system (IDS), wireless intrusion prevention system (IPS), and configurable wireless QoS policies.

You can manage the wireless access point from either an IPv4 or IPv6 address, and the wireless access point can allocate either IPv4 or IPv6 DHCP addresses to its wireless clients.

What Is in the Box?

The product package contains the following items:

- ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620
- Power adapter and cord (12 VCD, 1.5A)
- Straight-through Category 5 Ethernet cable
- Installation guide
- Resource CD, which includes this manual
- Wall-mount kit made up of brackets and hardware

Contact your reseller or customer support in your area if there are any missing or damaged parts.

See the NETGEAR website at *http://support.netgear.com/general/contact/default.aspx* for the telephone number of customer support in your area. Keep the installation guide, along with the original packing materials. If you need to return the wireless access point for repair, use the packing materials to repack the wireless access point.

System Requirements

Before installing the wireless access point, make sure that your system meets these requirements:

- A 10/100/1000 Mbps local area network device such as a hub or switch
- The Category 5 UTP straight-through Ethernet cable with RJ-45 connector included in the package, or one like it
- A 100–120V, 50–60 Hz AC power source
- A computer with the TCP/IP protocol installed and a web browser for configuration, such as Microsoft Internet Explorer 6.0 or later, or Mozilla 1.5 or later
- An 802.11a/n- or 802.11b/g/n-compliant device, such as the NETGEAR N600 Wireless-N Dual Band USB Adapter (WNDA3100)

Key Features and Standards

The wireless access point is easy to use and provides solid wireless and networking support. It also offers a wide range of security options.

Supported Standards and Conventions

The wireless access point supports the following standards and conventions:

- **Standards compliance***.* The wireless access point complies with the IEEE 802.11a/b/g standards for wireless LANs and is Wi-Fi certified for 802.11n standard.
- **WPA and WPA2**. The wireless access point provides WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. The WPA-PSK and WPA2-PSK pre-shared key authentication does not have the overhead of RADIUS servers but provides the strong security of WPA.
- **Multiple BSSIDs**. The wireless access point supports multiple BSSIDs. When a wireless access point is connected to a wired network and a set of wireless stations, it is called a basic service set (BSS). The basic service set identifier (BSSID) is a unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network.

  The multiple BSSID feature allows you to configure up to 16 SSIDs (8 per radio, but only one radio can be active at a time) on your wireless access point and assign different configuration settings to each SSID. All the configured SSIDs are active, and the network devices can connect to the wireless access point by using any of these SSIDs.

- **DHCP server and client**. The DHCP server of the wireless access point can provide a dynamic IPv4 or IPv6 address to wireless clients. The wireless access point can also act as a client and obtain an IPv4 or IPv6 address from a DHCP server on the LAN.
- **SNMP**. The wireless access point supports Simple Network Management Protocol (SNMP) for Management Information Base (MIB) management.
- **STP and LLDP**. The wireless access point supports Spanning Tree Protocol (STP) and Ethernet Link Layer Discovery Protocol (LLDP). LLDP is enabled by default.
- **802.1Q VLAN**. A network of computers can behave as if they are connected to the same network even though they might actually be physically on different segments of a LAN. Virtual LANs (VLANs) are configured through software rather than hardware, which makes them very flexible. VLANs are very useful for user and host management, bandwidth allocation, and resource optimization.

Key Features

The wireless access point provides solid functionality, including the following features:

- **Dual band**. The wireless access point can operate either in the 2.4 GHz band or the 5 GHz band. The choice of band is reflected in the wireless modes that you can select and the administration screens that are displayed in the web management interface.
- **IPv4 and IPv6**. The wireless access point is manageable from either an IPv4 or IPv6 address, it can function as an IPv4 or IPv6 DHCP client, and its DHCP server can allocate either IPv4 or IPv6 addresses.
- **Multiple operating modes**:
    - **Wireless access point**. Operates as a standard 802.11b/g/n or 802.11a/n wireless access point.
    - **Point-to-point bridge**. In this mode, the wireless access point communicates only with another bridge-mode wireless station or wireless access point. Network authentication should be used to protect this communication.
    - **Point-to-multipoint bridge**. Select this option only if this wireless access point is the master for a group of bridge-mode wireless stations. The other bridge-mode wireless stations send all traffic to this master and do not communicate directly with each other. Network authentication should be used to protect this traffic.
    - **Repeater**. In this mode, the wireless access point does not function as an access point for clients but functions only in point-to-multipoint bridge mode to repeat the wireless signal and send all traffic to a remote access point. Network authentication should be used to protect this communication.
- **WMM**. Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients also need to support WMM.

- **QoS**. Quality of Service (QoS) support lets you configure parameters that affect traffic flowing from the wireless access point to the client station and traffic flowing from the client station to the wireless access point:
  - The QoS settings let you prioritize traffic, such as voice and video traffic, so that packets do not get dropped.
  - The QoS policies let you configure classifications (match clauses) and apply traffic to eight priority queues based on IP precedence, DSCP, MAC address, IP address, and other information that might be present in Layer 2 and Layer 3 packet headers.
- **Wireless IDS/IPS**. The wireless intrusion detection system (IDS) and intrusion prevention system (IPS) can detect and prevent a variety of wireless attacks. Attacks are covered by preconfigured policy rules. When an attack occurs, the wireless access point can notify a network administrator though an email.
- **Hotspot support**. You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify.
- **Rogue AP and ad hoc network detection**. Rogue AP filtering and ad hoc network detection ensure that unknown APs and networks are not given access to any part of the secured wireless and wired LAN.
- **Access control**. MAC address filtering can ensure that only trusted wireless stations can use the wireless access point to gain access to the wireless and wired LAN.
- **Security profiles**. When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, and so on) for each BSSID.
- **Hidden mode**. The SSID is not broadcast, assuring that only clients configured with the correct SSID can connect.
- **Secure Telnet command-line interface**. The secure Telnet command-line interface (CLI) enables direct secure access over the serial port and easy scripting of configuration of multiple wireless access points across an extensive network through the Ethernet interface. A Secure Shell (SSH) client is required.
- **Upgradeable firmware**. Firmware is stored in a flash memory. You can upgrade it easily, using only your web browser, and you can upgrade it remotely. You can also use the command-line interface.
- **Configuration backup**. Configuration settings can be backed up to a file and restored.
- **Secure and economical operation**. Adjustable power output allows more secure or economical operation.
- **PoE support**. Using Power over Ethernet (PoE), any 802.3af-compliant midspan or end-span source can supply power to the wireless access point over its Ethernet port.
- **Autosensing Ethernet connection with Auto Uplink™ interface**. Connects to 10/100/1000 Mbps IEEE 802.3 Ethernet networks.
- **LED indicators**. Power/Test, Active, LAN, and WLAN for each radio mode are easily identified.
- **VLAN security profiles**. Each security profile is automatically allocated a VLAN ID when the security profile is modified.

802.11b/g/n and 802.11a/n Standards–Based Wireless Networking

The wireless access point provides a bridge between wired Ethernet LANs and 802.11b/g/n- and 802.11a/n-compatible wireless LAN networks. It provides connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

In addition, the wireless access point supports the following wireless features:

- Aggregation support
- Reduced InterFrame spacing support
- 3 x 3 multiple input, multiple output (MIMO) support
- Distributed coordinated function (CSMA/CA, back-off procedure, ACK procedure, retransmission of unacknowledged frames)
- RTS/CTS handshake
- Beacon generation
- Packet fragmentation and reassembly
- Auto or long preamble
- Roaming among wireless access points on the same subnet

Autosensing Ethernet Connections with Auto Uplink

The wireless access point can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

The wireless access point incorporates Auto Uplink technology. The Ethernet port automatically senses whether the Ethernet cable plugged into the port should have a “normal” connection such as to a computer or an “uplink” connection such as to a switch or hub. That port then configures itself correctly. This feature also eliminates any concerns about crossover cables, as Auto Uplink accommodates either type of cable to make the right connection.

Hardware Description

This section describes the top and rear hardware functions of the wireless access point.

- *Top Panel*
- *Rear Panel*
- *Bottom Panel with Product Label*

Top Panel

The LEDs of the wireless access point are described in the following figure and table:

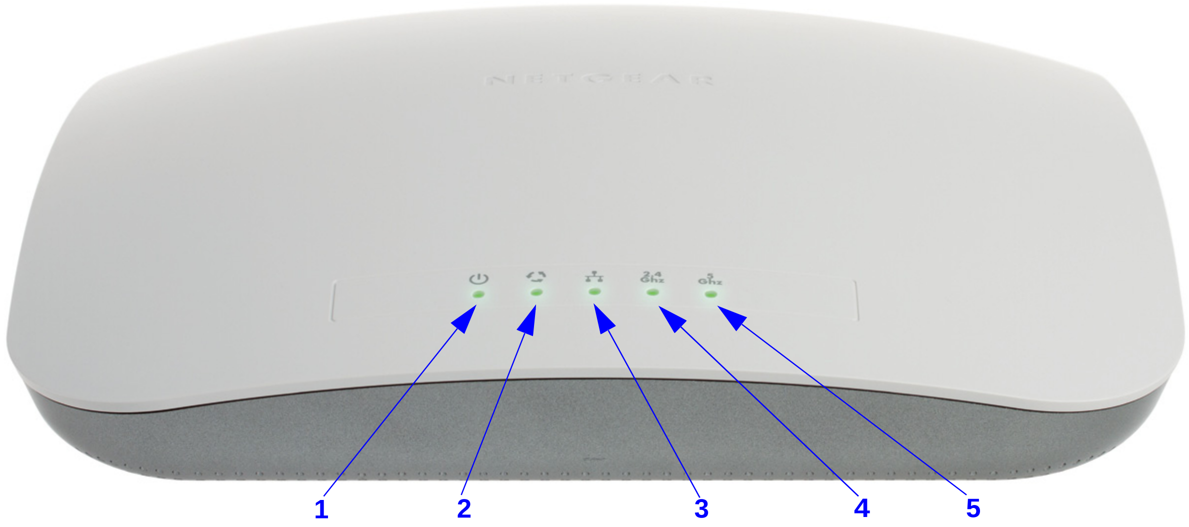


Figure 1.

Table 1. Top panel LEDs

Item	LED	Description		
1	⏻	**Power/Test**	Off	Power is off.
			On (green)	Power is on.
			Amber, then blinking green	A self-test is running or software is being loaded. During startup, the LED is first steady amber, then goes off, and then blinks green before turning steady green after about 45 seconds. If after 1 minute the LED remains amber or continues to blink green, it indicates a system fault.
2	↻	**Active**	Off	No Ethernet traffic is detected, or no link is detected.
			On or blinking (green)	Ethernet traffic is detected.
3	🖧	**LAN**	Off	10 Mbps or no link is detected.
			Amber	10/100 Mbps link is detected.
			Green	1000 Mbps link is detected.
4	**2.4 Ghz**	**WLAN**	Off	Wireless 802.11b/g/n (2.4 GHz) LAN is not ready, or no wireless activity is detected.
			On or blinking (green)	Wireless 802.11b/g/n (2.4 GHz) LAN is ready, or wireless activity is detected.
5	**5 Ghz**	**WLAN**	Off	Wireless 802.11n/a (5 GHz) LAN is not ready, or no wireless activity is detected.
			On or blinking (green)	Wireless 802.11n/a (5 GHz) LAN is ready, or wireless activity is detected.

Rear Panel

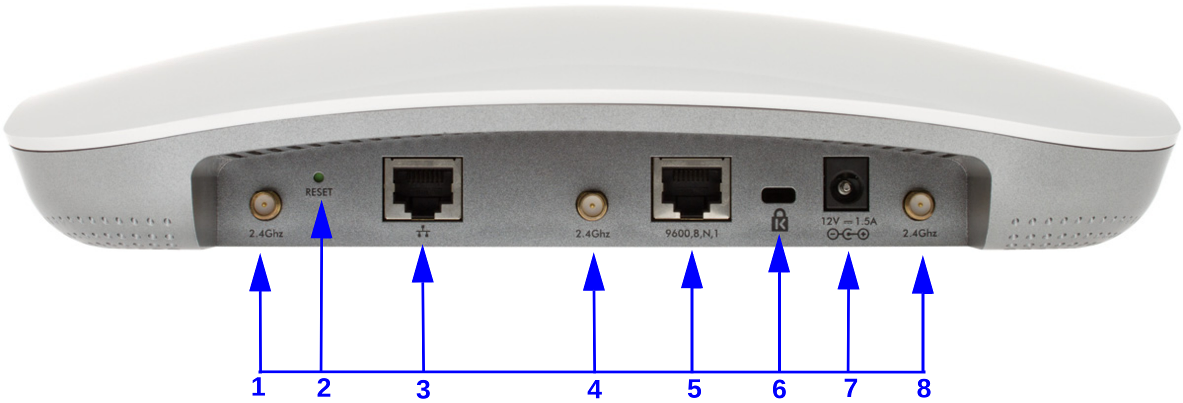


Figure 2.

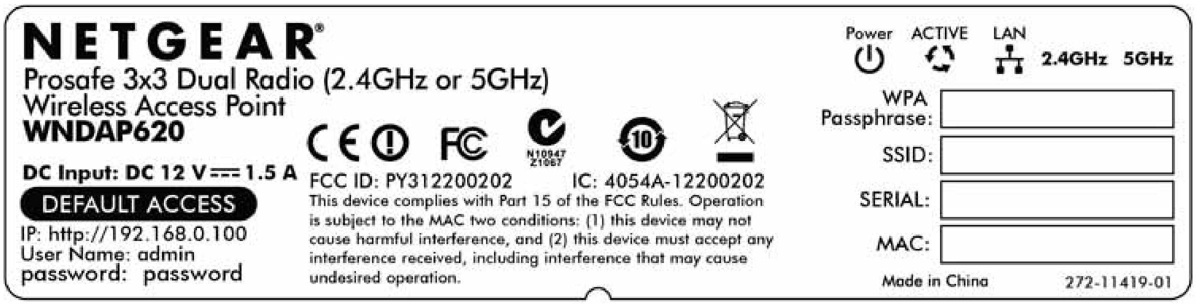
The rear panel components of the wireless access point, from left to right, are described in the following list:

1. First reverse SMA connector for an optional 2.4 GHz antenna.
2. Factory default Reset button. Using a sharp object, press and hold this button for about 5 seconds to reset the wireless access point to factory defaults settings. All configuration settings are lost, and the default password is restored. For more information, see *Restore the Wireless Access Point to the Factory Default Settings* on page 71.
3. 10/100/1000BASE-T Gigabit Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X) with IEEE 802.3af Power over Ethernet (PoE) support for connection to a switch or router.
4. Second reverse SMA connector for an optional 2.4 GHz antenna.
5. Console port for connecting to an optional console terminal. The port has an RJ-45 connector and supports the following settings: 9600 K default baud rate, 8 data bits, no (N) parity bit, and one (1) stop bit.
6. Cable security lock receptacle for an optional lock.
7. Power socket for a 12 VDC, 1.5A power adapter.
8. Third reverse SMA connector for an optional 2.4 GHz antenna.

Note: The wireless access point can support up to three optional 2.4 GHz antennas.

Bottom Panel with Product Label

The product label on the bottom of the wireless access point’s enclosure displays factory default settings, regulatory compliance, and other information:



NETGEAR®

Prosafe 3x3 Dual Radio (2.4GHz or 5GHz)
Wireless Access Point
WNDAP620

DC Input: DC 12 V ⎓ 1.5 A

DEFAULT ACCESS

IP: http://192.168.0.100
User Name: admin
password: password

FCC ID: PY312200202 IC: 4054A-12200202

This device complies with Part 15 of the FCC Rules. Operation is subject to the MAC two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

WPA Passphrase:

SSID:

SERIAL:

MAC:

Made in China 272-11419-01

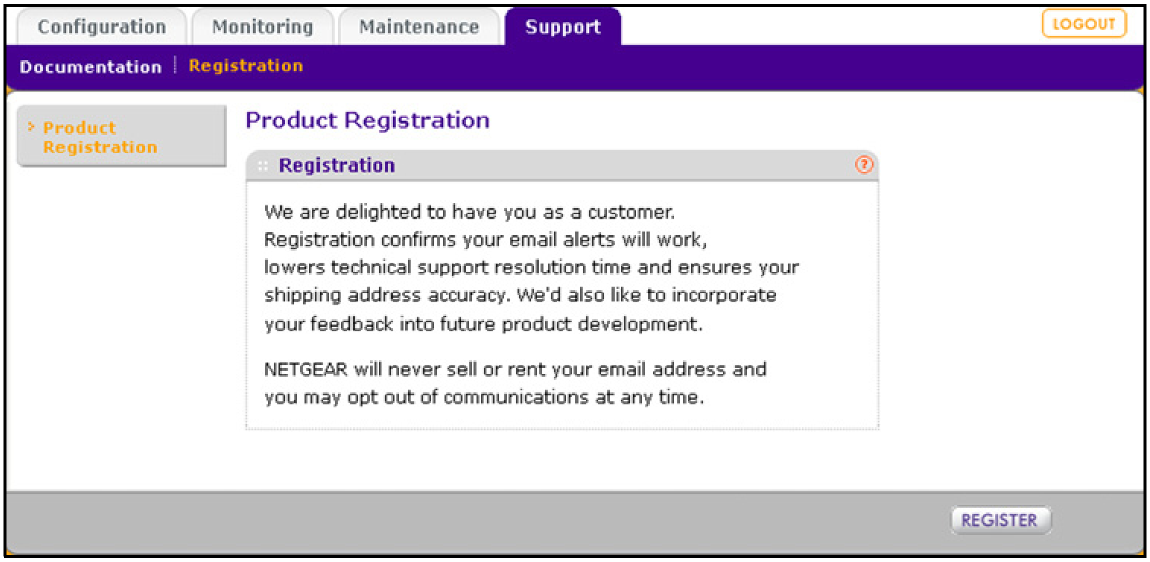
Figure 3.

Register the Wireless Access Point

To qualify for product updates and product warranty, NETGEAR encourages you to register your product. The first time that you connect to the wireless access point while it is connected to the Internet, you have the option to register your product. At any time, you can register your product from the web management interface, or you can go to the NETGEAR website for registration at *https://my.netgear.com/registration/login.aspx*.

➢ **To register the wireless access point with NETGEAR:**

1. Select **Support > Registration**. The Product Registration screen displays:



Product Registration

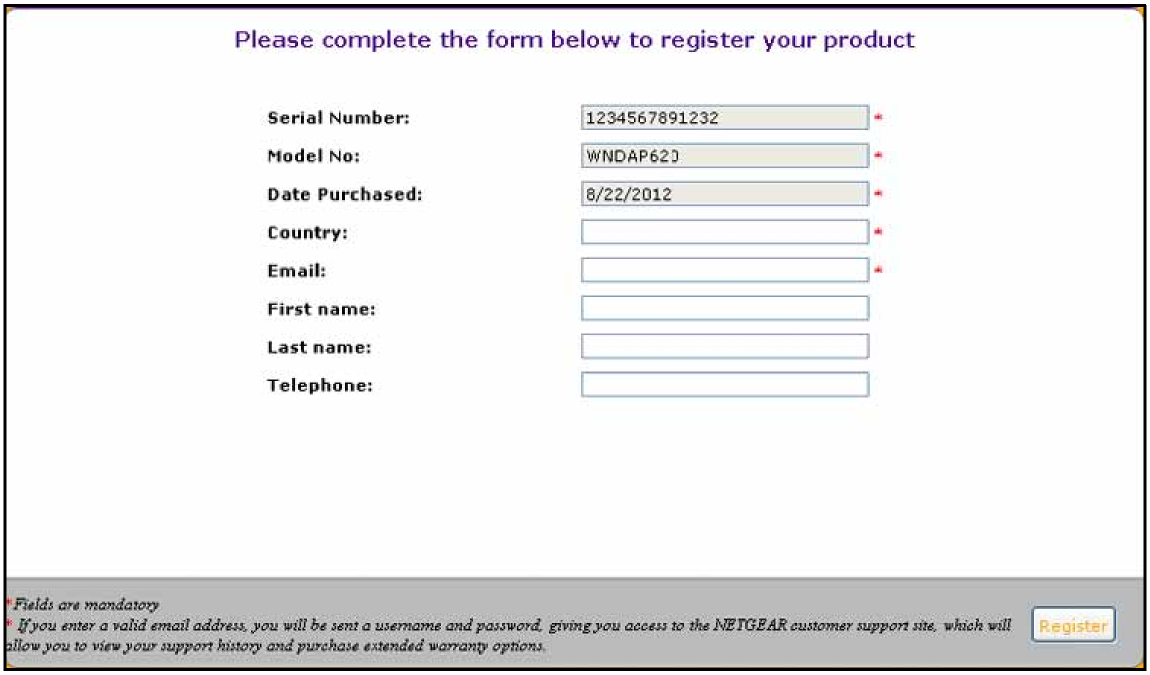
Registration

We are delighted to have you as a customer.
Registration confirms your email alerts will work,
lowers technical support resolution time and ensures your
shipping address accuracy. We'd also like to incorporate
your feedback into future product development.

NETGEAR will never sell or rent your email address and
you may opt out of communications at any time.

Figure 4.

2. Click **Register**. A new screen displays in your browser:



Please complete the form below to register your product

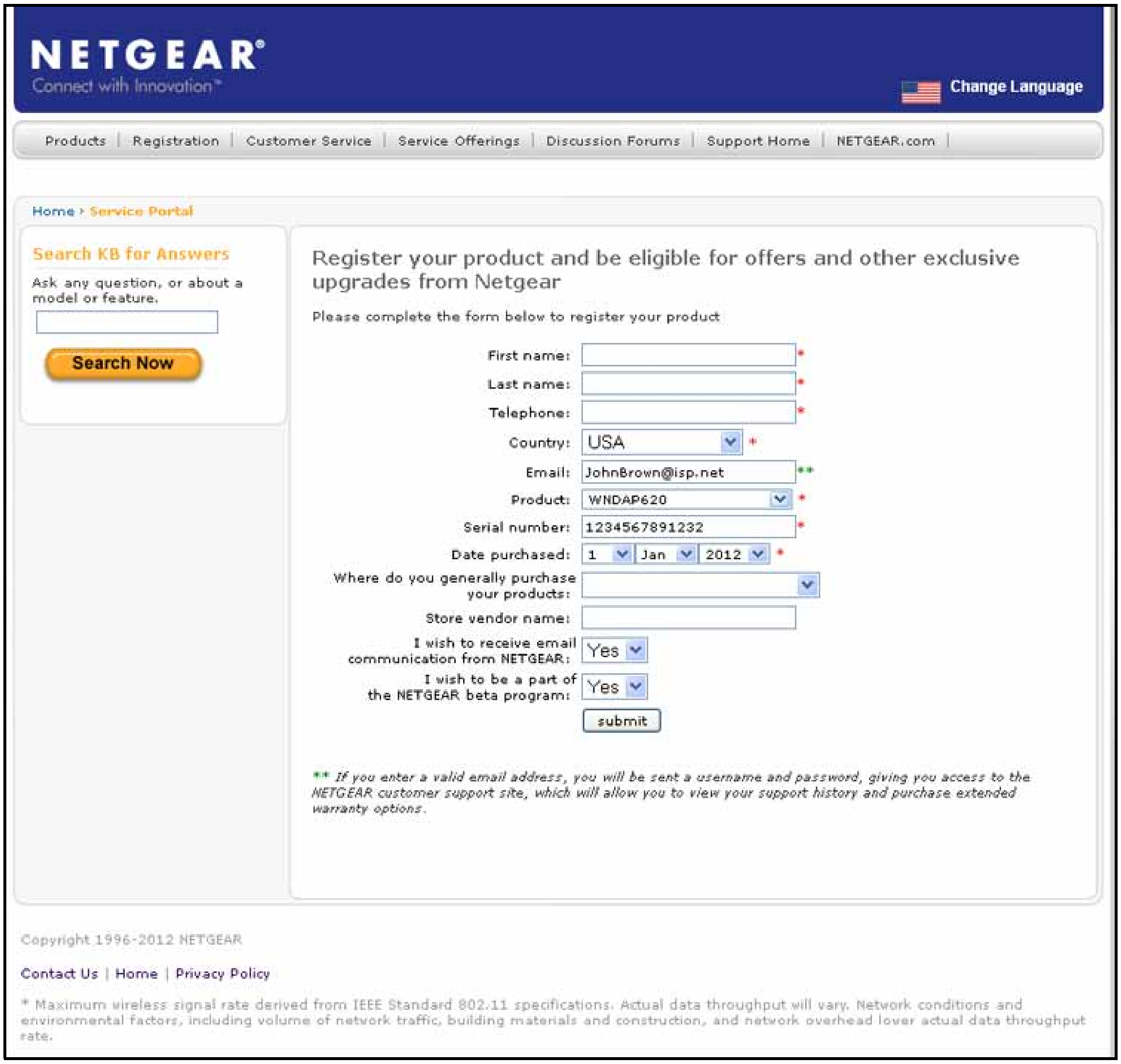
Serial Number:	1234567891232 *
Model No:	WNDAP620 *
Date Purchased:	8/22/2012 *
Country:	*
Email:	*
First name:	
Last name:	
Telephone:	

*Fields are mandatory

* If you enter a valid email address, you will be sent a username and password, giving you access to the NETGEAR customer support site, which will allow you to view your support history and purchase extended warranty options.

Figure 5.

3. Enter the information in the blank fields. The serial number, model number, and date of purchase are entered automatically.
4. Click **Register**. The registration web page displays:


NETGEAR®
Connect with Innovation™
Change Language
Products | Registration | Customer Service | Service Offerings | Discussion Forums | Support Home | NETGEAR.com |
Home › Service Portal
Search KB for Answers
Ask any question, or about a model or feature.
Search Now

Register your product and be eligible for offers and other exclusive upgrades from Netgear

Please complete the form below to register your product

First name:	*
Last name:	*
Telephone:	*
Country:	USA *
Email:	JohnBrown@isp.net **
Product:	WNDAP620 *
Serial number:	1234567891232 *
Date purchased:	1 Jan 2012 *
Where do you generally purchase your products:	
Store vendor name:	
I wish to receive email communication from NETGEAR:	Yes
I wish to be a part of the NETGEAR beta program:	Yes

submit

*** If you enter a valid email address, you will be sent a username and password, giving you access to the NETGEAR customer support site, which will allow you to view your support history and purchase extended warranty options.*

Copyright 1996-2012 NETGEAR

Contact Us | Home | Privacy Policy

* Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual data throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead lower actual data throughput rate.

Figure 6.

5. Complete the registration form.
6. Click **submit**.

Installation and Basic Configuration

2

This chapter describes how to install and configure the wireless access point for wireless connectivity to your LAN. This basic configuration enables computers with either 2.4 GHz 802.11b/g/n or 5 GHz 802.11a/n wireless adapters to connect to the Internet or access printers and files on your LAN. In planning your wireless network, consider the level of security required. *Chapter 3, Wireless Configuration and Security*, describes how to set up wireless security for your network. This chapter includes the following sections:

- *What You Need Before You Begin*
- *Install and Configure the Wireless Access Point*
- *Test Basic Wireless Connectivity*
- *Mount the Wireless Access Point*

What You Need Before You Begin

- *Wireless Equipment Placement and Range Guidelines*
- *Ethernet Cabling Requirements*
- *LAN Configuration Requirements*
- *Hardware Requirements for Computers on Your LAN*
- *Operating Frequency (Channel) Guidelines*
- *Requirements for Entering IP Addresses*

You need to consider the following guidelines and requirements before you can set up your wireless access point. See also *System Requirements* on page 8.

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless access point. The latency, data throughput performance, and power consumption of wireless adapters also vary depending on your configuration choices.

Note: Failure to follow these guidelines can result in significant performance degradation or inability to connect wirelessly to the wireless access point. For complete performance specifications, see *Appendix A, Supplemental Information*.

Note: Before you position and mount the wireless access point at its permanent position, first configure the wireless access point and test the computers on your LAN for wireless connectivity as explained in this chapter.

For best results, place your wireless access point according to the following general guidelines:

- Near the center of the area in which the wireless devices will operate.
- In an elevated location such as a high shelf where the wirelessly connected devices have line-of-sight access (even if through walls).
- Away from sources of interference, such as computers, microwaves ovens, and 2.4 GHz cordless phones.
- Away from large metal surfaces or water.
- Placing an external antenna in a vertical position provides best side-to-side coverage. Placing an external antenna in a horizontal position provides best up-and-down coverage. (An external antenna does not come standard with the wireless access point.)
- If you are using multiple wireless access points, it is better if adjacent wireless access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent wireless access points is five channels (for example, use Channels 1 and 6, or 6 and 11, or 1 and 11).

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 computer.

Ethernet Cabling Requirements

The wireless access point connects to your LAN using twisted-pair Category 5 Ethernet cable with RJ-45 connectors.

LAN Configuration Requirements

For the initial configuration of your wireless access point, you need to connect a computer to the wireless access point.

Hardware Requirements for Computers on Your LAN

To connect to the wireless access point on your network, each computer needs to have an 802.11b/g/n or 802.11a/n wireless adapter installed. NETGEAR recommends using the wireless access point with computers that have the NETGEAR N600 Wireless Dual Band USB Adapter (WNDA3100) installed.

Operating Frequency (Channel) Guidelines

You do not need to change the operating frequency (channel) unless you notice interference problems or you place the wireless access point near another wireless access point. If you do change the operating frequency, observe the following guidelines:

- Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available.
- If you use multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).
- In infrastructure mode (which is the default mode for the wireless access point), wireless stations normally scan all channels, looking for a wireless access point. If more than one wireless access point can be used, the one with the strongest signal is used. This is possible only if the wireless access points use the same SSID.

Requirements for Entering IP Addresses

IPv4

The fourth octet of an IP address needs to be between 0 and 255 (both inclusive). This requirement applies to any IP address that you enter on a screen of the web management interface.

IPv6

IPv6 addresses are denoted by eight groups of hexadecimal quartets that are separated by colons. Any four-digit group of zeroes within an IPv6 address can be reduced to a single zero or altogether omitted.

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row

Install and Configure the Wireless Access Point

Install and configure your wireless access point in the order of the following sections:

1. *Connect the Wireless Access Point to a Computer*
2. *Log In to the Wireless Access Point*
3. *Configure Basic General System Settings and Time Settings*
4. *Configure the IPv4 Settings*
5. *Configure the Optional DHCPv4 Server*
6. *Configure the Basic Wireless Settings*

Before installing the wireless access point, make sure that your Ethernet network functions. After you have connected the wireless access point to the Ethernet network, computers with either 802.11b/g/n or 802.11a/n wireless adapters are able to communicate with the Ethernet network.

For this to work correctly, verify that you have met all the system requirements, shown in *System Requirements* on page 8.

Connect the Wireless Access Point to a Computer

Tip: Before you place the wireless access point in an elevated position that is difficult to reach, first set up and test the wireless access point to verify wireless network connectivity.

➢ **To set up the wireless access point:**

1. Unpack the box and verify the contents.
2. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP configuration settings. Configure the computer with a static IP address of 192.168.0.210 and 255.255.255.0 as the subnet mask.
3. Connect an Ethernet cable from the wireless access point to the computer (point **A** in the following figure).
4. Securely insert the other end of the cable into the wireless access point’s Ethernet port (point **B** in the following figure).

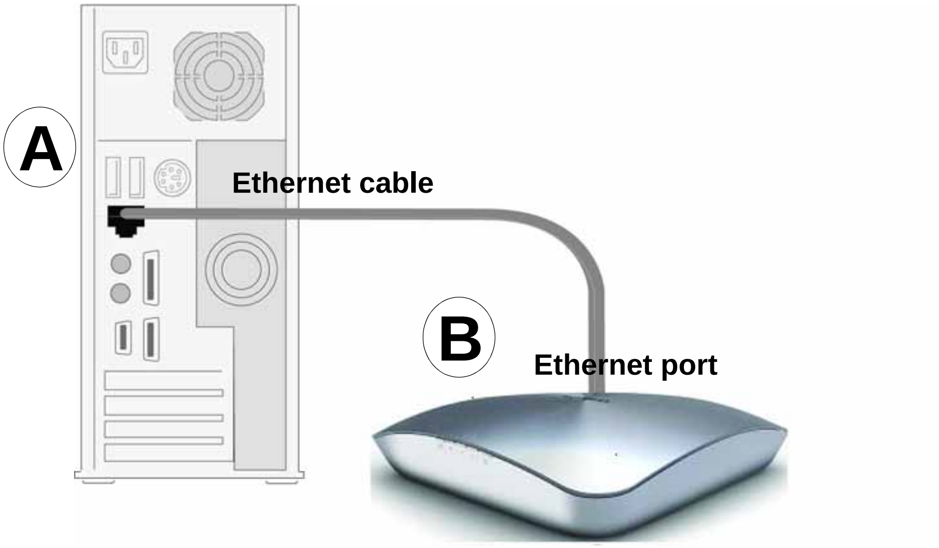


Figure 7.

5. Turn on your computer.
6. Connect the power adapter to the wireless access point.

> **Tip:** The wireless access point supports Power over Ethernet (PoE). If you have a switch that provides PoE, you do not need to use the power adapter to power the wireless access point. Using PoE can be especially convenient when the wireless access point is installed in a high location far away from a power outlet.

7. Verify the following:

⏻ **Power/Test LED**. The Power/Test LED blinks when the wireless access point is first turned on. (To be exact, during startup, the LED is first steady amber, then goes off, and then blinks green.) After about 45 seconds, the LED should stay lit (steady green). If after 1 minute the Power/Test LED is not lit or is still blinking, check the connections and see if the power outlet is controlled by a wall switch that is turned off.

Active LED. The Active LED is lit or blinks green when there is Ethernet traffic.

LAN LED. The LAN LED indicates the LAN speed: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps. If the LAN LED is not lit, make sure that the Ethernet cable is securely attached at both ends.

2.4 Ghz **WLAN LED**. The 2.4 GHz WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready.

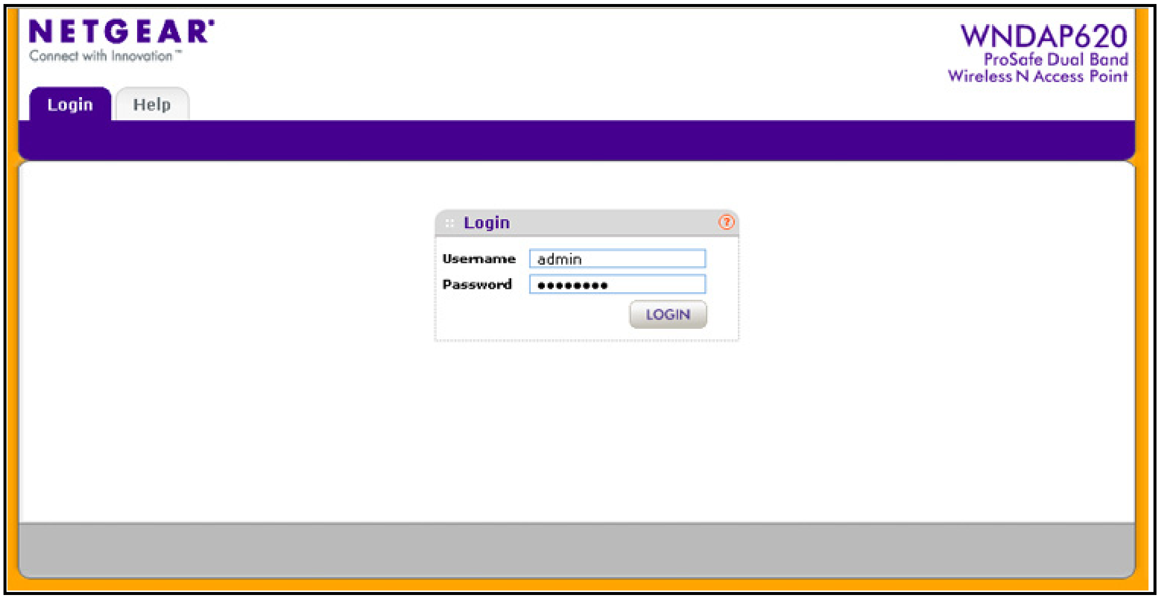
5 Ghz **WLAN LED**. The 5 GHz WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready.

Log In to the Wireless Access Point

The default IP address of your wireless access point is 192.168.0.100. By default, the DHCP client on the wireless access point is disabled so you can log in using the default IP address.

➢ **To log in to the wireless access point:**

1. Open a web browser such as Microsoft Internet Explorer 6.0 or later, or Mozilla Firefox 1.5 or later.
2. Connect to the wireless access point by entering its default address of **192.168.0.100** into your browser (use http and not https). The Login screen displays:



Username admin
Password ••••••••

Figure 8.

3. Enter the default user name of **admin** and the default password of **password**.
4. Click **Login**. The web browser displays the basic General system settings screen under the Configuration tab of the main menu as shown in *Figure 11* on page 23.

Web Management Interface

The navigation tabs across the top of the web management interface provide access to all the configuration functions of the wireless access point and remain constant. The menu items in the blue bar change according to the navigation tab that is selected.

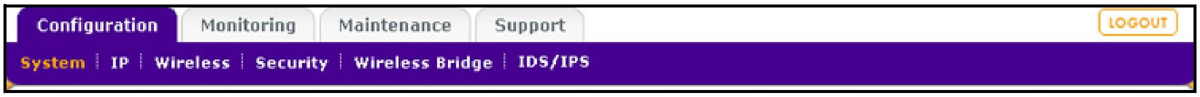


Figure 9.

The bottom right corner of all screens that allow you to make configuration changes show the Apply and Cancel buttons, and on several screens the Edit button.

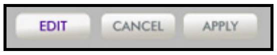


Figure 10.

These buttons have the following functions:

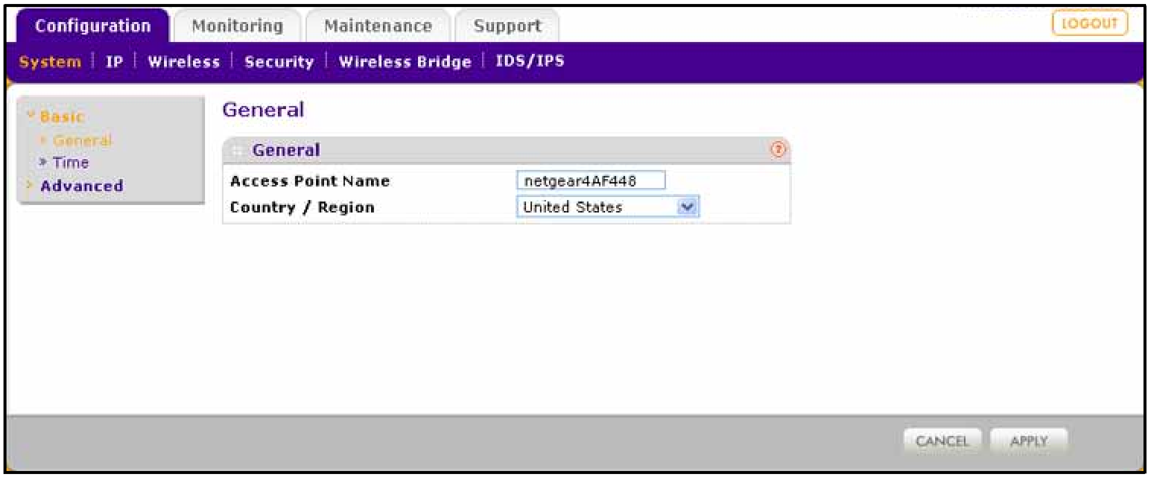
- **Edit**. Allows you to edit the existing configuration.
- **Cancel**. Cancels all configuration changes that you made on the screen.
- **Apply**. Saves and applies all configuration changes that you made on the screen.

Configure Basic General System Settings and Time Settings

Note: After you have successfully logged in to the wireless access point, the basic General system settings screen displays.

➤ **To configure basic system settings:**

1. Select **Configuration > System > Basic > General**. The basic General system settings screen displays:



General

General

Access Point Name: netgear4AF448

Country / Region: United States

Figure 11.

2. Configure the settings as explained in the following table:

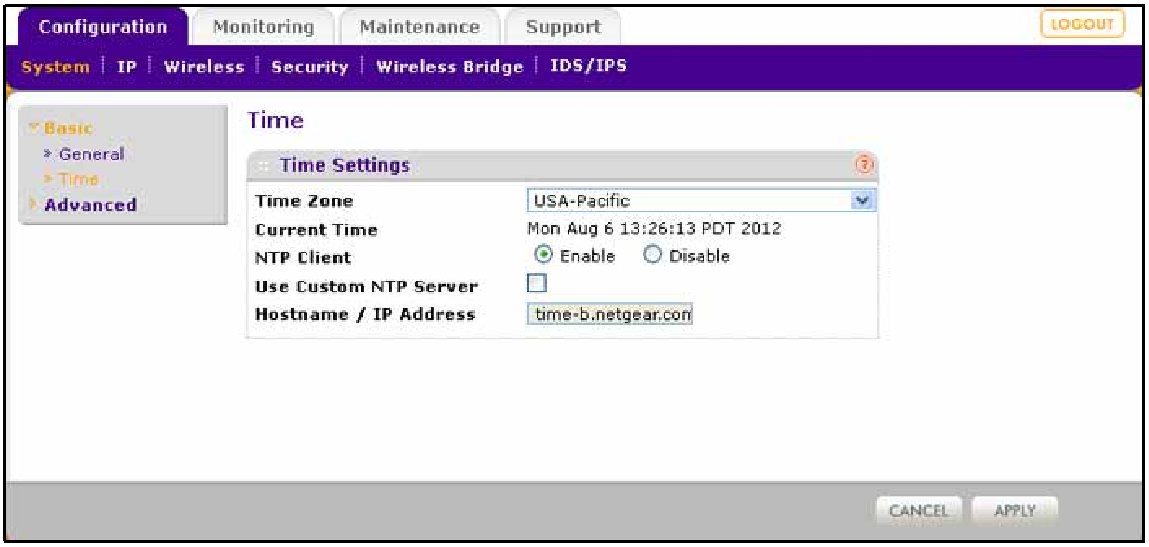
Table 2. Basic general system settings

Setting	Description
Access Point Name	This unique name is the wireless access point NetBIOS name. The name is printed on the rear label of the wireless access point. The default is netgear*xxxxxx*, in which *xxxxxx* represents the last 6 digits of the wireless access point MAC address. You can replace the default name with a unique name up to 15 characters long. The access point name can be retrieved through SNMP.
Country / Region	From the Country / Region drop-down list, select the country where the wireless access point is installed. **Note:** It might not be legal to operate this wireless access point in a region other than one of those identified in this field.

3. Click **Apply** to save your settings.

➢ To configure time settings:

1. Select **Configuration > System > Basic > Time**. The Time screen displays:



Time Zone: USA-Pacific

Current Time: Mon Aug 6 13:26:13 PDT 2012

NTP Client: ● Enable ○ Disable

Use Custom NTP Server: □

Hostname / IP Address: time-b.netgear.com

Figure 12.

2. Configure the settings as explained in the following table:

Table 3. Time system settings

Setting	Description
Time Zone	Select the time zone to match your location.
Current Time	This is a nonconfigurable field that displays the current date and time.

Table 3. Time system settings (continued)

Setting	Description	
NTP Client	Enable the Network Time Protocol (NTP) client to synchronize the time of the wireless access point with an NTP server. By default the Enable radio button is selected.	
Use Custom NTP Server	Select this check box if you want to use a custom NTP server. **Note:** You need to have an Internet connection to use an NTP server that is not on your local network.	
	Hostname / IP Address	Enter the host name or IP address of the custom NTP server. The default is time-b.netgear.com. **Note:** If you use a host name, make sure that you have configured a DNS server. For more information, see the next section.

3. Click **Apply** to save your settings.

Configure the IPv4 Settings

Note: For information about how to configure the IPv6 settings, see *Configure the IPv6 Settings* on page 99.

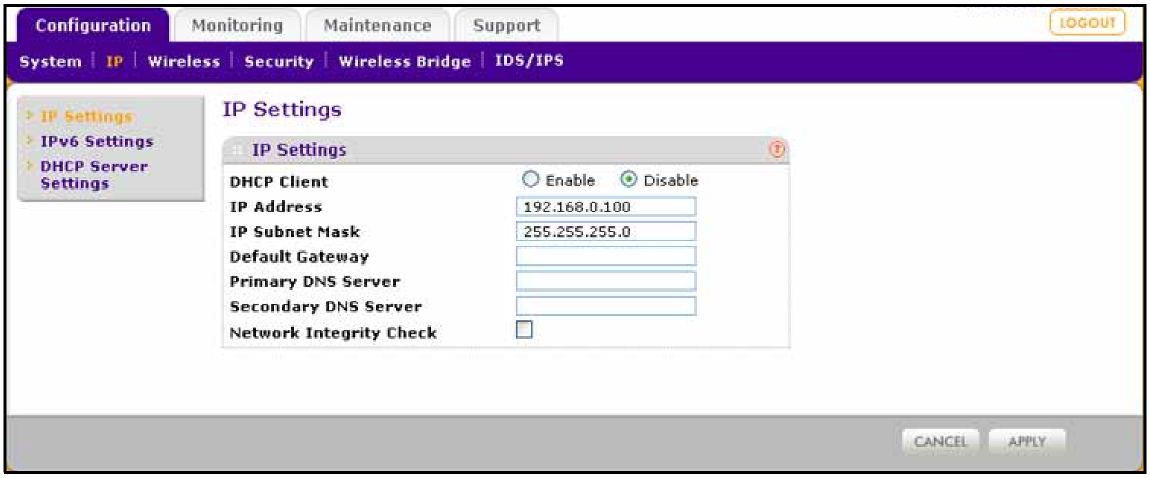
WARNING:

If you enable the DHCP client, the IP address of the wireless access point changes when you click Apply, causing you to lose your connection to the wireless access point. You then need to use the new IP address to reconnect to the wireless access point.

Tip: If you enable the DHCP client on the wireless access point, you can discover the new IP address of the wireless access point by accessing the DHCP server on your LAN, or by using a network IP address scanner application.

➢ **To configure the IPv4 settings:**

1. Select **Configuration > IP > IP Settings**. The IP Settings screen displays:



IP Settings

IP Settings

DHCP Client	○ Enable ● Disable
IP Address	192.168.0.100
IP Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS Server	
Secondary DNS Server	
Network Integrity Check	□

Figure 13.

2. Configure the IPv4 settings as explained in the following table:

Table 4. IPv4 settings

Setting	Description
DHCP Client	By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you select the Enable check box, the wireless access point receives its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the wireless access point to your LAN.
IP Address	Enter the IP address of your wireless access point. The default IP address is **192.168.0.100**. To change the address, enter an unused IP address from the address range used on your LAN, or enable DHCP the server.
IP Subnet Mask	Enter the network number portion of an IP address. Unless you are implementing subnetting, enter **255.255.0.0** as the subnet mask.
Default Gateway	Enter the IP address of the ISP gateway to which the wireless access point connects.
Primary DNS Server	Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your wireless access point during login. If the ISP does not transfer an address, you need to obtain it from the ISP and enter it manually in this field.
Secondary DNS Server	
Network Integrity Check	Select this check box to validate that the upstream link is active before allowing wireless associations. Ensure that the default gateway is configured.

3. Click **Apply** to save your settings.

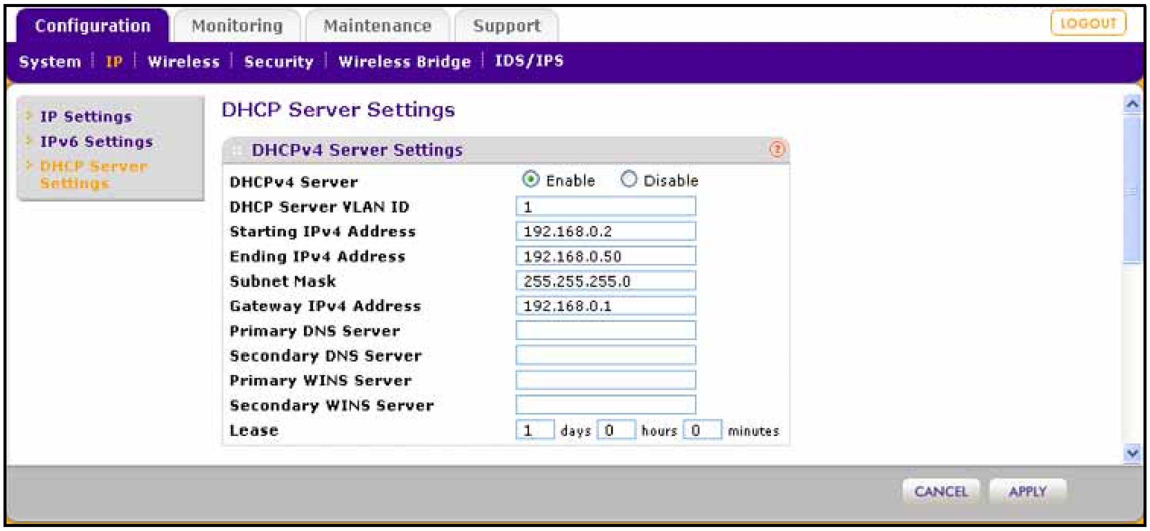
Configure the Optional DHCPv4 Server

The wireless access point provides a built-in DHCPv4 server for wireless clients only, which can be especially useful in small networks. When the DHCP server is enabled, the wireless access point provides preconfigured TCP/IP configurations to all connected wireless stations.

Note: For information about how to configure the DHCPv6 server, see *Configure the Optional DHCPv6 Server* on page 101.

➢ **To configure DHCPv4 server settings:**

1. Select **Configuration > IP > DHCP Server Settings**. The DHCP Server Settings screen displays. The following figure displays the DHCPv4 server settings only. For information about the DHCPv6 server settings, see *Configure the Optional DHCPv6 Server* on page 101.



DHCP Server Settings

DHCPv4 Server Settings

DHCPv4 Server	● Enable ○ Disable
DHCP Server VLAN ID	1
Starting IPv4 Address	192.168.0.2
Ending IPv4 Address	192.168.0.50
Subnet Mask	255.255.255.0
Gateway IPv4 Address	192.168.0.1
Primary DNS Server	
Secondary DNS Server	
Primary WINS Server	
Secondary WINS Server	
Lease	1 days 0 hours 0 minutes

Figure 14.

2. Configure the settings as explained in the following table:

Table 5. DHCP server settings for IPv4

Setting	Description
Select the **DHCPv4 Server** check box to enable the DHCP server. Use the default settings or specify the pool of IPv4 addresses to be assigned by setting the starting IPv4 address and ending IPv4 address. These addresses should be part of the same IPv4 address subnet as the wireless access point's LAN IPv4 address.	
DHCP Server VLAN ID	Enter the VLAN ID for the DHCP server. The VLAN ID range is from 1 to 4094. The default VLAN is 1.
Starting IPv4 Address	Enter the first address in the range of IPv4 addresses to be assigned to DHCP clients. The default address is 192.168.1.02.

Table 5. DHCP server settings for IPv4 (continued)

Setting	Description
Ending IPv4 Address	Enter the last address in the range of IPv4 addresses to be assigned to DHCP clients. The default address is 192.168.1.50.
Subnet Mask	Enter the subnet mask to be used by DHCP clients. The default mask is 255.255.255.0.
Gateway IPv4 Address	Enter the IPv4 address of the default routing gateway to be used by DHCP clients. The default address is 192.168.0.1.
Primary DNS Address	Enter the IP address of the primary Domain Name System (DNS) server available to DHCP clients.
Secondary DNS Address	Enter the IP address of the secondary DNS server available to DHCP clients.
Primary WINS Server	Enter the IP address of the primary WINS server for the network, if there is any.
Secondary WINS Server	Enter the IP address of the secondary WINS server for the network, if there is any.
Lease	Enter the period that the DHCP server grants to DHCP clients to use the assigned IP addresses. The default time is one day.

3. Click **Apply** to save your settings.

Configure the Basic Wireless Settings

For proper compliance and compatibility between similar products in your coverage area, you need to configure the 802.11b/g/n or 802.11a/n wireless adapter settings correctly, including the operating channel and country. You also need to configure the basic wireless network settings for wireless devices to connect to your network. For other wireless features, including wireless security, see *Chapter 3, Wireless Configuration and Security*.

WARNING:

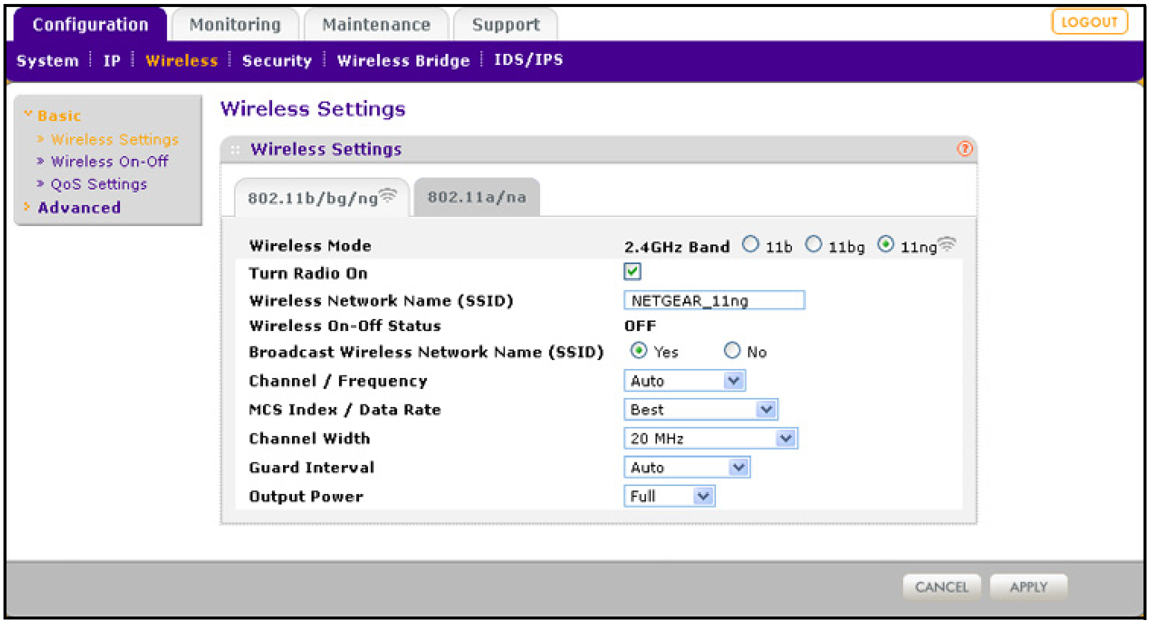
If you configure the wireless access point from a wireless computer and you change the wireless access point's SSID, channel, or wireless security settings, you lose your wireless connection when you click Apply. You then need to change the wireless settings of your computer to match the wireless access point's new settings.

Configure 802.11b/bg/ng Wireless Settings

➤ **To configure the 802.11b/g/n wireless settings:**

1. Select **Configuration > Wireless > Basic > Wireless Settings**. The basic Wireless Settings screen displays. (The following figure shows the 11ng settings.)

Note: The radio wave icon (📶) displays next to the enabled wireless mode.



Wireless Settings

Wireless Settings

Wireless Mode	2.4GHz Band ○ 11b ○ 11bg ● 11ng
Turn Radio On	☑
Wireless Network Name (SSID)	NETGEAR_11ng
Wireless On-Off Status	OFF
Broadcast Wireless Network Name (SSID)	● Yes ○ No
Channel / Frequency	Auto
MCS Index / Data Rate	Best
Channel Width	20 MHz
Guard Interval	Auto
Output Power	Full

Figure 15.

2. Specify the wireless mode in the 2.4 GHz band by selecting one of the following radio buttons:
   - **11b**. Both 802.11n- and 802.11g-compliant devices can connect to the access point because they are backward compatible.
   - **11bg**. 802.11n-compliant devices can connect to the access point because they are backward compatible.
   - **11ng**. This is the default setting. 802.11b-compliant devices cannot connect to the access point. If you keep the default setting, go to *Step 5*.

   When you change the wireless mode, the Turn Radio On check box is automatically cleared, and all fields, buttons, and drop-down lists onscreen are masked out.

3. Turn on the radio by selecting the **Turn Radio On** check box. A pop-up screen displays.

   Note: *Under normal conditions, you want the radio to be turned on. Turning off the radio disables access through the wireless access point, which can be helpful for configuration, network tuning, or troubleshooting activities.*

4. Click **OK** to confirm the change of wireless mode. The change does not take effect until you click the Apply button after you have completed the wireless configuration.

5. Specify the remaining wireless settings as explained the following table:

Table 6. Basic 2.4 GHz band wireless settings

Setting	Descriptions	
Wireless Network Name (SSID)	Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. The default is NETGEAR_11ng. The SSID assigned to a wireless device needs to match the wireless access point's SSID for the wireless device to communicate with the wireless access point. If the SSIDs do not match, you do not get a wireless connection to the wireless access point.	
Wireless On-Off Status	This field is not configurable. It shows the status of the wireless scheduler. For more information, see *Schedule the Wireless Radio to Be Turned Off* on page 61.	
Broadcast Wireless Network Name (SSID)	Select the **Yes** radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the **No** radio button.	
Channel / Frequency	From the drop-down list, select the channel you wish to use for your wireless LAN. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto. **Note:** It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see *Operating Frequency (Channel) Guidelines* on page 19. **Note:** For more information about available channels and frequencies, see *Technical Specifications* on page 139.	
11ng mode only **Note:** For most networks, the default settings work fine.	MCS Index / Data Rate	From the drop-down list, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the wireless network. The default setting is Best. For a list of all options that you can select from in 11ng mode, see *Factory Default Settings* on page 142.
	Channel Width	From the drop-down list, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, and 40 MHz. The default is 20 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz.
	Guard Interval	From the drop-down list, select the guard interval to protect transmissions from interference. The default is Auto, or you can select Long - 800 ns. Some legacy devices can operate only with a long guard interval.

Table 6. Basic 2.4 GHz band wireless settings (continued)

Setting	Descriptions	
11b and 11bg modes only	Data Rate	From the drop-down list, select the transmit data rate of the wireless network. The default setting is Best. For a list of all options that you can select from in 11b mode and 11bg mode, see *Factory Default Settings* on page 142.
Output Power	From the drop-down list, select the transmission power of the wireless access point: Full, Half, Quarter, Eighth, Minimum. The default is Full. **Note:** Increasing the power improves performance, but if two or more wireless access points are operating in the same area and on the same channel, interference can occur. **Note:** Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.	

6. Click **Apply** to save your settings and enable the selected wireless mode.

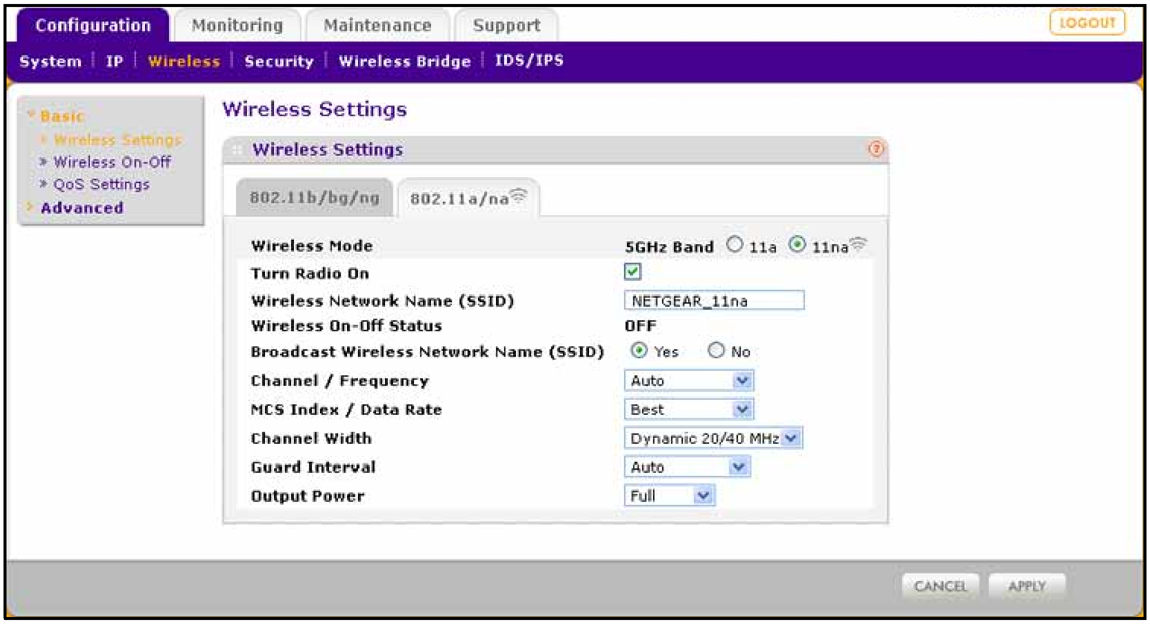
Note: For information about how to configure advanced wireless settings, see *Configure Advanced Wireless Settings* on page 107.

Configure 802.11a/na Wireless Settings

➢ **To configure the 802.11a/na wireless settings:**

1. Select **Configuration > Wireless > Basic > Wireless Settings**. The basic Wireless Settings screen displays. (The following figure shows the 802.11na settings.)

Note: The radio wave icon (📶) displays next to the selected radio mode.



Wireless Settings

Wireless Settings

Wireless Mode	5GHz Band ○ 11a ● 11na
Turn Radio On	☑
Wireless Network Name (SSID)	NETGEAR_11na
Wireless On-Off Status	OFF
Broadcast Wireless Network Name (SSID)	● Yes ○ No
Channel / Frequency	Auto
MCS Index / Data Rate	Best
Channel Width	Dynamic 20/40 MHz
Guard Interval	Auto
Output Power	Full

Figure 16.

2. Specify the wireless mode in the 5 GHz band by selecting one of the following radio buttons:
   - **11a**. 802.11n-compliant devices can connect to the access point because they are backward compatible.
   - **11na**. This is the default setting. If you keep the default setting, go to *Step 5*.

   When you change the wireless mode, the Turn Radio On check box is automatically cleared, and all fields, buttons, and drop-down lists onscreen are masked out.

3. Turn on the radio by selecting the **Turn Radio On** check box. A pop-up screen displays.

   Note: *Under normal conditions, you want the radio to be turned on. Turning off the radio disables access through the wireless access point, which can be helpful for configuration, network tuning, or troubleshooting activities.*

4. Click **OK** to confirm the change of wireless mode. The change does not take effect until you click the Apply button after you have completed the wireless configuration.

5. Specify the remaining wireless settings as explained the following table:

Table 7. Basic 5 GHz band wireless settings

<table>
<tr><th>Setting</th><th colspan="2">Descriptions</th></tr>
<tr><td>Wireless Network Name (SSID)</td><td colspan="2">Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. The default is NETGEAR_11na. The SSID assigned to a wireless device needs to match the wireless access point’s SSID for the wireless device to communicate with the wireless access point. If the SSIDs do not match, you do not get a wireless connection to the wireless access point.</td></tr>
<tr><td>Wireless On-Off Status</td><td colspan="2">This is a nonconfigurable field that shows the status of the wireless scheduler. For more information, see *Schedule the Wireless Radio to Be Turned Off* on page 61.</td></tr>
<tr><td>Broadcast Wireless Network Name (SSID)</td><td colspan="2">Select the **Yes** radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point’s SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the **No** radio button.</td></tr>
<tr><td>Channel / Frequency</td><td colspan="2">From the drop-down list, select the channel you wish to use on your wireless LAN. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto.
Note: It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see the guidelines following this table.
Note: For more information about available channels and frequencies, see *Technical Specifications* on page 139.</td></tr>
<tr><td rowspan="3">11na mode only
Note: For most networks, the default settings work fine.</td><td>MCS Index / Data Rate</td><td>From the drop-down list, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the wireless network. The default setting is Best. For a list of all options that you can select from in 11na mode, see *Factory Default Settings* on page 142.</td></tr>
<tr><td>Channel Width</td><td>From the drop-down list, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, and 40 MHz. The default is Dynamic 20/40 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz.</td></tr>
<tr><td>Guard Interval</td><td>From the drop-down list, select the guard interval to protect transmissions from interference. The default is Auto, or you can select Long - 800 ns. Some legacy devices can operate only with a long guard interval.</td></tr>
</table>

Table 7. Basic 5 GHz band wireless settings (continued)

Setting	Descriptions	
11a mode only	Data Rate	From the drop-down list, select the transmit data rate of the wireless network. The default setting is Best. For a list of all options that you can select from in 11a mode, see *Factory Default Settings* on page 142.
Output Power	From the drop-down list, select the transmission power of the wireless access point: Full, Half, Quarter, Eighth, Minimum. The default is Full. **Note:** Increasing the power improves performance, but if two or more wireless access points are operating in the same area and on the same channel, interference can occur. **Note:** Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.	

6. Click **Apply** to save your settings and enable the selected wireless mode.

Note: For information about how to configure advanced wireless settings, see *Configure Advanced Wireless Settings* on page 107.

Test Basic Wireless Connectivity

After you have configured the wireless access point as explained in the previous sections, test the computers on your LAN for wireless connectivity before you position and mount the wireless access point at its permanent position.

➢ **To test for wireless connectivity:**

1. Configure the 802.11b/g/n or 802.11a/n wireless adapters of your computers so that they all have the same SSID and channel that you have configured on the wireless access point.
2. Verify that your computers have a wireless link to the wireless access point. If you have enabled the DHCP server on the wireless access point, verify that your computers are able to obtain an IP address through DHCP from the wireless access point.
3. Verify network connectivity by using a browser such as Internet Explorer 6.0 or later or Mozilla Firefox 1.5 or later to browse the Internet, or check for file and printer access on your network.

Note: If you have trouble connecting to the wireless access point, see *Chapter 6, Troubleshooting*.

NETGEAR recommends that you complete the following tasks before you deploy the wireless access point in your network:

- Configure wireless security and other wireless features as described in *Chapter 3, Wireless Configuration and Security*.
- Configure any additional features that you might need as described in *Chapter 4, Management and Monitoring*, and *Chapter 5, Advanced Configuration*.

After you have completed the configuration of the wireless access point, you can reconfigure the computer that you used for this process back to its original TCP/IP settings.

Mount the Wireless Access Point

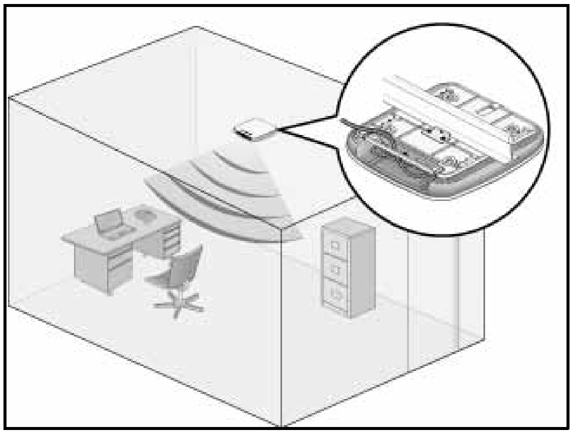
- *Ceiling Installation*
- *Wall Installation*
- *Desk Installation*

Note: NETGEAR recommends that you review the information in *Wireless Equipment Placement and Range Guidelines* on page 17 before you mount the wireless access point at its permanent position.

Note: The figures in the procedures in this section do not show the WNDAP620 wireless access point. However, the procedures are generic and do apply to the WNDAP620 wireless access point.

Ceiling Installation

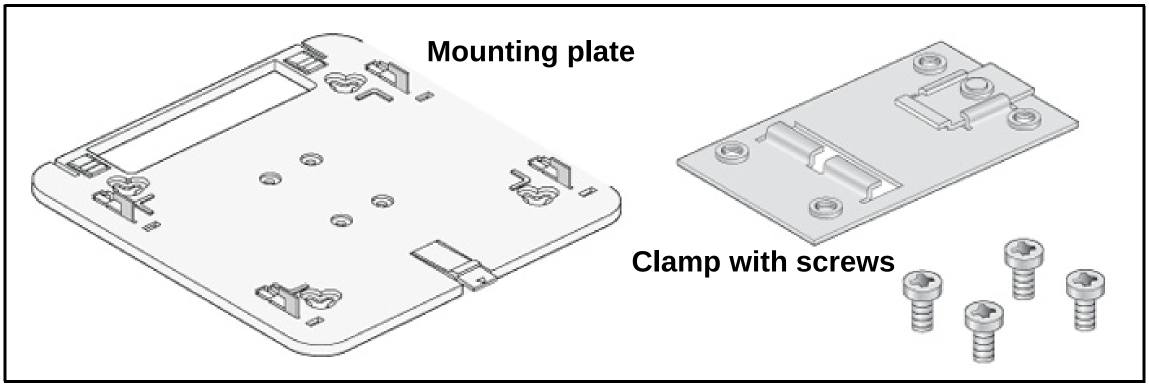
The best location for ceiling installation is at the center of your wireless coverage area, and within line of sight of all mobile devices. Make sure the top (the dome side) of the wireless access point is directed toward the users and not the ceiling.



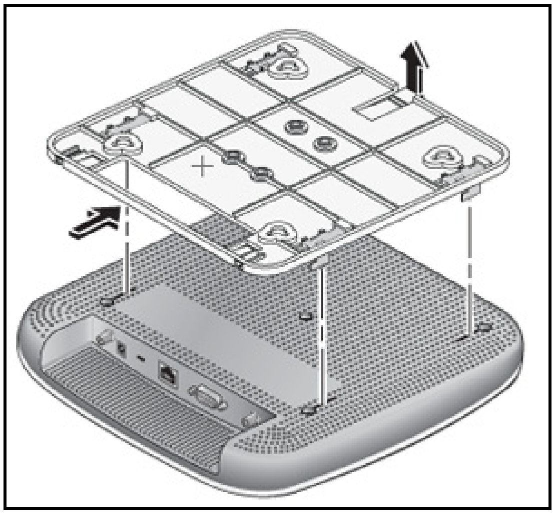
Note: Do not place the wireless access point in a false ceiling space facing up.

➢ To install the wireless access point using the ceiling installation kit:

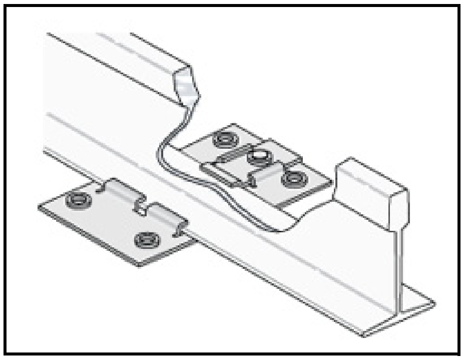
1. Verify the package contents of the ceiling installation kit.



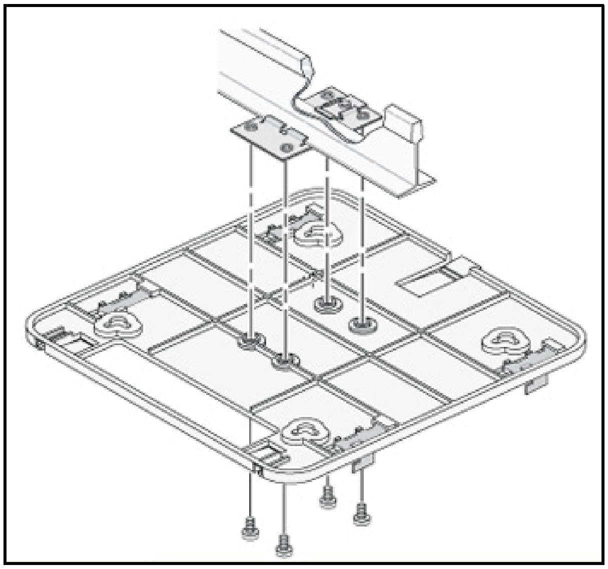
2. Detach the mounting plate from the wireless access point.



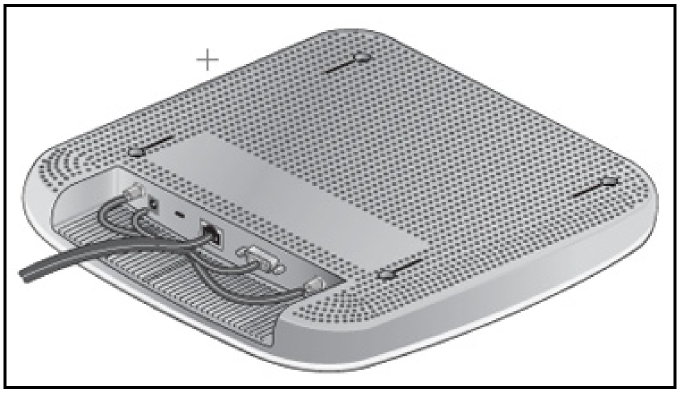
3. Attach the clamp to the ceiling rail.



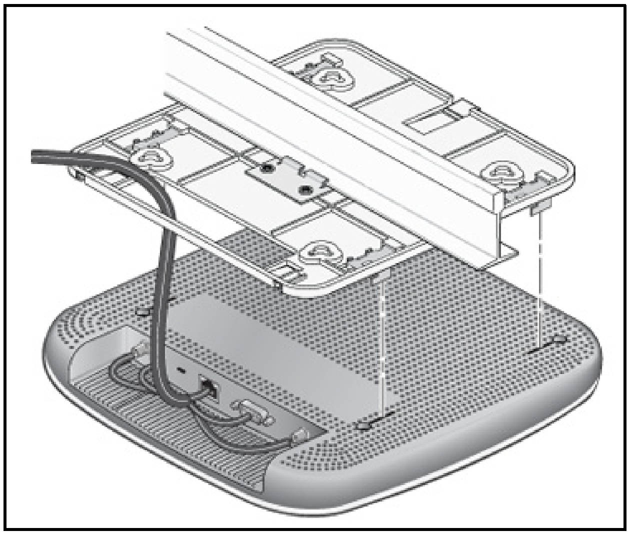
4. Attach the mounting plate to the clamp.



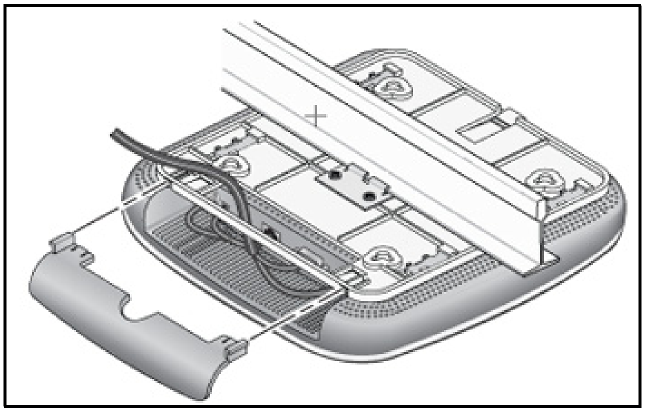
5. Connect the cables to the wireless access point.



6. Attach the wireless access point to the mounting plate.

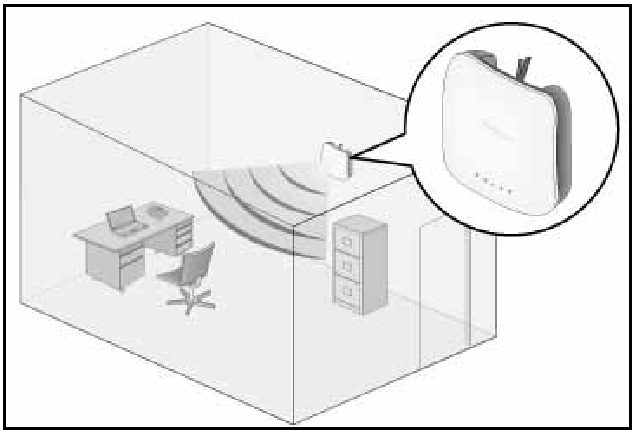


7. Attach the cover to the wireless access point.



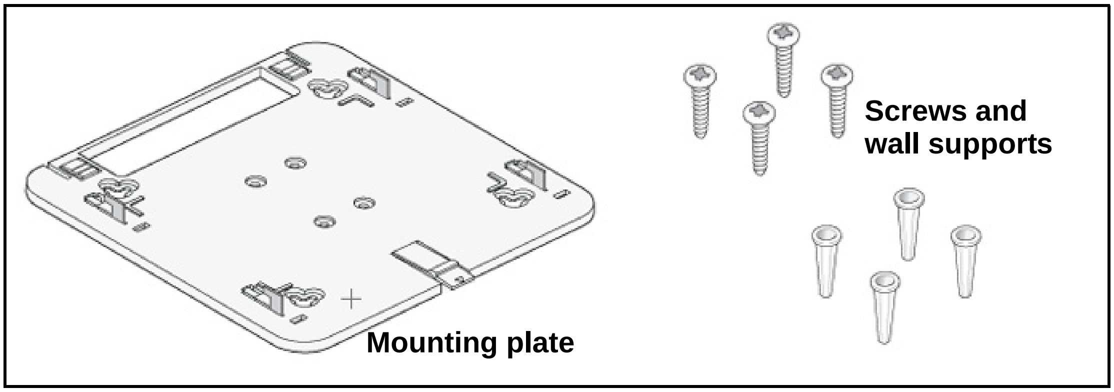
Wall Installation

The best location for wall installation is at the center of your wireless coverage area, and within line of sight of all mobile devices. Make sure the top (the dome side) of the wireless access point is directed toward the users and not the wall.

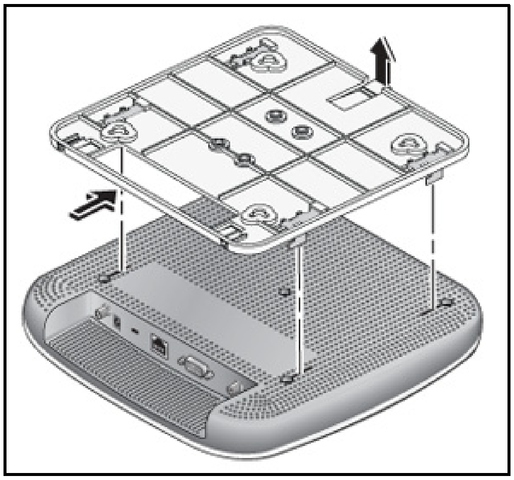


➢ **To install the wireless access point using the wall installation kit:**

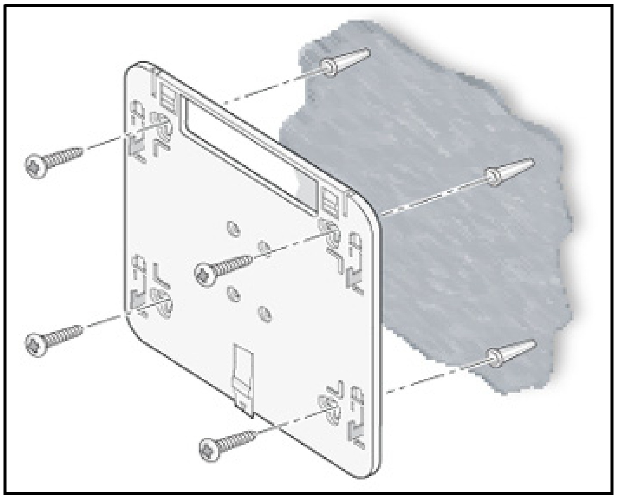
1. Verify the package contents of the wall installation kit.



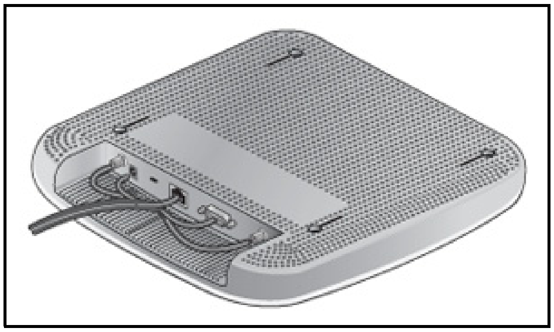
2. Detach the mounting plate from the wireless access point.



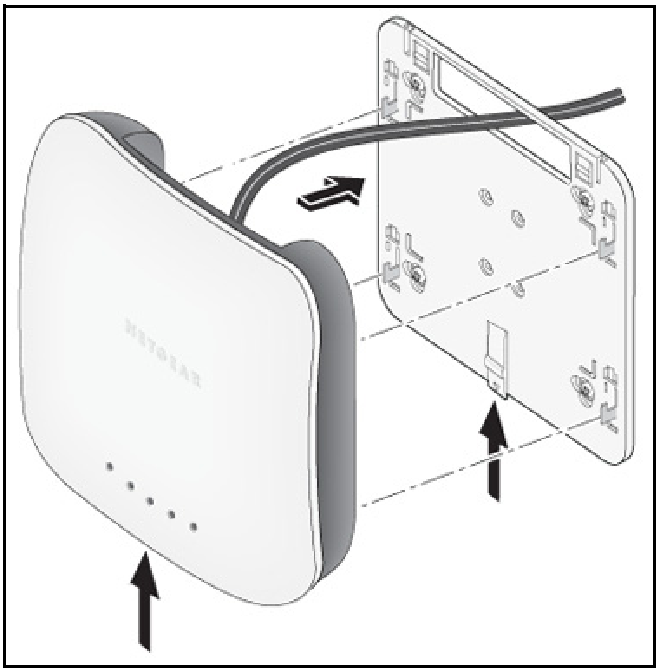
3. Attach the mounting plate to the wall.



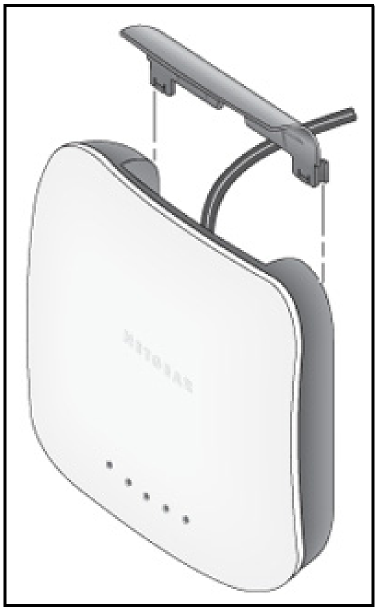
4. Connect the cables to the wireless access point.



5. Attach the wireless access point to the mounting plate.



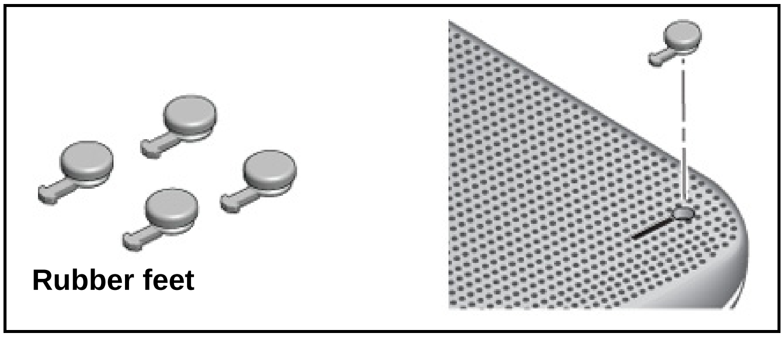
6. Attach the cover to the wireless access point.



Desk Installation

➤ **To install the wireless access point on a desk:**

Attach the rubber feet to the holes in the bottom of the wireless access point.



Wireless Configuration and Security

3

This chapter describes how to configure the wireless features of the wireless access point. The chapter includes the following sections:

- *Wireless Data Security Options*
- *Security Profiles*
- *Configure RADIUS Server Settings*
- *Restrict Wireless Access by MAC Address*
- *Schedule the Wireless Radio to Be Turned Off*
- *Configure Basic Wireless Quality of Service*

Before you set up wireless security and additional wireless features that are described in this chapter, connect the wireless access point, get the Internet connection working, and configure the 802.11b, 11bg, or 11ng wireless settings and the 802.11a or 11na wireless settings as described in *Chapter 2, Installation and Basic Configuration*. The wireless access point functions with an Ethernet LAN connection. Make sure that you have verified wireless connectivity before you set up wireless security and additional wireless features.

WARNING:

If you are configuring the wireless access point from a wireless computer and you change the wireless access point's SSID, channel, or wireless security settings, you lose your wireless connection when you click Apply. You then need to change the wireless settings of your computer to match the wireless access point's new settings.

Wireless Data Security Options

Indoors, computers can connect over 802.11n wireless networks at a maximum range of 300 feet. Typically, a wireless access point inside a building works best with devices within a 100-foot radius. Such distances can allow for others outside 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 wireless access point provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs.

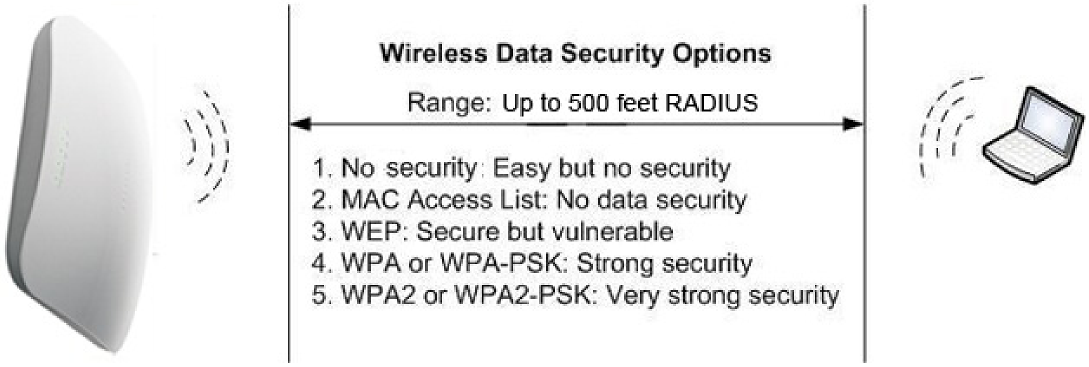

Wireless Data Security Options
Range: Up to 500 feet RADIUS
1. No security: Easy but no security
2. MAC Access List: No data security
3. WEP: Secure but vulnerable
4. WPA or WPA-PSK: Strong security
5. WPA2 or WPA2-PSK: Very strong security

Figure 17.

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

- **Use multiple BSSIDs combined with VLANs**. You can configure combinations of VLANS and BSSIDs (security profiles) with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network. For information about how to configure BSSIDs, see *Configure and Enable Security Profiles* on page 48.
- **Restrict access based by MAC address**. You can allow only trusted devices to connect so that unknown devices cannot wirelessly connect to the wireless access point. 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. For information about how to restrict access by MAC address, see *Restrict Wireless Access by MAC Address* on page 60.
- **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 exposed. For information about how to turn off broadcast of the SSID, see *Configure and Enable Security Profiles* on page 48.
- **WEP**. Wired Equivalent Privacy (WEP) data encryption provides data security. WEP shared key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK. For information about how to configure WEP, see *Configure and Enable Security Profiles* on page 48 and *Configure an Open System with WEP or Shared Key with WEP* on page 53.
- **Legacy 802.1X**. Legacy 802.1X uses RADIUS-based 802.1x authentication but no data encryption. For information about how to configure Legacy 802.1X, see *Configure and Enable Security Profiles* on page 48 and *Configure Legacy 802.1X* on page 54.

- **WPA and WPA-PSK (TKIP)**. Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. The very strong authentication along with dynamic per-frame rekeying of WPA makes it virtually impossible to compromise.

  WPA uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 48 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 55.

  WPA-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 48 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 56.

- **WPA2 and WPA2-PSK (AES)**. Wi-Fi Protected Access version 2 (WPA2) data encryption provides strong data security with Advanced Encryption Standard (AES) encryption. The very strong authentication along with dynamic per-frame rekeying of WPA2 makes it virtually impossible to compromise.

  WPA2 uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 48 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 55.

  WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 48 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 56.

- **WPA & WPA2 and WPA-PSK & WPA2-PSK mixed modes**. These modes support data encryption either with both WPA and WPA2 clients or with both WPA-PSK and WPA2-PSK clients and provide the most reliable security.

  WPA & WPA2 uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 48 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 55.

  WPA-PSK & WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 48 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 56.

Security Profiles

- *Before You Change the SSID, WEP, and WPA Settings*
- *Configure and Enable Security Profiles*

Security profiles let you configure unique security settings for each SSID on each radio of the wireless access point. For each radio, the wireless access point supports up to eight security profiles (BSSIDs) that you can configure on the individual Edit Wireless Network screens that are accessible from the Edit Security Profile screen (see *Configure and Enable Security Profiles* on page 48).

To set up a security profile, select its network authentication type, data encryption, wireless client security separation, and VLAN ID:

- **Network authentication**
  The wireless access point is set by default as an open system with no authentication. When you configure network authentication, bear in mind that not all wireless adapters support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions about how to configure WPA2 settings.

  For information about the types of network authentication that the wireless access point supports, see *Configure and Enable Security Profiles* on page 48.

- **Data encryption**
  Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data encryption settings are explained in *Configure and Enable Security Profiles* on page 48.
- **Wireless client security separation**
  If this feature is enabled, the associated wireless clients (using the same SSID) are not able to communicate with each other. This feature is useful for hotspots and other public access situations. By default, wireless client separation is disabled. For more information, see *Configure and Enable Security Profiles* on page 48.
- **VLAN ID**
  If this feature is enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802.1Q) standard, the default VLAN ID for the wireless access point is associated with each profile. The default VLAN ID needs to match the IDs that are used by the other network devices. For more information, see *Configure and Enable Security Profiles* on page 48.

Some concepts and guidelines regarding the SSID are explained in the following list:

- A basic service set (BSS) is a group of wireless stations and a single wireless access point, all using the same security profile or service set identifier (BSSID). The actual identifier in the BSSID is the MAC address of the wireless radio. (A wireless radio can have multiple MAC addresses, one for each security profile.)
- An extended service set (ESS) is a group of wireless stations and multiple wireless access points, all using the same identifier (ESSID).
- Different wireless access points within an ESS can use different channels. To reduce interference, adjacent wireless access points should use different channels.
- Roaming is the ability of wireless stations to connect wirelessly when they physically move from one BSS to another one within the same ESS. The wireless station automatically changes to the wireless access point with the least interference or best performance.

Before You Change the SSID, WEP, and WPA Settings

For a new wireless network, print or copy one of the following forms and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the country or region correctly as the first step.

Form for 802.11b/bg/ng Modes

Print this page and store the security information in a safe place:

- **SSID**: The service set identifier (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: ____________________________________

  The SSID in the wireless access point is the SSID you configure on the wireless adapter card. All wireless nodes in the same network need to be configured with the same SSID.

- **WEP key size and authentication**
  Choose the key size by circling one: 64, 128, or 152 bits.
  Choose the authentication type by circling one: open system or shared key.

  Passphrase: ____________________________________

  Note: If you select shared key, the other devices in the network cannot connect unless they are set to shared key and have the same keys in the same positions as those in the wireless access point.

- **WPA-PSK (pre-shared key) and WPA2-PSK**
  Record the WPA-PSK passphrase:

  WPA-PSK passphrase: _________________________________

  Record the WPA2-PSK passphrase:

  WPA2-PSK passphrase: _________________________________

- **WPA RADIUS settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary ________________ Secondary _________________

  Port: ____________________________________

  Shared secret: ____________________________________

- **WPA2 RADIUS settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary ________________ Secondary _________________

  Port: ____________________________________

  Shared secret: ____________________________________

  ---End of Form--

Form for 802.11a/an Modes

Print this page and store the security information in a safe place:

- **SSID**: The service set identifier (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumeric characters. Write your SSID on the line.

  SSID: ____________________________________

  The SSID in the wireless access point is the SSID you configure on the wireless adapter card. All wireless nodes in the same network need to be configured with the same SSID.

- **WEP key size and authentication**
  Choose the key size by circling one: 64, 128, or 152 bits.
  Choose the authentication type by circling one: open system or shared key.

  Passphrase: ____________________________________

  Note: If you select shared key, the other devices in the network cannot connect unless they are set to shared key and have the same keys in the same positions as those in the wireless access point.

- **WPA-PSK (pre-shared key) and WPA2-PSK**
  Record the WPA-PSK passphrase:

  WPA-PSK passphrase: _________________________________

  Record the WPA2-PSK passphrase:

  WPA2-PSK passphrase: _________________________________

- **WPA RADIUS settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary ________________ Secondary _________________

  Port: ____________________________________

  Shared secret: ____________________________________

- **WPA2 RADIUS settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:

  Server name/IP address: Primary ________________ Secondary _________________

  Port: ____________________________________

  Shared secret: ____________________________________

  --End of Form--

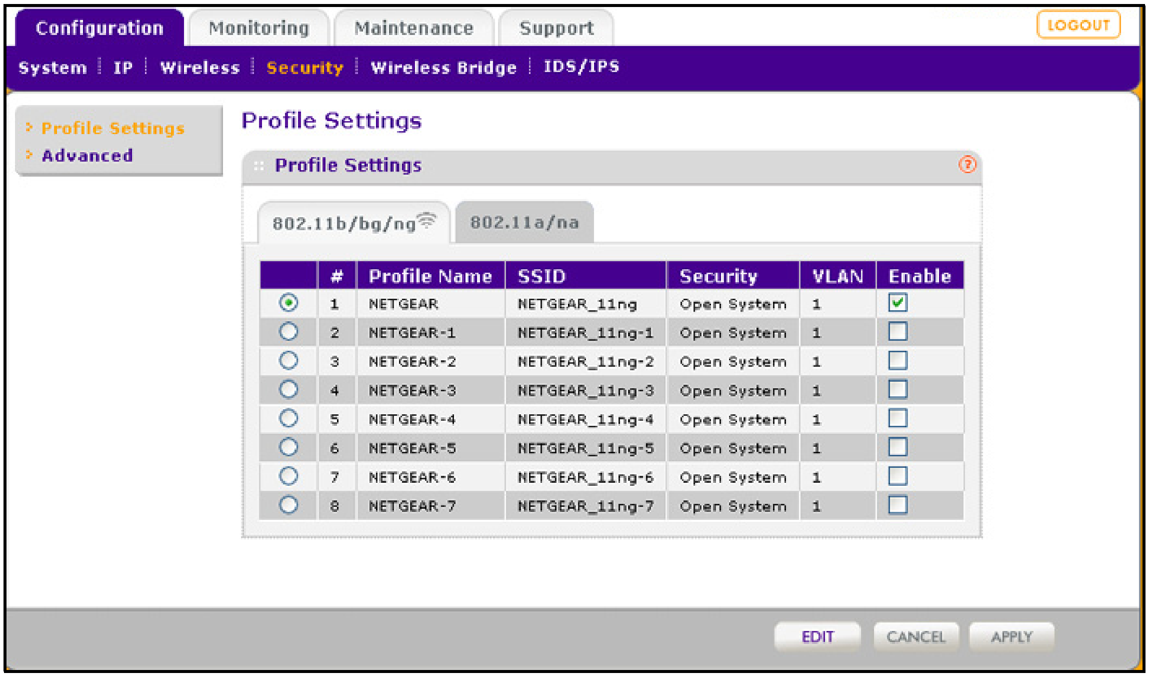
Configure and Enable Security Profiles

To configure and enable a security profile, you need to enable the associated radio:

- For 802.11b/bg/ng modes, the 2.4 GHz radio needs to be enabled (see *Configure 802.11b/bg/ng Wireless Settings* on page 28).
- For 802.11a/na modes, the 5 GHz radio needs to be enabled. (see *Configure 802.11a/na Wireless Settings* on page 31).

➢ To configure and enable a security profile:

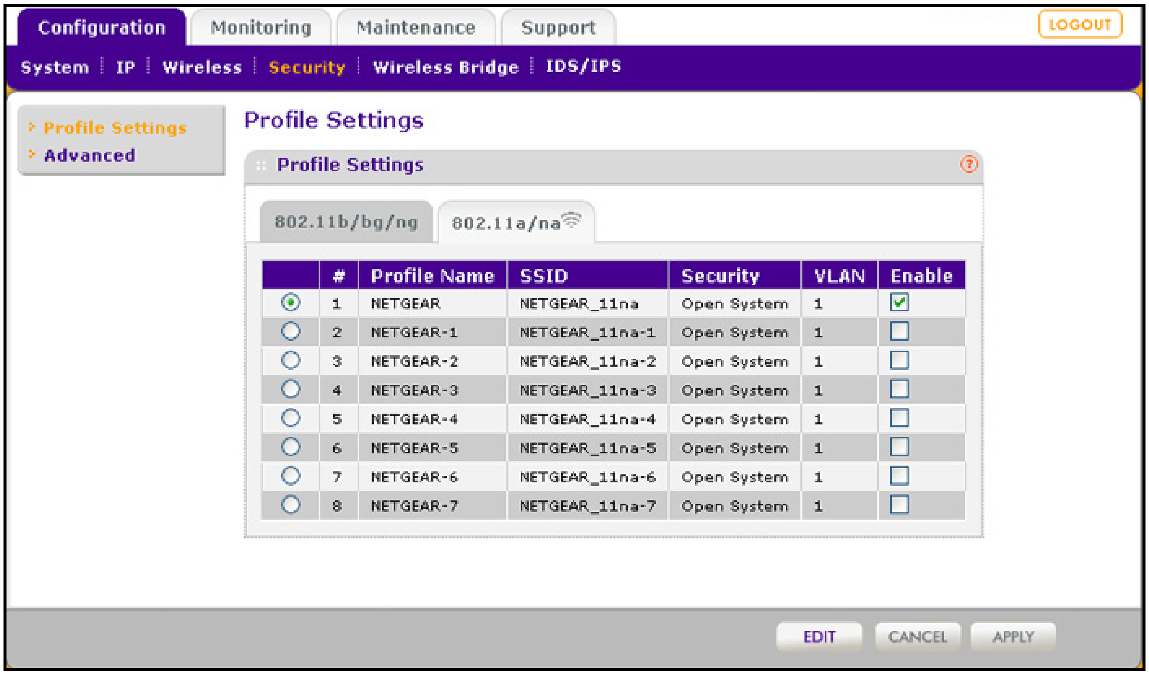
1. Select **Configuration > Security > Profile Settings**. The Profile Settings screen for the 802.11b/bg/ng modes displays, showing eight wireless security profiles. (If the 2.4 GHz radio is disabled, the Enable column is masked out.)



	#	Profile Name	SSID	Security	VLAN	Enable
●	1	NETGEAR	NETGEAR_11ng	Open System	1	☑
○	2	NETGEAR-1	NETGEAR_11ng-1	Open System	1	□
○	3	NETGEAR-2	NETGEAR_11ng-2	Open System	1	□
○	4	NETGEAR-3	NETGEAR_11ng-3	Open System	1	□
○	5	NETGEAR-4	NETGEAR_11ng-4	Open System	1	□
○	6	NETGEAR-5	NETGEAR_11ng-5	Open System	1	□
○	7	NETGEAR-6	NETGEAR_11ng-6	Open System	1	□
○	8	NETGEAR-7	NETGEAR_11ng-7	Open System	1	□

Figure 18.

2. Optional: To display the Profile Settings screen for the 802.11a/na modes, click the **802.11a/na** tab. This screen also shows eight wireless security profiles. (If the 5 GHz radio is disabled, the Enable column is masked out.)



	#	Profile Name	SSID	Security	VLAN	Enable
●	1	NETGEAR	NETGEAR_11na	Open System	1	☑
○	2	NETGEAR-1	NETGEAR_11na-1	Open System	1	□
○	3	NETGEAR-2	NETGEAR_11na-2	Open System	1	□
○	4	NETGEAR-3	NETGEAR_11na-3	Open System	1	□
○	5	NETGEAR-4	NETGEAR_11na-4	Open System	1	□
○	6	NETGEAR-5	NETGEAR_11na-5	Open System	1	□
○	7	NETGEAR-6	NETGEAR_11na-6	Open System	1	□
○	8	NETGEAR-7	NETGEAR_11na-7	Open System	1	□

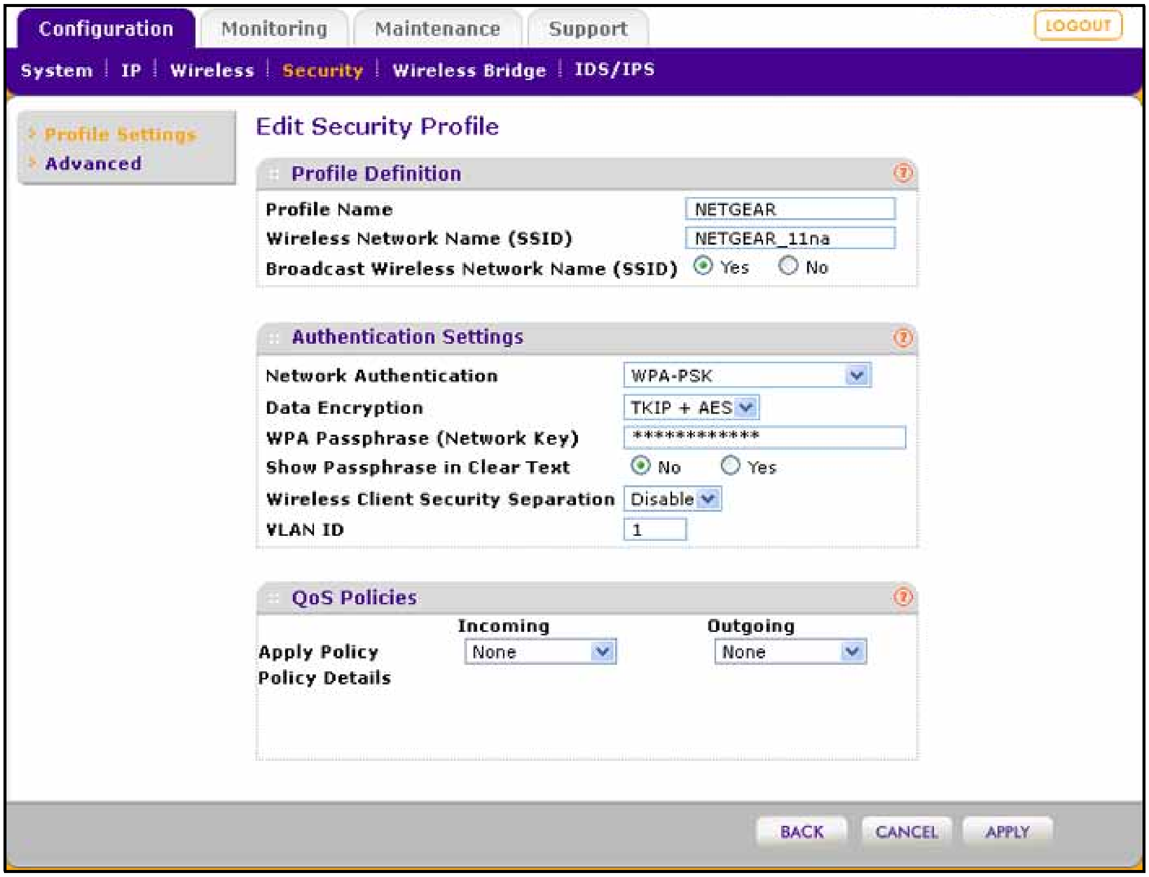
Figure 19.

The following table explains the fields of the Profile Settings screen:

Table 8. Profile settings

Setting	Description
Profile Name	The unique name of the wireless security profile that makes it easy to recognize the profile.
SSID	The wireless network name (SSID) for the wireless security profile.
Security	The configured wireless authentication method for the wireless security profile.
VLAN	The default VLAN ID that is associated with the wireless security profile.
Enable	The check box that lets you select the wireless security profile so you can enable it by clicking **Apply**.

3. To configure a wireless security profile, select the corresponding radio button to the left of the wireless security profile. The Edit Security Profile screen opens for the selected wireless security profile (see the following figure). The screen has three sections:
   - Profile Definition (see *Step 4*)
   - Authentication Settings (see *Step 5*)
   - QoS Policies (see *Step 6*)



Edit Security Profile

Profile Definition

Profile Name	NETGEAR
Wireless Network Name (SSID)	NETGEAR_11na
Broadcast Wireless Network Name (SSID)	● Yes ○ No

Authentication Settings

Network Authentication	WPA-PSK
Data Encryption	TKIP + AES
WPA Passphrase (Network Key)	************
Show Passphrase in Clear Text	● No ○ Yes
Wireless Client Security Separation	Disable
VLAN ID	1

QoS Policies

	Incoming	Outgoing
Apply Policy	None	None
Policy Details		

Figure 20.

4. Specify the settings of the Profile Definition section of the Edit Security Profile screen as explained in the following table:

Table 9. Profile definition settings

Setting	Description
Profile Name	Enter a unique name of the wireless security profile that makes it easy to recognize the profile. The default names are NETGEAR, NETGEAR-1, NETGEAR-2, and so on, through NETGEAR-7. You can enter a value of up to 32 alphanumeric characters.
Wireless Network Name (SSID)	The wireless network name (SSID) for the wireless security profile. The default names depend on the selected radio band: • **802.11b/bg/ng**. The default names are NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, and so on, through NETGEAR_11ng-7 for the eighth profile. • **802.11a/na**. The default names are NETGEAR_11na, NETGEAR_11na-1, NETGEAR_11na-2, and so on, through NETGEAR_11na-7 for the eighth profile.

Table 9. Profile definition settings (continued)

Setting	Description
Broadcast Wireless Network Name (SSID)	Select the **Yes** radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the **No** radio button.

5. Specify the settings of the Authentication Settings section of the Edit Security Profile screen as explained in the following table.

   The wireless access point is set by default as an open system with no authentication. When you configure network authentication, bear in mind the following:

   - If you are using access point mode (which is the default mode if you did not enable wireless bridging), then all options are available. In other modes such as bridge mode, some options might be unavailable.
   - Not all wireless adapters support WPA or WPA2. Windows XP, Windows 2000 with Service Pack 3, and Windows Vista do include the client software that supports WPA. However, client software is required on the client. Consult the product documentation for your wireless adapter and WPA or WPA2 client software for instructions about how to configure WPA2 settings.

Table 10. Profile authentication settings

Setting	Description	
Network Authentication and Data Encryption **Note:** The data encryption fields that display onscreen depend on your selection from the Network Authentication drop-down list.	Open System	This is the default setting. Use an open system without any encryption or with WEP encryption. See *Configure an Open System with WEP or Shared Key with WEP* on page 53.
	Shared Key	Use WEP encryption and enter at least one shared key. See *Configure an Open System with WEP or Shared Key with WEP* on page 53.
	Legacy 802.1X	Configure the RADIUS server settings. Encryption is not supported. See *Configure Legacy 802.1X* on page 54.
	WPA with Radius	Configure the RADIUS server settings and select TKIP or TKIP + AES encryption. See *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 55.
	WPA2 with Radius	Configure the RADIUS server settings and select AES or TKIP + AES encryption. See *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 55. **Note:** Select this setting only if all clients support WPA2.

Table 10. Profile authentication settings (continued)

Setting	Description	
Network Authentication and Data Encryption (continued)	WPA & WPA2 with Radius	Configure the RADIUS server setting. TKIP + AES encryption is the default encryption. See *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 55. **Note:** This setting allows clients to connect through either WPA with TKIP or WPA2 with AES.
	WPA-PSK	Enter a WPA passphrase and select TKIP or TKIP + AES encryption. See *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 56.
	WPA2-PSK	Enter a WPA passphrase and select AES or TKIP + AES encryption. See *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 56. **Note:** Select this setting only if all clients support WPA2.
	WPA-PSK & WPA2-PSK	Enter a WPA passphrase. TKIP + AES encryption is the default encryption. See *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 56. **Note:** This setting allows clients to connect through either WPA with TKIP or WPA2 with AES.
Wireless Client Security Separation	If you enable wireless client security separation by selecting Enable from the drop-down list, the associated wireless clients cannot communicate with each other. By default, Disable is selected from the drop-down list. This feature is intended for hotspots and other public access situations.	
VLAN ID	Enter the VLAN ID to be associated with this wireless security profile. The default VLAN ID is 1. The VLAN ID needs to match the VLAN ID that is used by the other devices in your network.	

6. Optional: In the QoS Policies section of the screen, select a QoS policy from the Incoming drop-down list, Outgoing drop-down list, or both. Depending on your selection, the policy is applied to incoming packets, outgoing packets, or both incoming and outgoing packets, and is displayed in the Policy Details fields.

   Note: *To be able to select a QoS policy, you first need to have configured one or more policies (see Configure Quality of Service Policies on page 112).*

7. Click **Apply** to save your settings.

WARNING:

If you use a wireless computer to configure wireless security settings, you are disconnected when you click Apply. Reconfigure your wireless computer to match the new settings, or access the wireless access point from a wired computer to make further changes.

➤ **To change the QoS policy selection on the Edit Security Profile screen:**

1. From the drop-down list from which you want select another QoS policy, select **None**.
2. Click **Apply** to remove the old policy from the security profile.
3. Select the new QoS policy from the same drop-down list.
4. Click **Apply** to save your settings.

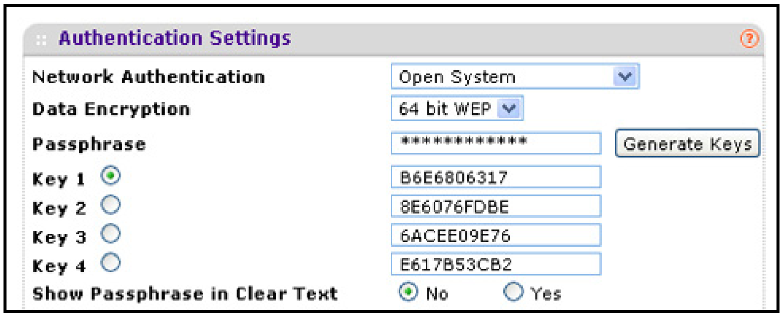
Configure an Open System with WEP or Shared Key with WEP

Whether you use an open system with WEP or shared key with WEP, configure the settings that are explained in the following table.

- **Open system with WEP**

  An open system can function without any encryption or with pre-shared WEP key encryption without RADIUS authentication. The security level of static WEP is not very strong.

  When you select Open System from the Network Authentication drop-down list and any selection other than None from the Data Encryption drop-down list, the screen expands to display the WEP fields:



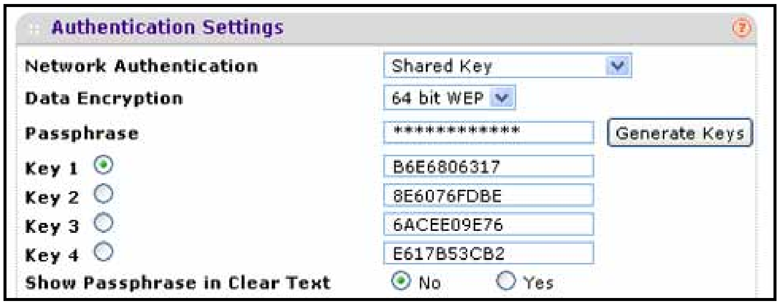
Authentication Settings

Network Authentication	Open System
Data Encryption	64 bit WEP
Passphrase	************ Generate Keys
Key 1 ●	B6E6806317
Key 2 ○	8E6076FDBE
Key 3 ○	6ACEE09E76
Key 4 ○	E617B53CB2
Show Passphrase in Clear Text	● No ○ Yes

Figure 21.

- **Shared key with WEP**

  Shared key provides pre-shared WEP key encryption without RADIUS authentication. The security level of static WEP is not very strong. When you select Shared Key from the Network Authentication drop-down list, the screen expands to display the WEP fields:



Authentication Settings

Network Authentication	Shared Key	
Data Encryption	64 bit WEP	
Passphrase	************	Generate Keys
Key 1 ●	B6E6806317	
Key 2 ○	8E6076FDBE	
Key 3 ○	6ACEE09E76	
Key 4 ○	E617B53CB2	
Show Passphrase in Clear Text	● No ○ Yes	

Figure 22.

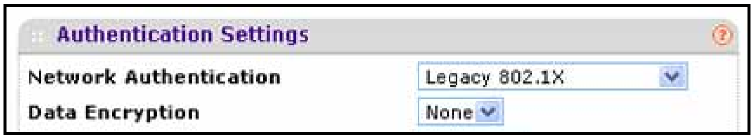
Table 11. WEP encryption settings

Setting	Descriptions
Data Encryption	Select the encryption key size from the drop-down list: • **64-bit WEP**. Standard WEP encryption, using 40/64-bit encryption. • **128-bit WEP**. Standard WEP encryption, using 104/128-bit encryption. • **152-bit WEP**. Proprietary WEP encryption mode, using 128+24 bit encryption. This mode functions only with other wireless stations that support this mode.
Passphrase	Enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). The secret passphrase allows you to generate the keys automatically by clicking **Generate Keys**. The default passphrase is sharedsecret. You can display the actual passphrase by selecting the Show Passphrase in Clear Text **Yes** radio button.
Encryption Key (Key1–Key4)	Either enter a key manually or allow the key to be automatically generated by clicking **Generate Keys**. • For ASCII format, depending on the key size selected, the manually entered encryption key needs to have a length of 5 (64-bit WEP), 13 (128-bit WEP), or 16 characters (152-bit WEP). • For HEX format, depending on the key size selected, the manually entered or automatically generated encryption key needs to have a length of 10 (64-bit WEP), 26 (128-bit WEP), or 32 (152-bit WEP) characters. **Note:** Wireless stations need to use the key to access the wireless access point.
Show Passphrase in Clear Text	Select the **Yes** radio button to display the actual passphrase in the Passphrase field. The default setting is No.

Configure Legacy 802.1X

To use legacy 802.1X security, you need to define RADIUS server settings. For information about RADIUS servers, see *Configure RADIUS Server Settings* on page 57.

When you select Legacy 802.1X from the Network Authentication drop-down list, the Data Encryption drop-down list is automatically set to None. To use legacy 802.1X security, you need to define the RADIUS servers only.



Authentication Settings

Network Authentication: Legacy 802.1X

Data Encryption: None

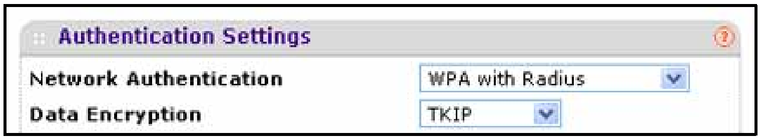
Figure 23.

Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS

WPA, WPA2, and WPA & WPA2 security requires RADIUS-based 802.1x authentication, so you also need to define RADIUS server settings. For information about RADIUS servers, see *Configure RADIUS Server Settings* on page 57.

The selections that are available from the Data Encryption drop-down list depend on the type of WPA authentication that you select from the Network Authentication drop-down list and are shown in the table that follows the figures.

- **WPA with RADIUS**



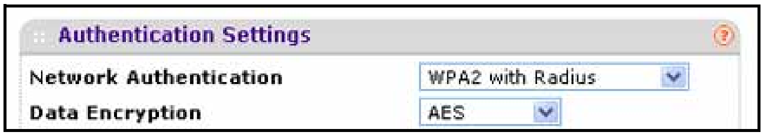
Authentication Settings

Network Authentication: WPA with Radius

Data Encryption: TKIP

Figure 24.

- **WPA2 with RADIUS**



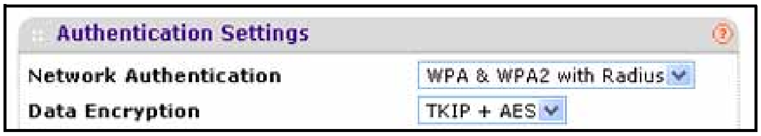
Authentication Settings

Network Authentication: WPA2 with Radius

Data Encryption: AES

Figure 25.

- **WPA & WPA2 with RADIUS**



Authentication Settings

Network Authentication: WPA & WPA2 with Radius

Data Encryption: TKIP + AES

Figure 26.

Table 12. Settings for WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS

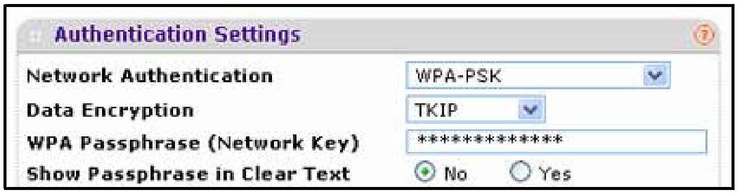
Setting	Descriptions
TKIP	Temporal Key Integrity Protocol (TKIP) is the standard encryption method used with WPA. You can also use TKIP with WPA2. **Note:** TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 authentication with AES encryption if you want to use the 11n rates and speed.
AES	Advanced Encryption Standard (AES) is the standard encryption method used with WPA2. **Note:** Although some wireless clients might support AES with WPA, the WNDAP620 wireless access point does not support WPA with AES.
TKIP + AES	The TKIP + AES encryption method is supported both for WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method.

Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK

WPA-PSK, WPA-PSK, and WPA-PSK & WPA2-PSK authentication use a pre-shared key (PSK, also called a passphrase or a network key) and do not require authentication from a RADIUS server.

The selections that are available from the Data Encryption drop-down list depend on the type of WPA-PSK authentication that you select from the Network Authentication drop-down list and are shown in the table that follows the figures.

- **WPA-PSK**

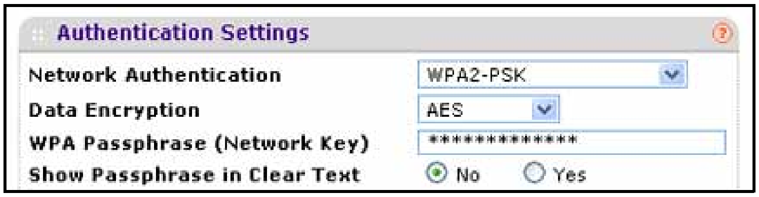


Authentication Settings

Network Authentication	WPA-PSK
Data Encryption	TKIP
WPA Passphrase (Network Key)	*************
Show Passphrase in Clear Text	● No ○ Yes

Figure 27.

- **WPA2-PSK**

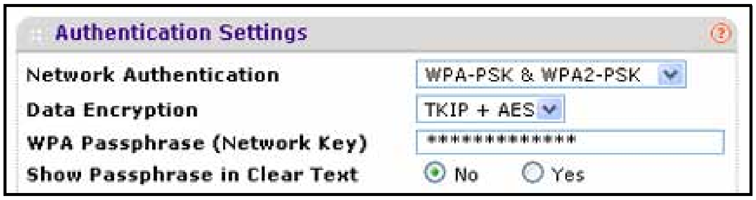


Authentication Settings

Network Authentication	WPA2-PSK
Data Encryption	AES
WPA Passphrase (Network Key)	*************
Show Passphrase in Clear Text	● No ○ Yes

Figure 28.

- **WPA-PSK & WPA2-PSK**



Authentication Settings

Network Authentication	WPA-PSK & WPA2-PSK
Data Encryption	TKIP + AES
WPA Passphrase (Network Key)	*************
Show Passphrase in Clear Text	● No ○ Yes

Figure 29.

Table 13. Settings for WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK

Setting	Descriptions	
Data Encryption	TKIP	Temporal Key Integrity Protocol (TKIP) is the standard encryption method used with WPA. You can also use TKIP with WPA2. **Note:** TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 authentication with AES encryption if you want to use the 11n rates and speed.
	AES	Advanced Encryption Standard (AES) is the standard encryption method used with WPA2. **Note:** Although some wireless clients might support AES with WPA, the WNDAP620 wireless access point does not support WPA with AES.
	TKIP + AES	TKIP + AES supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method.
Passphrase	Enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). The default passphrase is sharedsecret. You can display the actual passphrase by selecting the Show Passphrase in Clear Text **Yes** radio button.	
Show Passphrase in Clear Text	Select the **Yes** radio button to display the actual passphrase in the Passphrase field. The default setting is No.	

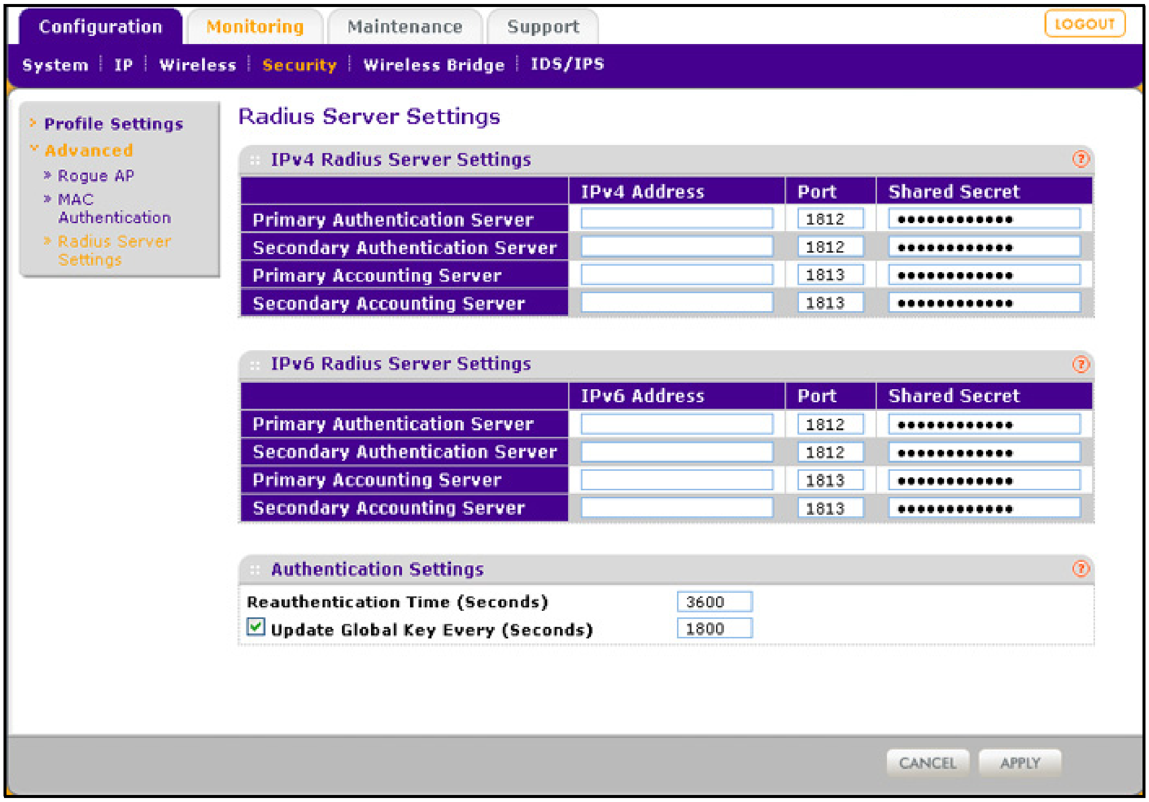
Configure RADIUS Server Settings

For authentication, accounting, or both authentication and accounting using RADIUS, you need to configure primary servers and optional secondary servers. These RADIUS server settings can apply to all devices that are connected to the wireless access point.

You can configure both IPv4 and IPv6 servers. In the IPv4 Radius Server Settings section, enter IPv4 addresses only; in the IPv6 Radius Server Settings section, enter IPv6 addresses only.

To configure the RADIUS server settings:

1. Select **Configuration > Security > Advanced > Radius Server Settings**. The Radius Server Settings screen displays.



Radius Server Settings

IPv4 Radius Server Settings

	IPv4 Address	Port	Shared Secret
Primary Authentication Server		1812	●●●●●●●●●●●●
Secondary Authentication Server		1812	●●●●●●●●●●●●
Primary Accounting Server		1813	●●●●●●●●●●●●
Secondary Accounting Server		1813	●●●●●●●●●●●●

IPv6 Radius Server Settings

	IPv6 Address	Port	Shared Secret
Primary Authentication Server		1812	●●●●●●●●●●●●
Secondary Authentication Server		1812	●●●●●●●●●●●●
Primary Accounting Server		1813	●●●●●●●●●●●●
Secondary Accounting Server		1813	●●●●●●●●●●●●

Authentication Settings

Reauthentication Time (Seconds) 3600

☑ Update Global Key Every (Seconds) 1800

Figure 30.

2. Specify the settings as explained in the following table:

Table 14. RADIUS server settings for IPv4 and IPv6

Setting	Descriptions	
Radius Server Settings		
Primary Authentication Server	IPv4 Address or IPv6 Address	Enter the IP address of the primary RADIUS server for authentication.
	Port	Enter the number of the UDP port on the wireless access point that is used to access the primary RADIUS server for authentication. The default port number is 1812.
	Shared Secret	Enter the shared key that is used between the wireless access point and the primary RADIUS server during authentication.

Table 14. RADIUS server settings for IPv4 and IPv6 (continued)

Setting	Descriptions	
Secondary Authentication Server	IPv4 Address or IPv6 Address	Enter the IP address of the secondary RADIUS server for authentication. The secondary RADIUS server is used when the primary RADIUS server is not available.
	Port	Enter the number of the UDP port on the wireless access point that is used to access the secondary RADIUS server for authentication. The default port number is 1812.
	Shared Secret	Enter the shared key that is used between the wireless access point and the secondary RADIUS server during authentication.
Primary Accounting Server	IPv4 Address or IPv6 Address	Enter the IP address of the primary RADIUS server for accounting.
	Port	Enter the number of the UDP port on the wireless access point that is used to access the primary RADIUS server for accounting. The default port number is 1813.
	Shared Secret	Enter the shared key that is used between the wireless access point and the primary RADIUS server during the accounting process.
Secondary Accounting Server	IPv4 Address or IPv6 Address	Enter the IP address of the secondary RADIUS server for accounting. The secondary RADIUS server is used when the primary RADIUS server is not available.
	Port	Enter the number of the UDP port on the wireless access point that is used to access the secondary RADIUS server for accounting. The default port number is 1813.
	Shared Secret	Enter the shared key that is used between the wireless access point and the secondary RADIUS server during the accounting process.
Authentication Settings		
Reauthentication Time (Seconds)	The interval in seconds after which the supplicant is reauthenticated with the RADIUS server. The default interval is 3600 seconds (1 hour). Enter **0** to disable reauthentication.	
Update Global Key Every (Seconds)	Select the check box to allow the global key update, and enter the interval in seconds. The check box is selected by default, and the default interval is 1800 seconds (30 minutes). Clear the check box to prevent the global key update.	

3. Click **Apply** to save your settings.

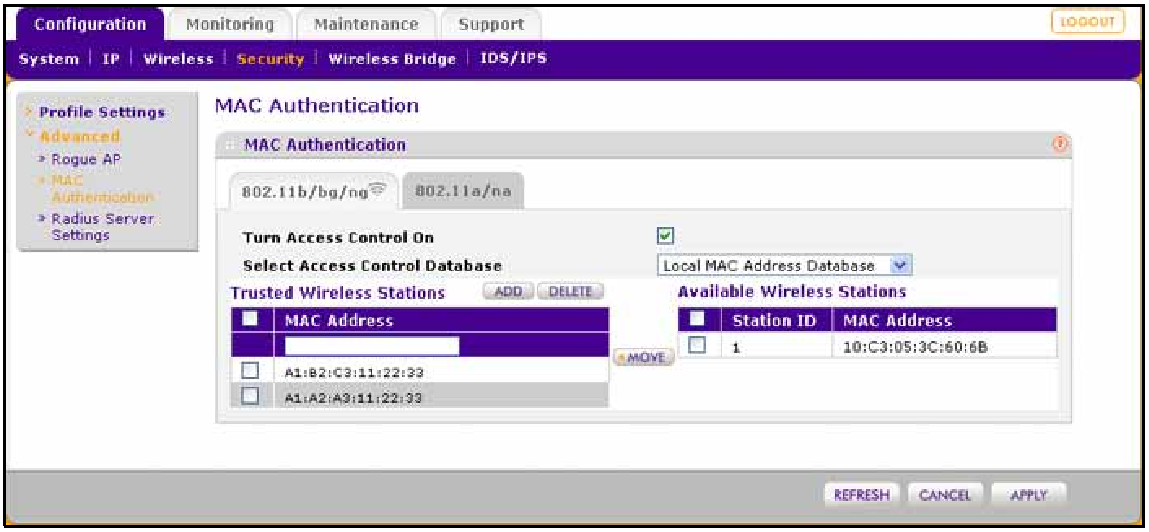
Restrict Wireless Access by MAC Address

For increased security, you can restrict access to an SSID by allowing access to only specific computers or wireless stations based on their MAC addresses. You can restrict access to only trusted computers so that unknown computers cannot connect wirelessly to the wireless access point. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

Note: For wireless adapters, you can usually find the MAC address printed on the wireless adapter.

➢ **To restrict access based on MAC addresses:**

1. Select **Configuration > Security > Advanced > MAC Authentication**. The MAC Authentication screen displays. (The following figure shows some examples.)



MAC Authentication

MAC Authentication

Turn Access Control On ☑

Select Access Control Database: Local MAC Address Database

Trusted Wireless Stations

□	MAC Address
□	A1:B2:C3:11:22:33
□	A1:A2:A3:11:22:33

Available Wireless Stations

□	Station ID	MAC Address
□	1	10:C3:05:3C:60:6B

Figure 31.

2. Optional: To display the MAC Authentication screen for the 802.11a/na modes, click the **802.11a/na** tab.
3. Select the **Turn Access Control On** check box to enable the access control feature.
4. From the Select Access Control Database drop-down list, select one of the following database options:
   - **Local MAC Address Database**. The wireless access point uses the local MAC address database for access control. This is the default setting.
   - **Remote MAC Address Database**. The wireless access point uses the MAC address database on an external RADIUS server on the LAN for access control. If you select this database, you first need to configure the RADIUS server settings (see *Configure RADIUS Server Settings* on page 57).

5. Click **Refresh** to refresh the Available Wireless Stations table. The wireless access point places the MAC addresses of the attached wireless stations in this table.
6. Populate the Trusted Wireless Stations table by one of the following methods:
   - Select MAC addresses from the Available Wireless Stations table:
     a. Select individual check boxes for MAC addresses, or select all MAC addresses by selecting the check box in the heading.
     b. Click **Move** to transfer the MAC addresses from the Available Wireless Stations table to the Trusted Wireless Stations table.
   - Enter MAC addresses manually:
     a. Enter a MAC address directly in the Trusted Wireless Stations table.
     b. Click **Add**.

   To delete a MAC address from the Trusted Wireless Stations table, select individual check boxes for MAC addresses, or select all MAC addresses by selecting the check box in the heading, and then click **Delete**.
7. Click **Apply** to save your settings.

   Now, only devices in the Trusted Wireless Stations table are allowed to connect to the wireless access point over a wireless connection.

WARNING:

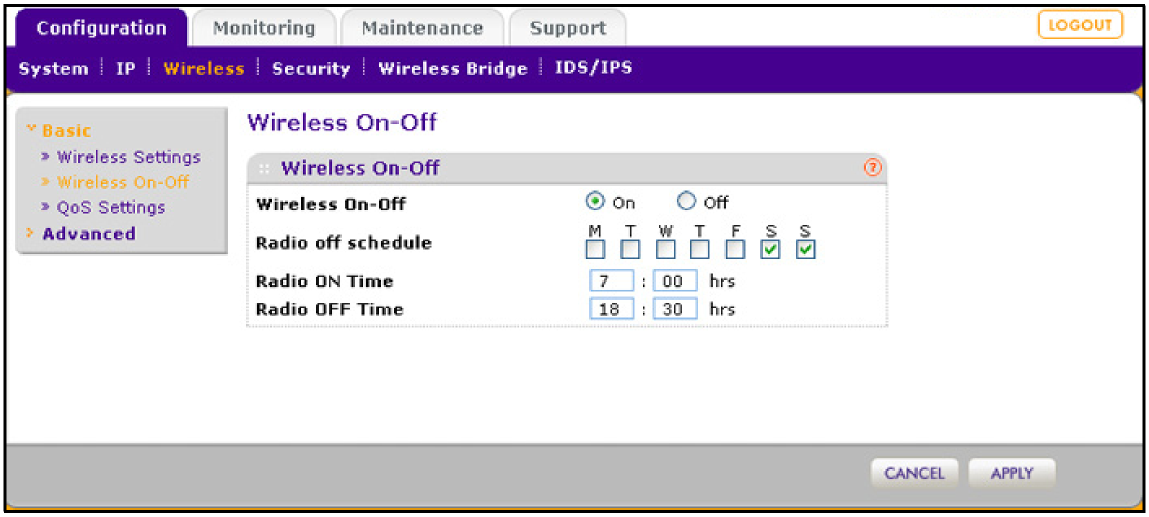
When configuring the wireless access point from a wireless computer whose MAC address is not on the access control list, you lose your wireless connection when you click Apply. You then need to access the wireless access point from a wired computer or from a wireless computer that is on the access control list to make any further changes.

Schedule the Wireless Radio to Be Turned Off

Scheduling the wireless radio to be turned off is a green feature that allows you to turn off the wireless radio during scheduled vacations, office shutdowns, on evenings, or on weekends.

➤ **To schedule the radio to be turned on and off:**

1. Select **Configuration > Wireless > Basic > Wireless On-Off**. The Wireless On-Off screen displays:



Wireless On-Off

Wireless On-Off	● On ○ Off
Radio off schedule	M □ T □ W □ T □ F □ S ☑ S ☑
Radio ON Time	7 : 00 hrs
Radio OFF Time	18 : 30 hrs

Figure 32.

2. Specify the settings as explained in the following table:

Table 15. Wireless radio on/off settings

Setting	Description
Wireless On-Off	Select the **On** radio button to enable the timer. By default, the Off radio button is selected.
Radio off schedule	Select check boxes to specify the days when you want to schedule the radio to be turned off. By default, Saturday and Sunday are selected.
Radio ON Time	Enter the time that you want the radio to be turned back on. Use 24-hour time format.
Radio OFF Time	Enter the time that you want the radio to be turned off. Use 24-hour time format.

3. Click **Apply** to save your settings.

Configure Basic Wireless Quality of Service

Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the type of data. Time-dependent information, such as video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients also need to support WMM.

By enabling WMM, you allow Quality of Service (QoS) control for upstream traffic flowing from a wireless station to the wireless access point and for downstream traffic flowing from the wireless access point to a wireless station.

WMM defines the following four queues in decreasing order of priority:

- **Voice**. The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media.

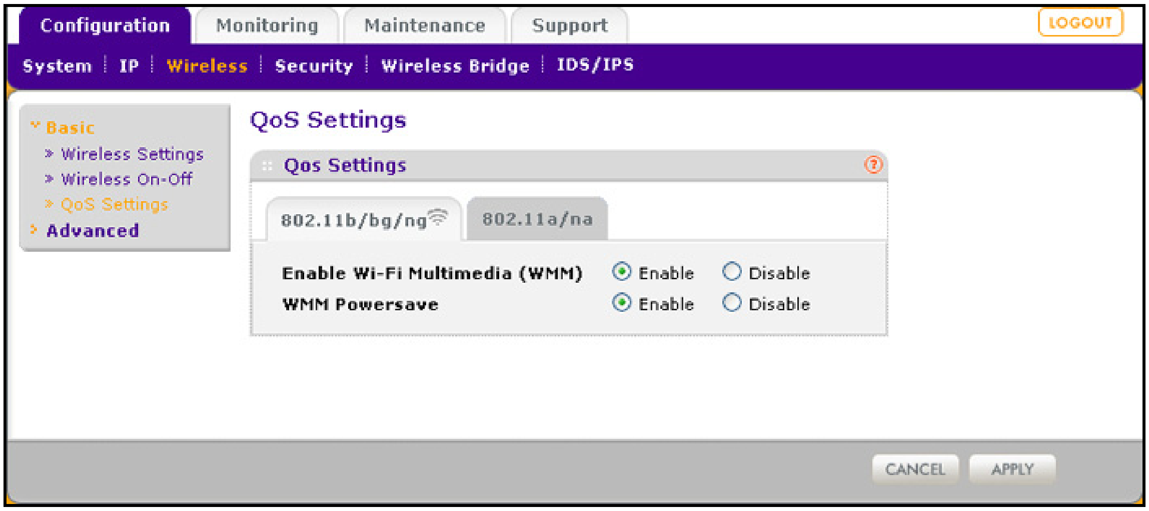
- **Video**. The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue.
- **Best Effort**. The medium priority queue with medium delay is given to this queue. Most standard IP applications use this queue.
- **Background**. Low priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue.

The WMM Powersave feature saves power for battery-powered equipment by increasing the efficiency and flexibility of data transmission.

Note: For information about how to configure advanced wireless QoS, that is, to configure specific Enhanced Distributed Channel Access (EDCA) settings, see *Configure Advanced Quality of Service Settings* on page 110.

➢ To configure basic wireless QoS:

1. Select **Configuration > Wireless > Basic > QoS Settings**. The basic QoS Settings screen displays:



Enable Wi-Fi Multimedia (WMM) ● Enable ○ Disable

WMM Powersave ● Enable ○ Disable

Figure 33.

2. Optional: To display the basic QoS Settings screen for the 802.11a/na modes, click the **802.11a/na** tab.
3. Enable or disable the WMM features:
   - **Enable Wi-Fi Multimedia (WMM)**. To enable this feature, select the **Enable** radio button, which is the default setting. Select the **Disable** radio button to disable the feature.
   - **WMM Powersave**. To enable this feature, select the **Enable** radio button, which is the default setting. Select the **Disable** radio button to disable the feature.
4. Click **Apply** to save your settings.

Management and Monitoring

4

This chapter describes how to use the management and monitoring features of the wireless access point. The chapter includes the following sections:

- *Enable Remote Management*
- *Upgrade the Wireless Access Point Software*
- *Manage the Configuration File or Reset to Factory Defaults*
- *Change the Administrator Password*
- *Manage User Accounts*
- *Enable the Syslog Server*
- *Monitor the Wireless Access Point*
- *Enable Rogue AP Detection and Monitor Access Points*
- *Configure Wireless Intrusion Detection and Prevention*

Enable Remote Management

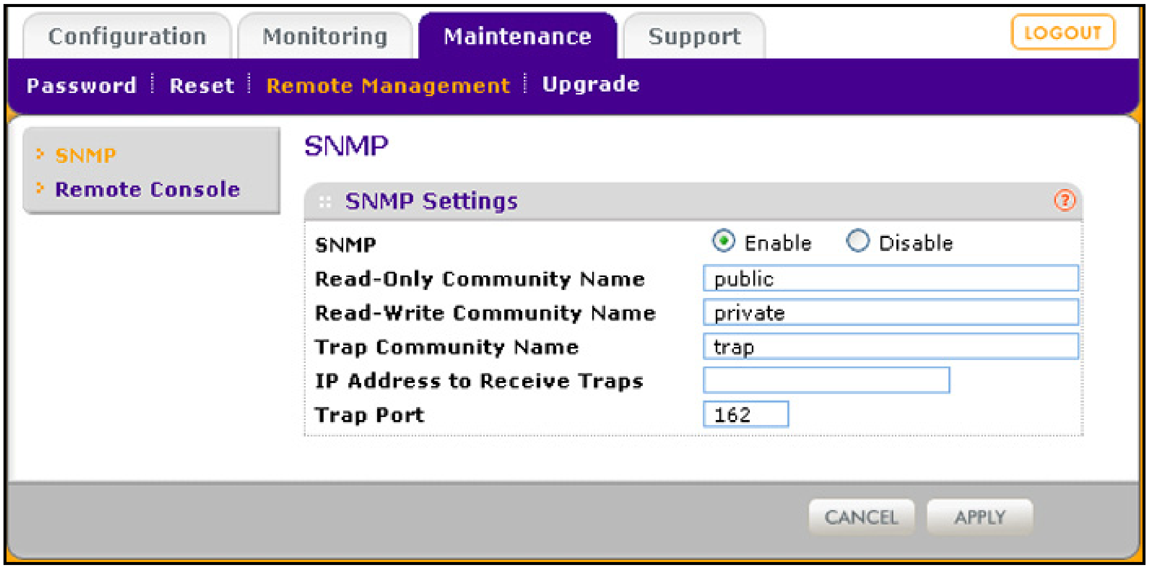
- *SNMP Management*
- *Secure Shell and Telnet Management*

Both Simple Network Management Protocol (SNMP) and the remote console Secure Shell (SSH) are enabled by default, which allows for remote management of the wireless access point from a client running SNMP management software, as well as from an SSH client. The Telnet console is disabled by default.

SNMP Management

➢ **To set up an SNMP management interface:**

1. Select **Maintenance > Remote Management > SNMP**. The SNMP screen displays:



SNMP

SNMP Settings

SNMP	● Enable ○ Disable
Read-Only Community Name	public
Read-Write Community Name	private
Trap Community Name	trap
IP Address to Receive Traps	
Trap Port	162

Figure 34.

2. Specify the settings as explained in the following table:

Table 16. SNMP settings

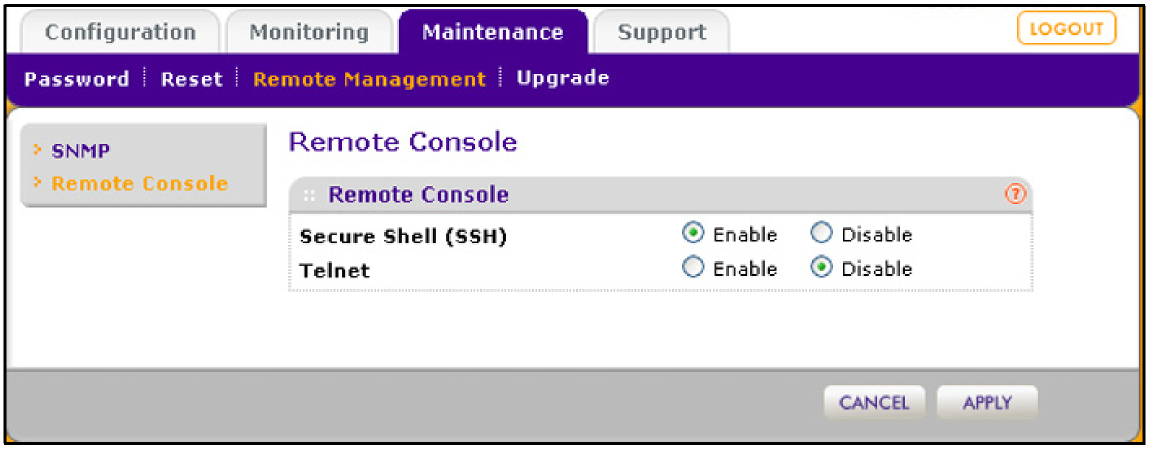
Setting	Description
SNMP	Select the **Enable** radio button to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point through SNMPv1/v2 protocol. By default, the Disable radio button is selected.
Read-Only Community Name	Enter the community string to allow the SNMP manager to read the wireless access point’s Management Information Base (MIB) objects. The default is public.
Read-Write Community Name	Enter the community string to allow the SNMP manager to read and write the wireless access point’s MIB objects. The default is private.
Trap Community Name	Enter the community string to allow the SNMP manager to send traps. The default is trap.
IP Address to Receive Traps	Enter the IP address of the SNMP manager to receive traps sent from the wireless access point.
Trap Port	Enter the number of the SNMP manager port to receive traps sent from the wireless access point. The default is 162.

3. Click **Apply** to save your settings.

Secure Shell and Telnet Management

➢ To configure remote console features:

1. Select **Maintenance > Remote Management > Remote Console**. The Remote Console screen displays:



Remote Console

Remote Console

Secure Shell (SSH) ● Enable ○ Disable

Telnet ○ Enable ● Disable

Figure 35.

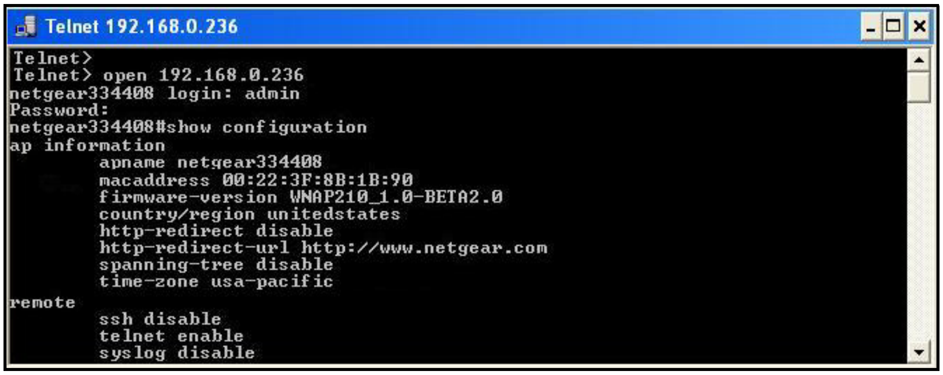
2. Enable or disable the remote console features:
   - **Secure Shell (SSH)**. To enable this feature, select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature.
   - **Telnet**. To enable this feature, select the **Enable** radio button. Select the **Disable** button to disable the feature, which is the default setting.
3. Click **Apply** to save your settings.

➢ To manage the wireless access point over a Telnet connection:

1. Connect an Ethernet cable to the console port of the wireless access point.
2. Connect the other end of the cable to a VT100/ANSI terminal or a workstation.

   If you attach a PC, Apple Macintosh, or UNIX workstation, start a secure terminal emulation program, and configure the terminal emulation program to use the following settings:

   - Baud rate: 9600 bps
   - Data bits: 8
   - Parity: none
   - Stop bit: 1
   - Flow control: none
3. Start a secure Telnet session from the terminal or workstation to the wireless access point. A screen similar to the following displays:



```
Telnet>
Telnet> open 192.168.0.236
netgear334408 login: admin
Password:
netgear334408#show configuration
ap information
        apname netgear334408
        macaddress 00:22:3F:8B:1B:90
        firmware-version WNAP210_1.0-BETA2.0
        country/region unitedstates
        http-redirect disable
        http-redirect-url http://www.netgear.com
        spanning-tree disable
        time-zone usa-pacific
remote
        ssh disable
        telnet enable
        syslog disable
```

Figure 36.

4. Enter the login name and password (**admin** and **password** are the defaults).

   After successful login, the **>** prompt appears, preceded by the name of the wireless access point. In this example, the prompt is netgear334408.

5. Enter the CLI commands that you want to use. You can enter **`show configuration`** to display the available CLI commands. The CLI commands are also listed in *Appendix B, Command-Line Reference*.

Note: You can also access the wireless access point remotely over a Telnet or SSH session using an application such as PuTTY, if such an encryption application is allowed by law in your country. After you have connected to the wireless access point, enter the login name and password to access the CLI.

Upgrade the Wireless Access Point Software

The software of the wireless access point is stored in flash memory and can be upgraded as NETGEAR releases new software. You can download upgrade files from the NETGEAR website. If the upgrade file is compressed (.zip file), you first need to extract the image (.rmt) file before sending it to the wireless access point. You can send the upgrade file using your browser. There are two methods to perform a software upgrade that are described in the following sections:

- *Web Browser Upgrade Procedure*
- *TFTP Server Upgrade Procedure*

Note: The web browser that you use to upload new firmware into the wireless access point needs to support HTTP uploads. Use a browser such as Microsoft Internet Explorer 6.0 or later or Mozilla 1.5 or later.

Note: You cannot perform the software upgrade from a computer that is connected to the wireless access point over a wireless link. You need to use a computer that is connected to the wireless access point over an Ethernet cable.

WARNING:

When uploading software to the wireless access point, do *not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, the upload might fail, corrupt the software, and render the wireless access point inoperable.

IMPORTANT:

In some cases, such as a major upgrade, you might need to erase the configuration and manually reconfigure your wireless access point after upgrading it. See the release notes included with the software to find out if you need to reconfigure the wireless access point.

Web Browser Upgrade Procedure

➢ **To use a web browser to upgrade the wireless access point firmware:**

1. Download the new software file from the NETGEAR website and save it to your hard disk.
2. If necessary, unzip the new software file.
3. If available, read the release notes before upgrading the software.
4. Select **Maintenance > Upgrade > Firmware Upgrade**. The Firmware Upgrade screen displays:

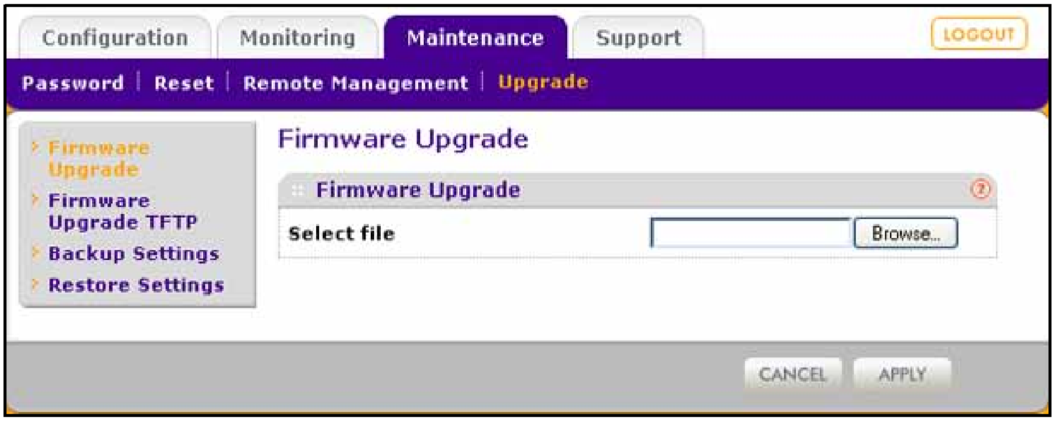


Figure 37.

5. Click **Browse** and locate the image (.zip) upgrade file.
6. Click **Apply** to initiate the upgrade process.

   During the upgrade process, the wireless access point automatically restarts. The upgrade process typically takes several minutes. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.

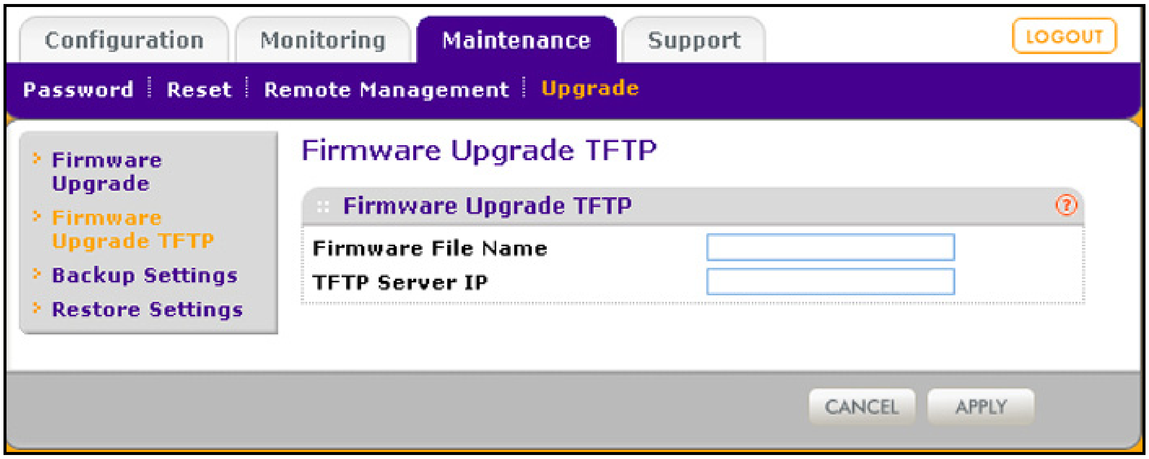
7. Verify that the new software file has been installed by selecting **Monitoring > System**. The System screen displays (see *Figure 46* on page 78). The firmware version is shown in the Access Point Information section of the screen.

TFTP Server Upgrade Procedure

To use this method, you need to have a TFTP server set up.

➢ **To use a TFTP server to upgrade the wireless access point firmware:**

1. Download the new software file from the NETGEAR website and save it to your hard disk.
2. Place the software file in your TFTP server location. (You do not need to unzip the file.)
3. If available, read the release notes before upgrading the software.
4. Select **Maintenance > Upgrade > Firmware Upgrade TFTP**. The Firmware Upgrade TFTP screen displays:



Firmware Upgrade TFTP

Firmware Upgrade TFTP

Firmware File Name	
TFTP Server IP	

Figure 38.

5. Specify the following information:
   - **Firmware File Name**. The name of the unzipped software file.
   - **TFTP Server IP**. The IP address of your TFTP server.
6. Click **Apply** to initiate the upgrade process.

   During the upgrade process, the wireless access point automatically restarts. The upgrade process typically takes several minutes. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.

7. Verify that the new software file has been installed by selecting **Monitoring > System**. The System screen displays (see *Figure 46* on page 78). The firmware version is shown in the Access Point Information section of the screen.

Manage the Configuration File or Reset to Factory Defaults

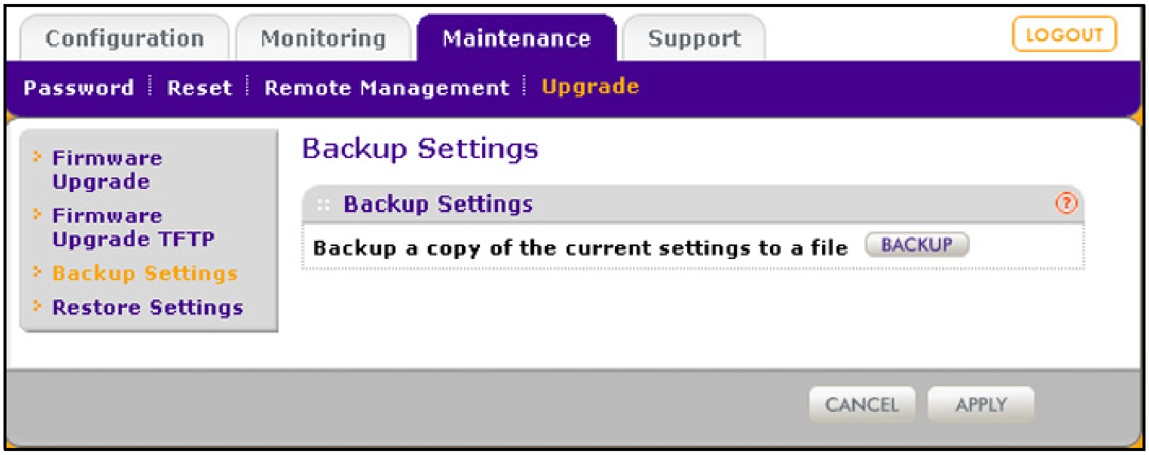
- *Save the Configuration*
- *Restore the Configuration*
- *Restore the Wireless Access Point to the Factory Default Settings*
- *Reboot the Wireless Access Point without Restoring the Default Configuration*

The wireless access point settings are stored in the configuration file. You can save this file (back it up) to a computer, restore it from a computer, or reset it to factory default settings.

Save the Configuration

➢ **To save your settings:**

1. Select **Maintenance > Upgrade > Backup Settings**. The Backup Settings screen displays (see the following figure).
2. Click **Backup**. Your browser extracts the configuration file (the file name is config) from the wireless access point and prompts you for a location on your computer to store the file.
3. Follow the instructions of your browser to save the file.



Backup a copy of the current settings to a file

Figure 39.

Restore the Configuration

IMPORTANT:

During the restoration process, do not try to go online, turn off the wireless access point, shut down the computer, or do anything else to the wireless access point until it finishes restarting!

➢ **To restore your settings from a saved configuration file:**

1. Select **Maintenance > Upgrade > Restore Settings**. The Restore Settings screen displays:

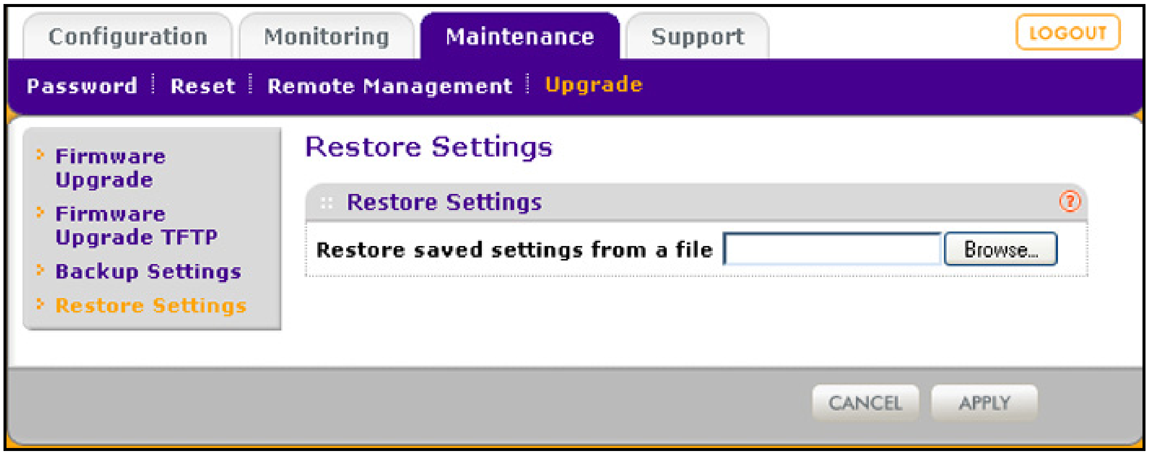


Figure 40.

2. Click **Browse** and locate the backup configuration file (the file name is config).
3. Click **Apply** to initiate the restoration process. During the restoration process, the wireless access point automatically restarts. The restoration process typically takes about 1 minute. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.

Restore the Wireless Access Point to the Factory Default Settings

You can restore the wireless access point to the factory default settings by two methods that are described in the following sections:

- *Use the Web Management Interface to Restore Factory Default Settings*
- *Use the Reset Button to Restore Factory Default Settings*

Note: After you have restored the factory default settings on the wireless access point:
* All custom configurations are lost.
* The login password is **password.**
* The default LAN IP address is **192.168.0.100**.
* The DHCP client is disabled.
* The Access Point Name field is reset to the name printed on the label on the bottom of the unit.

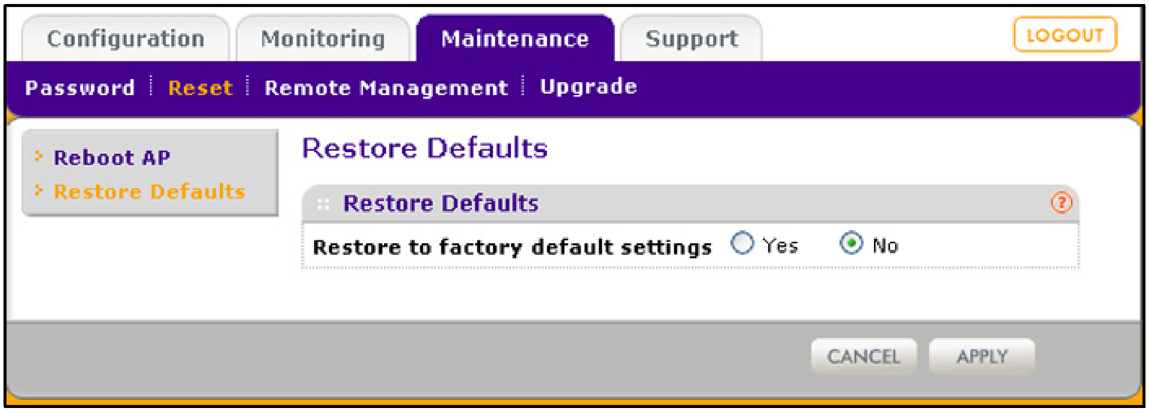
Use the Web Management Interface to Restore Factory Default Settings

IMPORTANT:

During the restoration process, do not try to go online, turn off the wireless access point, shut down the computer, or do anything else to the wireless access point until it finishes restarting!

➢ **To restore the factory default settings using the web management interface:**

1. Select **Maintenance > Reset > Restore Defaults**. The Restore Defaults screen displays:



Restore to factory default settings ○ Yes ● No

Figure 41.

2. Select the **Yes** radio button. (By default, the No radio button is selected.)
3. Click **Apply** to reset the wireless access point to the factory default settings.

   During the restoration process, the wireless access point automatically restarts. The restoration process typically takes about 1 minute. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.

Use the Reset Button to Restore Factory Default Settings

To restore the factory default settings when you do not know the login user name, login password, or IP address, you need to use the Reset button on the rear panel of the wireless access point (see *Figure 2* on page 13).

➤ **To restore the factory default settings using the Reset button:**

1. Using a sharp object, press and hold the **Reset** button for about 5 seconds (until the Test LED blinks rapidly) to reset the wireless access point to factory defaults settings.

> **Note:** Pressing the Reset button for a shorter time simply causes the wireless access point to reboot.

2. Release the **Reset** button.

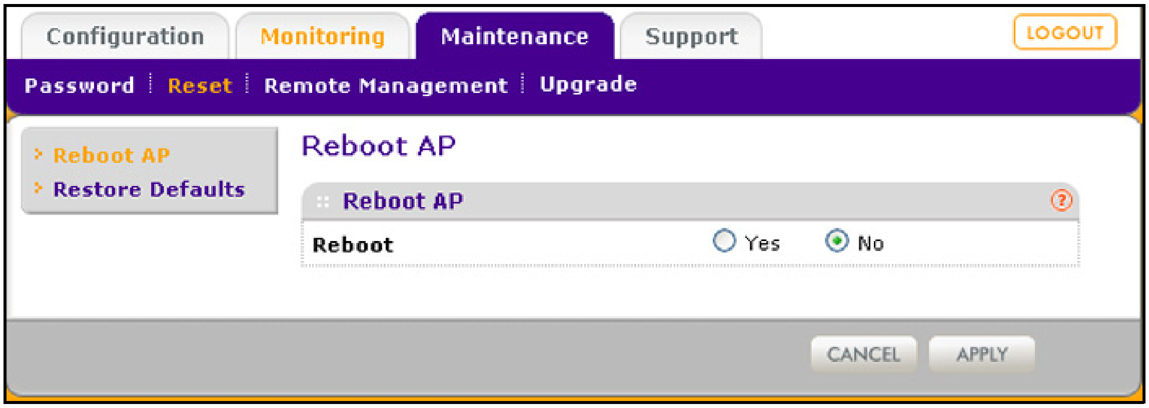
   During the restoration process, the wireless access point automatically restarts. The restoration process typically takes about 1 minute. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.

Reboot the Wireless Access Point without Restoring the Default Configuration

If you do not have physical access to the wireless access point to switch it off and on again, you can use the software to reboot the wireless access point.

➤ **To reboot the wireless access point:**

1. Select **Maintenance > Reset > Reboot AP**. The Reboot AP screen displays:



Reboot AP

Reboot AP

Reboot ○ Yes ● No

Figure 42.

2. Select the **Yes** radio button. (By default, the No radio button is selected.)
3. Click **Apply** to reboot the wireless access point.

The reboot process typically takes about 1 minute. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.

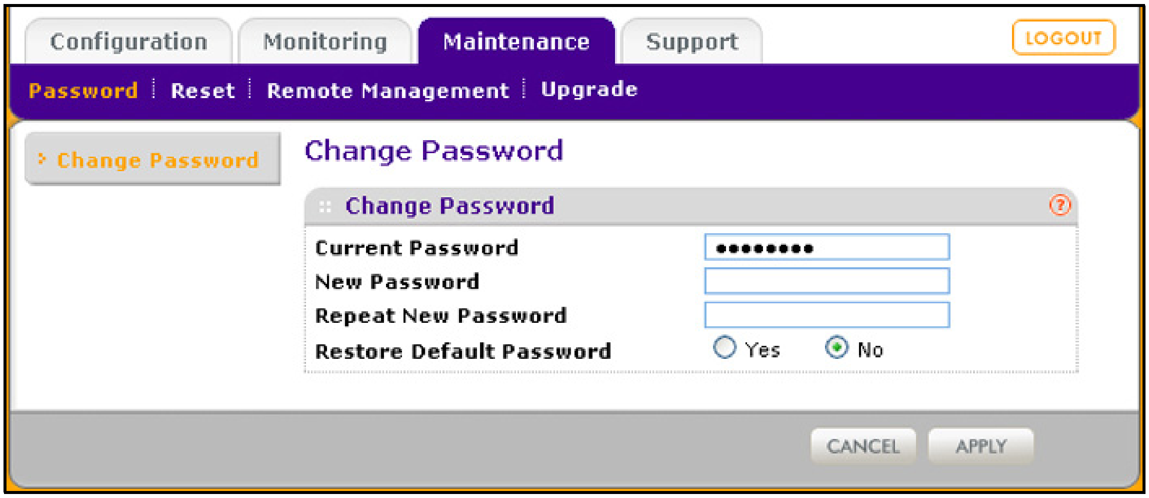
Change the Administrator Password

The default password is **password**. NETGEAR recommends that you change this password to a more secure password. You cannot change the administrator login name (admin).

The ideal password contains no dictionary words from any language and is a mixture of letters (both uppercase and lowercase), numbers, and symbols. Your password can be up to 30 characters.

➢ **To change the administrator password:**

1. Select **Maintenance > Password > Change Password**. The Change Password screen displays:



Change Password

Change Password

Current Password	•••••••••
New Password	
Repeat New Password	
Restore Default Password	○ Yes ● No

Figure 43.

2. Take one of the following actions:
   - Enter a new password twice, once in the New Password field and again in the Repeat New Password field.
   - Next to Restore Default Password, select the **Yes** radio button to restore the default password. By default, the No radio button is selected.
3. Click **Apply** to save your settings.

   If you have restored the default password, the login password is **password**. If you have configured a new password, write it down in a secure place.

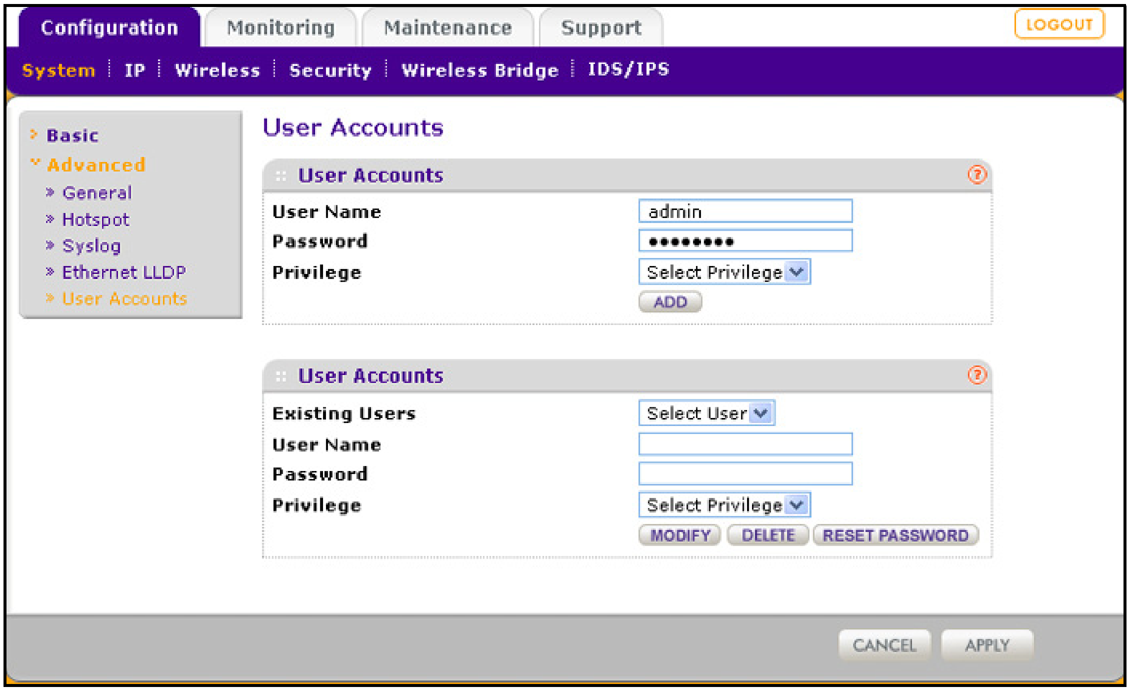
Manage User Accounts

The admin user account is the default user account, which you cannot delete. However, you can add other user accounts, modify them, and delete them. Users for whom you set up an account can access the web management interface with read-only or read-write privileges.

Note: Only the administrator can create, change, and delete user accounts.

➢ To add a new user account:

1. Select **Configuration > System > Advanced > User Accounts**. The User Accounts screen displays:



User Accounts

User Accounts

User Name	admin
Password	••••••••
Privilege	Select Privilege

User Accounts

Existing Users	Select User
User Name	
Password	
Privilege	Select Privilege

Figure 44.

2. Configure the settings in the upper part of the screen as explained in the following table:

Table 17. Add user account settings

Setting	Description
User Name	Enter a new user name
Password	Enter a password between 4 and 12 characters in length.
Privilege	From the Privilege drop-down list, select **Read Write** or **Read Only**.

3. Click **Add**.
4. Click **Apply** to save your settings.

➢ **To change the name for a user account:**

1. On the User Accounts screen, in the lower part of the screen, select the user from the Existing Users drop-down list.
2. In the User Name field, modify the name.
3. Click **Modify**.
4. Click **Apply** to save your settings.

➢ **To change the privilege for a user account:**

1. On the User Accounts screen, in the lower part of the screen, select the user from the Existing Users drop-down list.
2. From the Privilege drop-down list, select another privilege.
3. Click **Reset Password**. The password is reset to the default password, which is password.
4. Click **Apply** to save your settings.

➢ **To reset the password for a user account:**

1. On the User Accounts screen, in the lower part of the screen, select the user from the Existing Users drop-down list.
2. Click **Reset Password**. The password is reset to the default password, which is password.
3. Click **Apply** to save your settings.

Note: If you want to modify a password, delete the user account, and then recreate the user account with the password of your choice.

➢ **To delete a user account:**

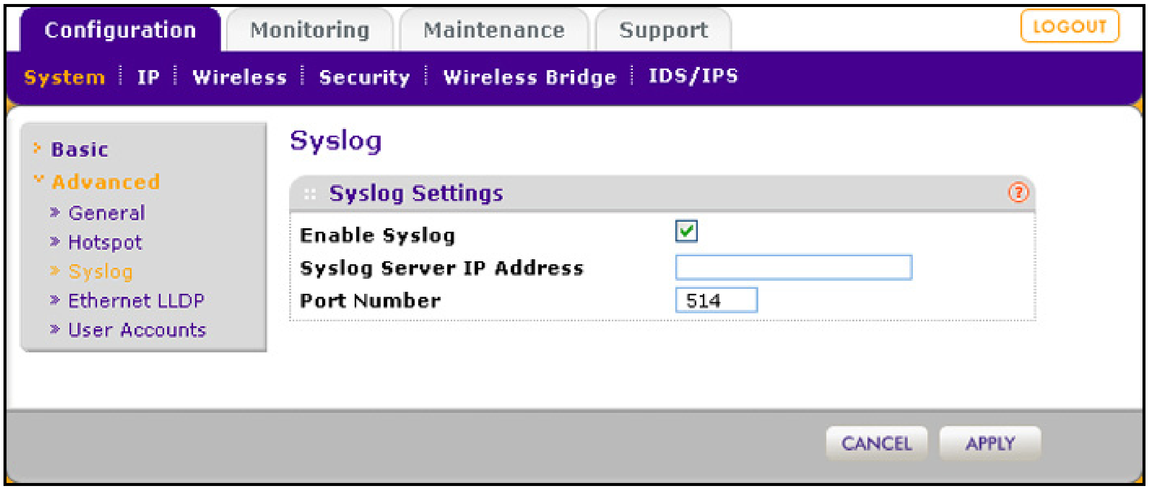
1. On the User Accounts screen, in the lower part of the screen, select the user from the Existing Users drop-down list.
2. Click **Delete**.
3. Click **Apply** to save your settings.

Enable the Syslog Server

The Syslog screen allows you to enable the syslog option if you have a syslog server on your LAN. If syslog is enabled, the wireless access point sends its syslog files to the syslog server.

➢ **To enable a syslog server:**

1. Select **Configuration > System > Advanced > Syslog**. The Syslog screen displays:



Syslog

Syslog Settings

Enable Syslog ☑

Syslog Server IP Address

Port Number 514

Figure 45.

Specify the settings as explained in the following table:

Table 18. Syslog settings

Setting	Description
Enable Syslog	Select the check box to enable the syslog option. By default, the syslog option is disabled.
Syslog Server IP Address	Enter the IP address of the syslog server to which the wireless access point sends the syslog files.
Port Number	Enter the port number that is configured on the syslog server. The default port number is 514.

2. Click **Apply** to save your settings.

Monitor the Wireless Access Point

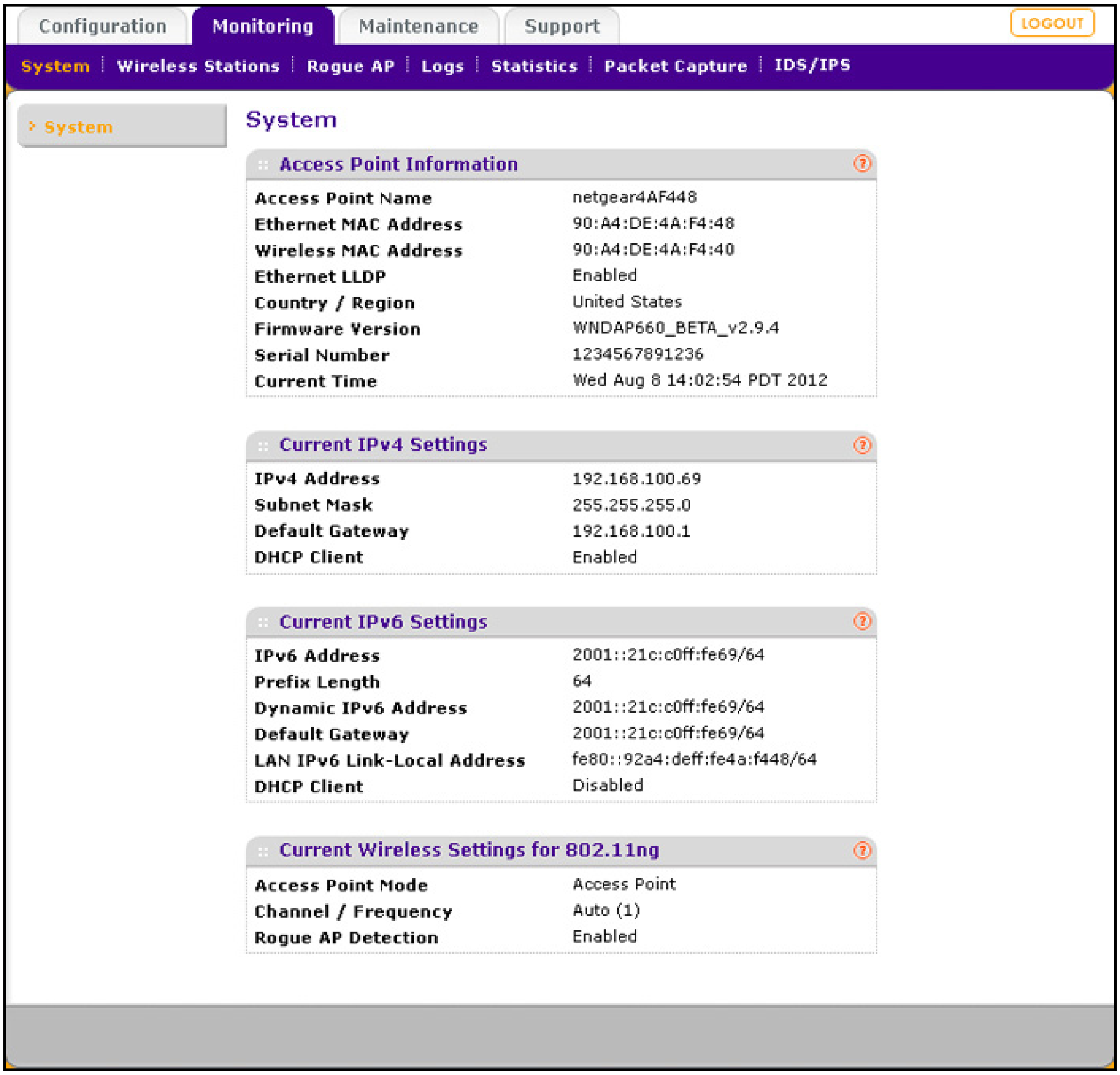
- *View System Information*
- *Monitor Wireless Stations*
- *View the Activity Log*
- *Traffic Statistics*

View System Information

The System screen provides a summary of the current wireless access point configuration settings, including current IP settings and current wireless settings. This information is read only, so any changes need to be made on other screens.

➢ To view the System screen:

Select **Monitoring > System**.



System

Access Point Information

Access Point Name	netgear4AF448
Ethernet MAC Address	90:A4:DE:4A:F4:48
Wireless MAC Address	90:A4:DE:4A:F4:40
Ethernet LLDP	Enabled
Country / Region	United States
Firmware Version	WNDAP660_BETA_v2.9.4
Serial Number	1234567891236
Current Time	Wed Aug 8 14:02:54 PDT 2012

Current IPv4 Settings

IPv4 Address	192.168.100.69
Subnet Mask	255.255.255.0
Default Gateway	192.168.100.1
DHCP Client	Enabled

Current IPv6 Settings

IPv6 Address	2001::21c:c0ff:fe69/64
Prefix Length	64
Dynamic IPv6 Address	2001::21c:c0ff:fe69/64
Default Gateway	2001::21c:c0ff:fe69/64
LAN IPv6 Link-Local Address	fe80::92a4:deff:fe4a:f448/64
DHCP Client	Disabled

Current Wireless Settings for 802.11ng

Access Point Mode	Access Point
Channel / Frequency	Auto (1)
Rogue AP Detection	Enabled

Figure 46.

The following table explains the fields of the System screen:

Table 19. System screen fields

Setting	Description
Access Point Information	
Access Point Name	The NetBIOS name. For information about how to change the default name, see *Configure Basic General System Settings and Time Settings* on page 23.
Ethernet MAC Address	The MAC address of the wireless access point's Ethernet port.
Wireless MAC Address	The MAC address of the wireless access point's wireless card.
Ethernet LLDP	Enabled indicates that LLDP is enabled. Disabled indicates that it is not.
Country/Region	The country or region for which the wireless access point is licensed for use. For information about how to change the country or region, see *Configure Basic General System Settings and Time Settings* on page 23. **Note:** It might not be legal to operate this wireless access point in a country or region other than one of those identified in this field.
Firmware Version	The version of the firmware that is currently installed.
Serial Number	The serial number of the wireless access point.
Current Time	The current time. For information about how to change the time settings, see *Configure Basic General System Settings and Time Settings* on page 23.
Current IPv4 Settings For information about how to change any of these IP settings, see *Configure the IPv4 Settings* on page 25.	
IP Address	The IPv4 address of the wireless access point.
Subnet Mask	The subnet mask for the address of the wireless access point.
Default Gateway	The default IPv4 gateway for the wireless access point communication.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCPv4 server on your LAN network. Disabled indicates a static IP configuration.
Current IPv6 Settings For information about how to change any of these IP settings, see *Configure IPv6 Settings and Optional DHCPv6 Server Settings* on page 99.	
IPv6 Address	The default IPv6 address of the wireless access point.
Prefix Length	The prefix length for the address of the wireless access point.
Dynamic IPv6 Address	The dynamically assigned IPbv6 address if the DHCPv6 server has the stateful option enabled.
Default Gateway	The default IPv6 gateway for the wireless access point communication.
LAN IPv6 Link-Local Address	This is an automatically generated IPv6 address that uses the IPv4 address in the interface portion of its address.

Table 19. System screen fields (continued)

Setting	Description
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCPv6 server on your LAN network. Disabled indicates a static IP configuration.
Current Wireless Settings for 802.11b, **802.11g**, or **802.11ng** or **Current Wireless Settings for 802.11a** or **802.11na** **Note:** The section heading depends on the configured wireless mode.	
Access Point Mode	The operating mode of the wireless access point. One of the following modes is indicated: • Access Point • Point-to-Point Bridge • Point-to-Point Bridge with Access Point • Multi-Point Bridge with/without client association For information about how to change the mode, see *Configure Wireless Bridging* on page 118.
Channel / Frequency	The channel that the wireless port is using. For information about how to change the channel and frequency, see *Configure 802.11b/bg/ng Wireless Settings* on page 28 and *Configure 802.11a/na Wireless Settings* on page 31.
Rogue AP Detection	Enabled indicates that rogue AP detection is enabled. Disabled indicates that it is not.

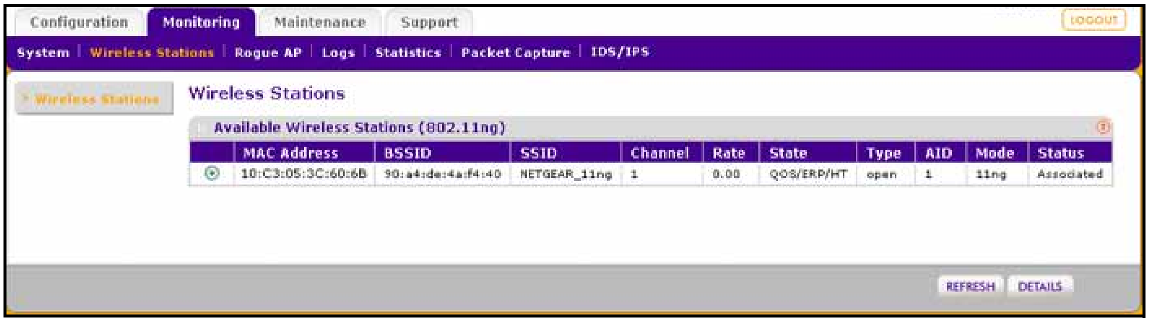
Monitor Wireless Stations

The Wireless Stations screen contains the Available Wireless Stations table. This table shows all IP devices that are associated with the wireless access point in the wireless network that is defined by the wireless network name (SSID). The table heading indicates the wireless mode (802.11b, 802.11bg, or 802.11ng for the 2.4-GHz band, or 802.11a or 802.11na for the 5-GHz band).

Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This uniformity extends the reach of the wireless network and allows users to roam from one wireless access point to another, providing seamless network connectivity. Under these circumstances, be aware that the Available Wireless Stations table includes only the stations associated with this wireless access point.

➢ **To view the attached wireless stations, and to view details for a wireless station:**

1. Select **Monitoring > Wireless Stations**. The Wireless Stations screen displays:


Configuration
Monitoring
Maintenance
Support
LOGOUT
System | Wireless Stations | Rogue AP | Logs | Statistics | Packet Capture | IDS/IPS
› Wireless Stations
REFRESH
DETAILS

Wireless Stations

Available Wireless Stations (802.11ng)

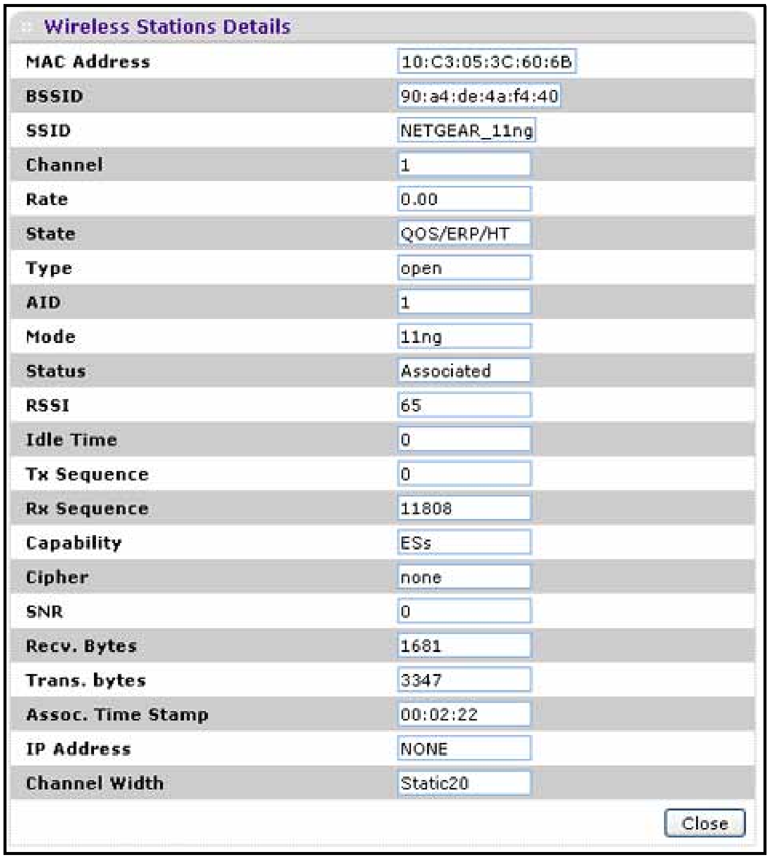
	MAC Address	BSSID	SSID	Channel	Rate	State	Type	AID	Mode	Status
●	10:C3:05:3C:60:6B	90:a4:de:4a:f4:40	NETGEAR_11ng	1	0.00	QOS/ERP/HT	open	1	11ng	Associated

Figure 47.

To update the list, click **Refresh**. If the wireless access point is rebooted, the wireless station data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click **Refresh**.

The Available Wireless Stations table shows the MAC address, BSSID, SSID, channel, rate, state, type, AID, mode, and status for each device. For information about these and more fields, see the table that follows the next figure.

2. To view details of a wireless station, select the corresponding radio button, and then click **Details**. The Wireless Stations Details screen displays:



Wireless Stations Details

MAC Address	10:C3:05:3C:60:6B
BSSID	90:a4:de:4a:f4:40
SSID	NETGEAR_11ng
Channel	1
Rate	0.00
State	QOS/ERP/HT
Type	open
AID	1
Mode	11ng
Status	Associated
RSSI	65
Idle Time	0
Tx Sequence	0
Rx Sequence	11808
Capability	ESs
Cipher	none
SNR	0
Recv. Bytes	1681
Trans. bytes	3347
Assoc. Time Stamp	00:02:22
IP Address	NONE
Channel Width	Static20

Figure 48.

The following table explains the fields of the Wireless Stations Details screen:

Table 20. Wireless stations details fields

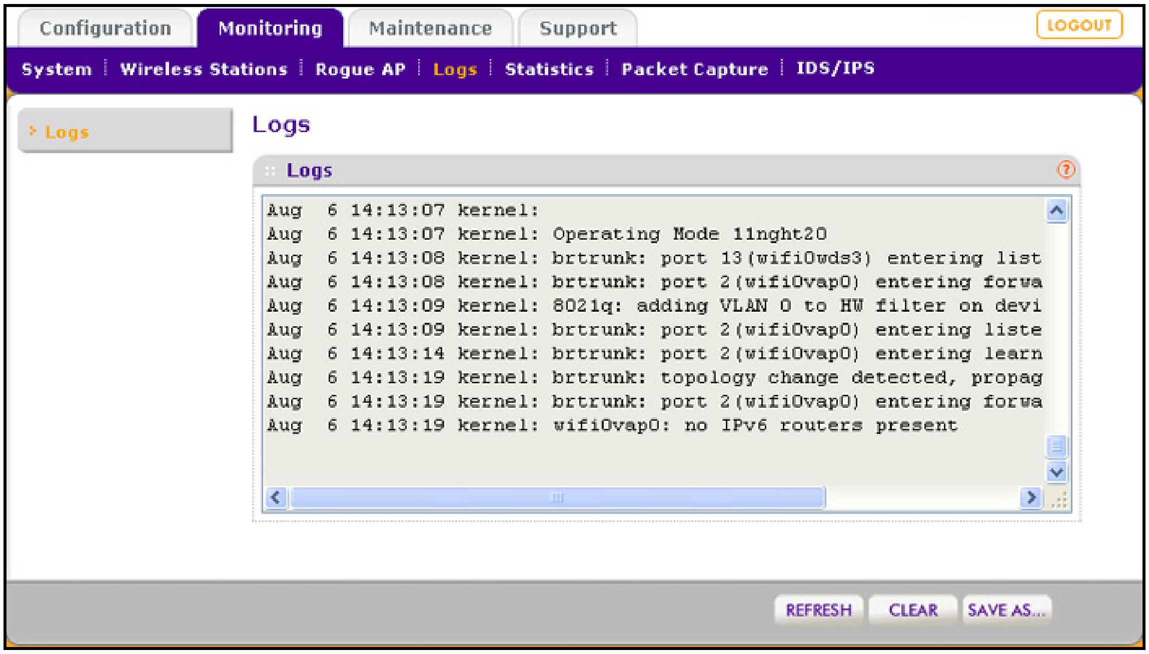
Setting	Description
MAC Address	The MAC address of the wireless station.
BSSID	The BSSID that the wireless station is using.
SSID	The SSID that the wireless station is using.
Channel	The channel that the wireless station is using.
Rate	The transmit data rate in Mbps of the wireless station.
State	The features that are enabled on the wireless station.
Type	The authentication and encryption type that the wireless station is using.
AID	The associated identifier (AID) of the wireless station.
Mode	The wireless mode in which the wireless station is operating.
Status	The wireless status of the wireless station (Associated).
RSSI	The received signal strength indicator (RSSI) of the wireless station.
Idle Time	The time since the last frame was received from the wireless station.
Tx Sequence	The sequence number of the last frame that was transmitted to the wireless station.
Rx Sequence	The sequence number of the last frame that was received from the wireless station.
Capability	The summary of the capability of the wireless station that was detected during association.
Cipher	The cipher that the wireless station is using and that defines the type of encryption.
SNR	The signal-to-noise ratio (SNR) that indicates how much the signal of the wireless station has been corrupted by noise.
Recv. Bytes	The number of bytes received on the wireless station since it last started up.
Trans. bytes	The number of bytes transmitted by the wireless station since it last started up.
Assoc. Time Stamp	The time when these details of the wireless station were retrieved.
IP Address	The IP address of the wireless station.
Channel Width	The channel width at which the wireless station operates.

View the Activity Log

You can view the wireless access point's activity logs onscreen and save the logs.

➢ To display the activity log and save it:

1. Select **Monitoring > Logs**. The Logs screen displays:



```
Aug  6 14:13:07 kernel:
Aug  6 14:13:07 kernel: Operating Mode 11nght20
Aug  6 14:13:08 kernel: brtrunk: port 13(wifi0wds3) entering list
Aug  6 14:13:08 kernel: brtrunk: port 2(wifi0vap0) entering forwa
Aug  6 14:13:09 kernel: 8021q: adding VLAN 0 to HW filter on devi
Aug  6 14:13:09 kernel: brtrunk: port 2(wifi0vap0) entering liste
Aug  6 14:13:14 kernel: brtrunk: port 2(wifi0vap0) entering learn
Aug  6 14:13:19 kernel: brtrunk: topology change detected, propag
Aug  6 14:13:19 kernel: brtrunk: port 2(wifi0vap0) entering forwa
Aug  6 14:13:19 kernel: wifi0vap0: no IPv6 routers present
```

Figure 49.

2. Click **Save As** to save the log contents to a file on your computer or to a disk drive.

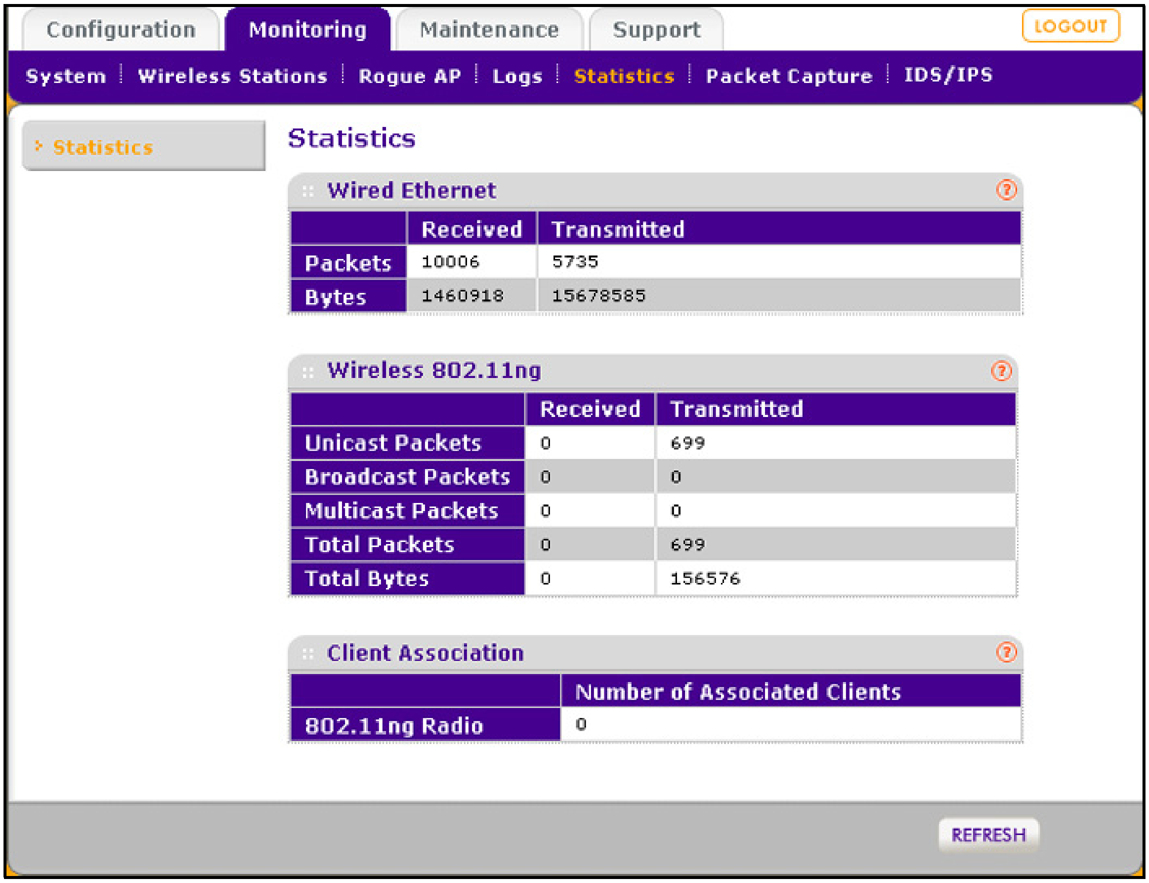
   To update the display onscreen, click **Refresh**; to clear the log content, click **Clear**.

Traffic Statistics

The Statistics screen displays information for both wired (LAN) and wireless (WLAN) network traffic.

➢ To display the Statistics screen:

Select **Monitoring > Statistics**.



Statistics

Wired Ethernet

	Received	Transmitted
Packets	10006	5735
Bytes	1460918	15678585

Wireless 802.11ng

	Received	Transmitted
Unicast Packets	0	699
Broadcast Packets	0	0
Multicast Packets	0	0
Total Packets	0	699
Total Bytes	0	156576

Client Association

	Number of Associated Clients
802.11ng Radio	0

Figure 50.

To update the statistics information, click **Refresh**.

The following table explains the fields of the Statistics screen:

Table 21. Statistics fields

Setting	Description
Wired Ethernet	
Packets	The number of packets received and transmitted over the Ethernet connection since the wireless access point was restarted.
Bytes	The number of bytes received and transmitted over the Ethernet connection since the wireless access point was restarted.
Wireless 802.11b, **Wireless 802.11bg**, **Wireless 801.11ng**, **Wireless 802.11a**, or **Wireless 802.11na** **Note:** The section heading depends on the configured wireless mode.	
Unicast Packets	The number of unicast packets received and transmitted over the wireless connection since the wireless access point was restarted.

Table 21. Statistics fields (continued)

Setting	Description
Broadcast Packets	The number of broadcast packets received and transmitted over the wireless connection since the wireless access point was restarted.
Multicast Packets	The number of multicast packets received and transmitted over the wireless connection since the wireless access point was restarted.
Total Packets	The total number of packets received and transmitted over the wireless connection since the wireless access point was restarted.
Total Bytes	The total number of bytes received and transmitted over the wireless connection since the wireless access point was restarted.
Client Association	
802.11b Radio, 802.11bg Radio, or 802.11ng Radio 802.11na Radio or 802.11a Radio	The number of associated clients connected to the radio in the configured wireless modes.

Enable Rogue AP Detection and Monitor Access Points

- *Enable and Configure Rogue AP Detection*
- *View and Save Access Point Lists*

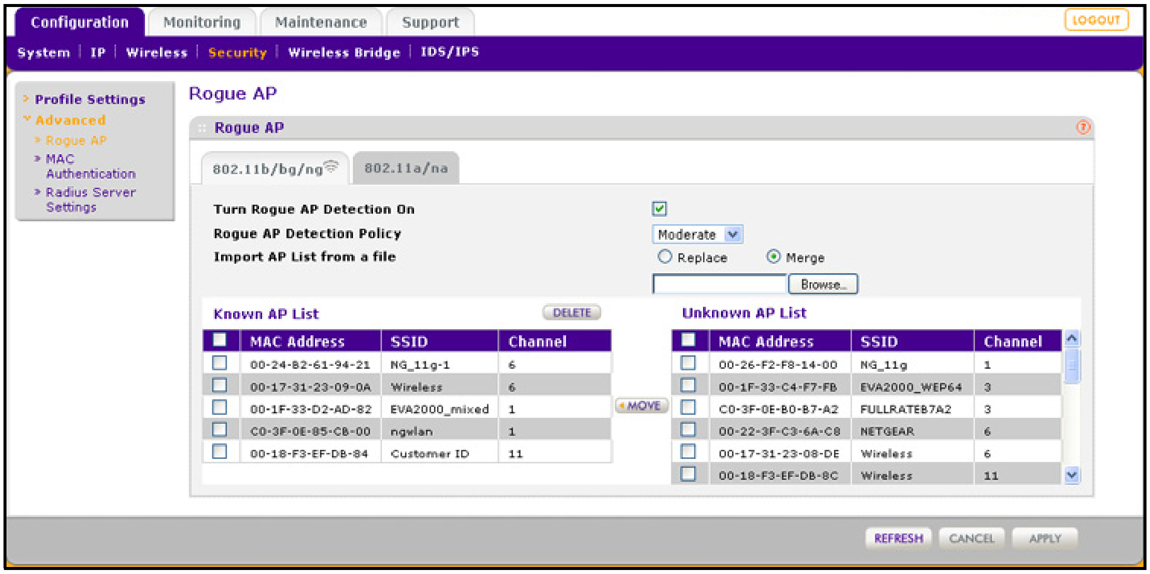
Enable and Configure Rogue AP Detection

The wireless access point can detect rogue access points and prevent them from connecting to the wireless access point. The wireless access point maintains a list of access points it detects in the area. Initially all detected access points are displayed in the Unknown AP List. You restrict communication to approved access points by adding them to the Known AP List and enabling the rogue AP detection feature.

If you enable rogue AP detection, the wireless access point continuously scans the wireless network and collects information about all access points on its channel.

➤ **To enable and configure rogue AP detection:**

1. Select **Configuration > Security > Advanced > Rogue AP**. The Rogue AP screen displays. (The following figure shows examples in the Known AP List and Unknown AP List.)



Rogue AP

Rogue AP

Turn Rogue AP Detection On ☑

Rogue AP Detection Policy: Moderate

Import AP List from a file: ○ Replace ● Merge

Known AP List

□	MAC Address	SSID	Channel
□	00-24-B2-61-94-21	NG_11g-1	6
□	00-17-31-23-09-0A	Wireless	6
□	00-1F-33-D2-AD-82	EVA2000_mixed	1
□	C0-3F-0E-85-CB-00	ngwlan	1
□	00-18-F3-EF-DB-84	Customer ID	11

Unknown AP List

□	MAC Address	SSID	Channel
□	00-26-F2-F8-14-00	NG_11g	1
□	00-1F-33-C4-F7-FB	EVA2000_WEP64	3
□	C0-3F-0E-B0-B7-A2	FULLRATEB7A2	3
□	00-22-3F-C3-6A-C8	NETGEAR	6
□	00-17-31-23-08-DE	Wireless	6
□	00-18-F3-EF-DB-8C	Wireless	11

Figure 51.

2. Optional: To enable and configure rogue AP detection for the 802.11a/na modes, click the **802.11a/na** tab.
3. Select the **Turn Rogue AP Detection On** check box to enable rogue AP detection.
4. Specify the detection policy by making a selection from the Rogue AP Detection Policy drop-down list:
   - **Mild**. The wireless access point scans for rogue access points every 10 seconds.
   - **Moderate**. The wireless access point scans for rogue access points every 5 seconds. This is the default setting.
   - **Aggressive**. The wireless access point scans for rogue access points every second.
5. Click **Refresh** to let the wireless access point discover the access points and populate the Unknown AP List.
6. In the Unknown AP List, select individual check boxes for access points, or select all access points by selecting the check box in the column heading.
7. Click **Move** to transfer the access points from the Unknown AP List to the Known AP List.
8. Click **Apply** to save your settings.

➢ To remove APs from the Known AP List and return them to the Unknown AP List:

1. In the Known AP List, select individual check boxes for access points, or select all access points by selecting the check box in the column heading.
2. Click **Delete**.

➢ To import a file with a precompiled list of access points into the Known AP List:

1. Take one of the following actions:
   - Select the **Replace** radio button to let the imported list of access points replace the existing Known AP List.

- Select the **Merge** radio button to add the imported list of access points to the existing Known AP List.

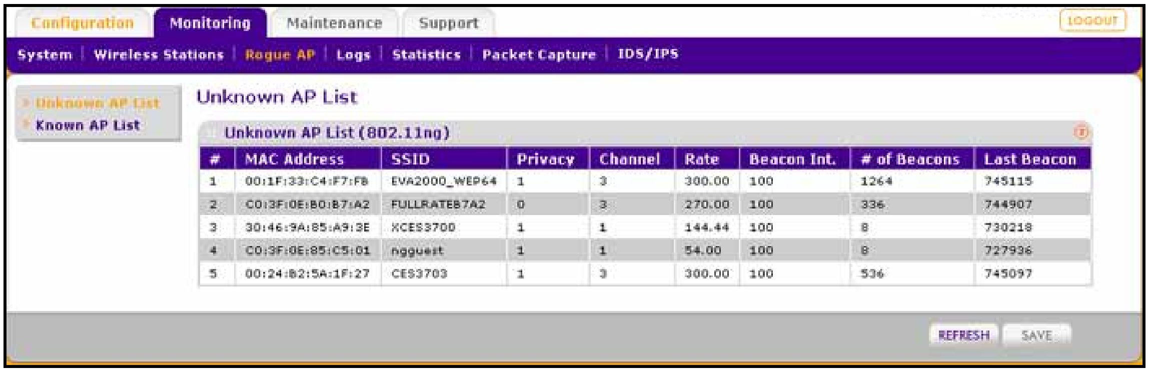
2. Click **Browse** and locate the file that contains the list of access points. This file needs to be a simple text file with one MAC address per line.
3. Select the file, and click **Open**.
4. Click **Apply** to upload the list of access points to the Known AP List.

View and Save Access Point Lists

The wireless access point detects nearby APs and wireless stations and maintains them in a list. You can use this list to prevent them from connecting to the wireless access point.

➢ **To view the Unknown AP List and save it to a file:**

1. Select **Monitoring > Rogue AP > Unknown AP List**. The Unknown AP List screen displays:



Unknown AP List

Unknown AP List (802.11ng)

#	MAC Address	SSID	Privacy	Channel	Rate	Beacon Int.	# of Beacons	Last Beacon
1	00:1F:33:C4:F7:FB	EVA2000_WEP64	1	3	300.00	100	1264	745115
2	C0:3F:0E:B0:B7:A2	FULLRATEB7A2	0	3	270.00	100	336	744907
3	30:46:9A:85:A9:3E	XCES3700	1	1	144.44	100	8	730218
4	C0:3F:0E:85:C5:01	ngguest	1	1	54.00	100	8	727936
5	00:24:B2:5A:1F:27	CES3703	1	3	300.00	100	536	745097

Figure 52.

2. Click **Refresh** to let the wireless access point discover the access points and populate the Unknown AP List for the configured wireless mode.

   The following table explains the fields of the Unknown AP List screen:

Table 22. Unknown AP List fields

Setting	Description
MAC Address	The MAC address of the unknown AP.
SSID	The SSID that the unknown AP is using.
Privacy	Indicates whether security is enabled (1 means enabled; 0 means disabled).
Channel	The channel that the unknown AP is using.
Rate	The transmit data rate in Mbps of the unknown the AP.
Beacon Int.	The interval for each beacon transmission in ms.

Table 22. Unknown AP List fields (continued)

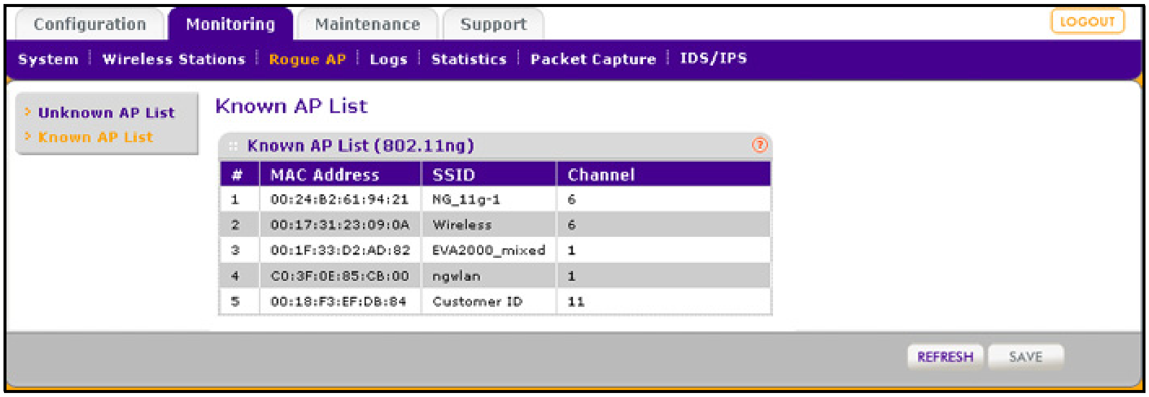
Setting	Description
# of Beacons	The number of beacons transmitted by the unknown AP that the wireless access point has detected.
Last Beacon	The time stamp that indicates the time when the most recent beacon was detected.

3. Click **Save** to export the list of unknown or known APs to a file. A window opens so you can browse to the location where you want to save the file. The default file name is macList.txt.

If you wish, you can now import the saved list into the Known AP List on the Rogue AP screen (see *Enable and Configure Rogue AP Detection* on page 85).

➢ To view the Known AP Lists and save it to a file:

1. Select **Monitoring > Rogue AP > Known AP List**. The Known AP List screen displays:



Known AP List

Known AP List (802.11ng)

#	MAC Address	SSID	Channel
1	00:24:B2:61:94:21	NG_11g-1	6
2	00:17:31:23:09:0A	Wireless	6
3	00:1F:33:D2:AD:82	EVA2000_mixed	1
4	C0:3F:0E:85:CB:00	ngwlan	1
5	00:18:F3:EF:DB:84	Customer ID	11

Figure 53.

2. Click **Refresh** to let the wireless access point discover the access points and populate the Known AP List for the configured wireless mode.

   The following table explains the fields of the Known AP List screen:

Table 23. Known AP List fields

Setting	Description
MAC Address	The MAC address of the known AP.
SSID	The SSID that the known AP is using.
Channel	The channel that the known AP is using.

3. Click **Save** to export the list of known access points to a file. A window opens so you can browse to the location where you want to save the file. The default file name is macList.txt.

You can now import the saved list into the Known AP List on the Rogue AP screen (see *Enable and Configure Rogue AP Detection* on page 85).

Configure Wireless Intrusion Detection and Prevention

- *Configure Wireless Intrusion Detection and Prevention Policy Settings*
- *Configure Wireless Intrusion Detection and Prevention Mail Settings*
- *Monitor Traps, Counters, and Ad Hoc Networks*

Configure Wireless Intrusion Detection and Prevention Policy Settings

The wireless access point provides a wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS) to detect and mitigate wireless attacks. These intrusion systems are referred to as IDS/IPS.

If enabled, the IDS recognizes multiple types of wireless attacks, and the IPS automatically neutralizes many attacks. Attacks are covered by preconfigured policy rules. When an attack occurs, the wireless access point can notify a network administrator though an email.

The following table lists all IDS/IPS policies with their policy rules. Most of these policies provide protection against denial of service (DoS) attacks. You can enable or disable IDS/IPS policies, but both the policies and the policy rules are not configurable.

All thresholds are measured over a short period. For the IDS/IPS to send a notification according to the policy rule, you first need to configure the email settings (see *Configure Wireless Intrusion Detection and Prevention Mail Settings* on page 95).

Table 24. IDS/IPS policies and policy rules

Policy	**Description**	**Policy Rule**	
		Threshold	**Notification**
Authentication flood	• **Attack**. Multiple authentication requests (5 or more) that use spoofed MAC addresses of legitimate clients are sent to the wireless access point. • **Result**. The client association table overflows, causing authentication requests from legitimate clients to be denied. • **Solution**. The oldest clients that are stuck in the authentication phase are removed from the table.	5	Trap
Association flood	• **Attack**. Multiple association requests (5 or more) that use spoofed MAC addresses of legitimate clients are sent to the wireless access point. • **Result**. The client association table overflows, causing association requests from legitimate clients to be denied. • **Solution**. The oldest associations are removed from the table.	5	Trap

Table 24. IDS/IPS policies and policy rules (continued)

Policy	Description	Policy Rule	
		Threshold	Notification
Unauthenticated association	• **Attack**. Multiple unauthenticated association requests (5 or more) that use spoofed MAC addresses of legitimate clients are sent to the wireless access point. • **Result**. The client association table overflows, causing authentication requests from legitimate clients to be denied. • **Solution**. The oldest clients that are stuck in the authentication phase are removed from the table.	5	Trap
Association table overflow	• **Attack**. Multiple clients (5 or more) that use spoofed MAC addresses of legitimate clients attempt to connect to the wireless access point. • **Result**. The client association table overflows, causing association requests from legitimate clients to be denied. • **Solution**. The oldest associations are removed from the table.	5	Trap
Authentication failure attack	• **Attack**. Multiple invalid authentication requests (5 or more) that use the spoofed MAC address of a legitimate client are sent to the wireless access point. • **Result**. The client is disconnected from the wireless access point. • **Solution**. The wireless access point determines if the legitimate client is already connected before processing an authentication request.	5	Trap
Deauthentication broadcast attack	• **Attack**. Multiple deauthentication frames (5 or more) that use the spoofed MAC address of the wireless access point are sent to legitimate clients. • **Result**. Clients are disconnected from the wireless access point. **Note:** The IDS detects this attack, but the IPS does not take action against this attack.	5	Trap
Disassociation flood	• **Attack**. Multiple disassociation frames (5 or more) that use the spoofed MAC address of the wireless access point are sent to a legitimate client. • **Result**. The client is disconnected from the wireless access point. **Note:** The IDS detects this attack, but the IPS does not take action against this attack.	5	Trap
Malformed 802.11 packets detected	• **Detection**. Multiple malformed packets (5 or more) are sent to the wireless access point. • **Result**. Clients behave unexpectedly or crash. • **Solution**. The wireless access point drops the malformed packets.	5	Trap

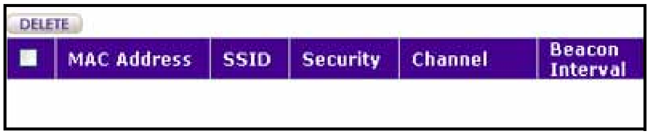
Table 24. IDS/IPS policies and policy rules (continued)

Policy	Description	Policy Rule	
		Threshold	Notification
EAPOL-start attack	• **Attack**. Multiple EAPOL start frames (5 or more) are sent to the wireless access point to initiate the RADIUS authentication process for clients. • **Result**. Wireless service is disrupted. • **Solution**. The wireless access point determines if the legitimate clients have already been authenticated before processing EAPOL start frames.	5	Trap
EAPOL-logoff attack	• **Attack**. Several EAPOL logoff frames (2 or more) that use the spoofed MAC address of a legitimate client are sent to the wireless access point to terminate a RADIUS-authenticated session. • **Result**. The client is disconnected from the wireless access point. • **Solution**. The wireless access point determines if it still receives traffic from the client before disconnecting the client.	2	Trap
Premature EAP failure attack	• **Attack**. Several premature EAP failure frames (2 or more) are sent to a legitimate client to suggest RADIUS authentication failure. • **Result**. The client cannot be authenticated and cannot connect to the wireless access point. **Note:** The IDS detects this attack, but the IPS does not take action against this attack.	2	Trap
Premature EAP success attack	• **Attack**. Several premature EAP success frames (2 or more) are sent to a legitimate client to suggest RADIUS authentication success. • **Result**. The client cannot be authenticated and cannot connect to the wireless access point. **Note:** The IDS detects this attack, but the IPS does not take action against this attack.	2	Trap
CTS flood	• **Attack**. Multiple clear-to-send (CTS) frames (60 or more) are sent to the wireless access point. • **Result**. Wireless service is disrupted. • **Solution**. The wireless access point sends a channel change frame to the legitimate clients and uses automatic channel selection to switch to a new clear channel.	60	Trap
RTS flood	• **Attack**. Multiple request-to-send (RTS) frames (60 or more) are sent to the wireless access point. • **Result**. Wireless service is disrupted. • **Solution**. The wireless access point sends a channel change frame to the legitimate clients and uses automatic channel selection to switch to a new clear channel.	60	Trap

Table 24. IDS/IPS policies and policy rules (continued)

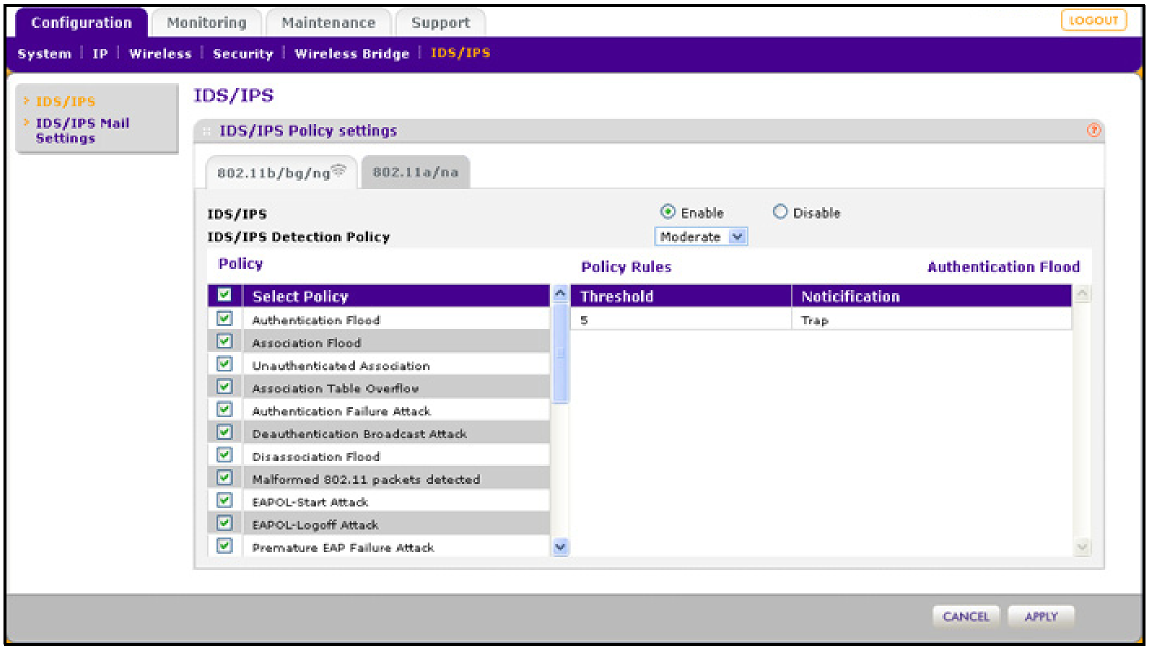
Policy	Description	Policy Rule	
		Threshold	Notification
RF jamming attack	• **Attack**. Multiple RF transmissions (100 or more) are sent to the wireless access point, jamming the radio frequency. • **Result**. Wireless service is disrupted. **Note:** The IDS detects this attack, but the IPS does not take action against this attack.	100	Trap
Virtual carrier attack	• **Attack**. Multiple frames (60 or more) with a large duration value are sent to the wireless access point. • **Result**. Wireless service is disrupted. • **Solution**. The wireless access point sends a channel change frame to the legitimate clients and uses automatic channel selection to switch to a new clear channel.	60	Trap
MAC spoofing	• **Attack**. Several frames (3 or more) that contain the spoofed MAC address of the wireless access point itself or the spoofed MAC address of a legitimate client are sent to the wireless access point. • **Result**. Wireless security might be compromised. **Note:** The IDS detects MAC spoofing, but the IPS does not take action against MAC spoofing.	3	Trap
Rogue AP detection	• **Detection**. A wireless access point is not in the managed AP list (see *View and Save Access Point Lists* on page 87) and is not connected to the secured wireless or wired network. • **Result**. Wireless security might be compromised. **Note:** The IDS detects rogue APs, but the IPS does not take action against rogue APs. For information about how to exclude rogue APs from your network, see *Enable Rogue AP Detection and Monitor Access Points* on page 85.	0	Trap
Ad-hoc network detected	• **Detection**. A group of wireless access points are part of an ad hoc network that might broadcast the same SSID as the secured wireless network. • **Result**. Wireless security might be compromised. **Note:** The IDS detects ad hoc networks, but the IPS does not take action against ad hoc networks.	0	Trap
Ad-hoc network with wired connectivity	• **Detection**. A group of wireless access points are part of an ad hoc network that has a wired connection and that might broadcast the same SSID as the secured wireless network. • **Result**. Wireless security might be compromised. **Note:** The IDS detects ad hoc networks, but the IPS does not take action against ad hoc networks.	0	Trap

Table 24. IDS/IPS policies and policy rules (continued)

Policy	Description	Policy Rule	
		Threshold	Notification
Known client associating with ad-hoc network	• **Detection**. Clients that should be connected to the secured wireless network are instead connected to wireless access points that are part of an ad hoc network. • **Result**. Wireless security might be compromised. • **Solution**. The clients are disconnected from the ad hoc network.	0	Trap
AP property changed	• **Detection**. Unauthorized changes such as a change of SSID, security settings, or channel are made on a known wireless access point in the network. • **Result**. Wireless security is compromised and clients cannot connect to the wireless access point. **Note:** The IDS detects that the properties of a known wireless access point in the network are changed, but the IPS does not take action. The changes that the IDS detects are listed in a table. The affected wireless access point is identified by its MAC address. To correct the situation, access the web management interface of the affected wireless access point, and reverse the changes.  □ | MAC Address | SSID | Security | Channel | Beacon Interval To remove the detected changes from the table: 1. Select the check box to the left of the wireless access point for which you want to remove the changes from the table. 2. Above the table, click **Delete**.	0	Trap
Device probing for access points	• **Detection**. Multiple probe requests (30 or more) are sent to collect information about the wireless access point for possible future attacks. For example, it is suspect when there are too many probe requests with a different SSID from same MAC address. • **Result**. An attack might occur, or wireless security might become compromised. • **Solution**. The wireless access point does not respond to probe requests that do not contain its SSID.	30	Trap
PS poll flood attack	• **Attack**. Multiple power save (PS)–Poll frames (50 or more) are sent to the wireless access point from an address that has a spoofed MAC address of a legitimate client. • **Result**. Traffic that is intended for the legitimate client is sent to the attacking address and is lost. • **Solution**. PS-Poll frames without a corresponding traffic indication map (TIM) are rejected.	50	Trap

➢ To enable and configure the IDS/IPS:

1. Select **Configuration > IDS/IPS**. The IDS/IPS screen displays:



IDS/IPS

IDS/IPS Policy settings

IDS/IPS ● Enable ○ Disable

IDS/IPS Detection Policy: Moderate

Policy

☑	Select Policy
☑	Authentication Flood
☑	Association Flood
☑	Unauthenticated Association
☑	Association Table Overflow
☑	Authentication Failure Attack
☑	Deauthentication Broadcast Attack
☑	Disassociation Flood
☑	Malformed 802.11 packets detected
☑	EAPOL-Start Attack
☑	EAPOL-Logoff Attack
☑	Premature EAP Failure Attack

Policy Rules — Authentication Flood

Threshold	Noticification
5	Trap

Figure 54.

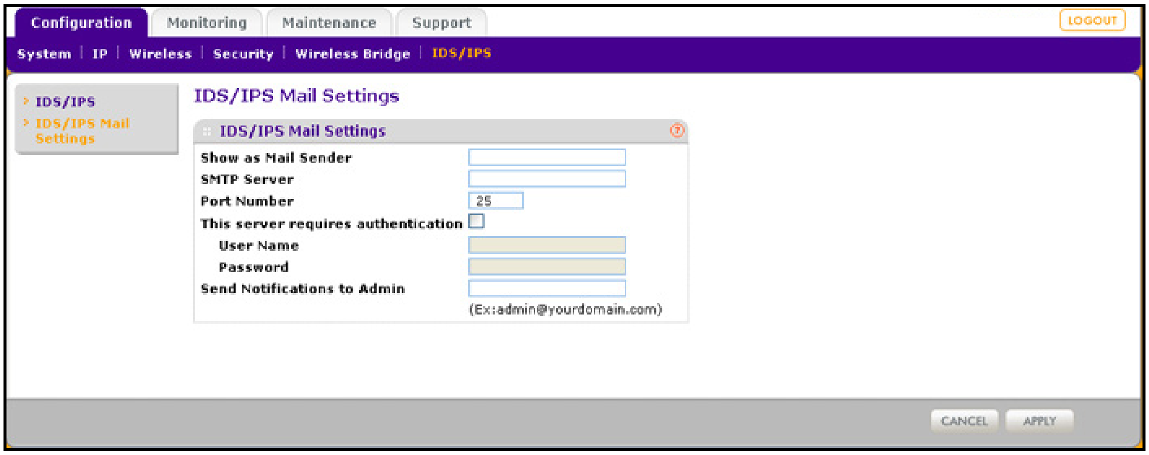
2. Select the **Enable** radio button. By default, the IDS/IPS is disabled.
3. Specify the detection policy by making a selection from the IDS/IPS Detection Policy drop-down list:
   - **Mild**. The wireless access point scans for attacks every 10 seconds.
   - **Moderate**. The wireless access point scans for attacks every 5 seconds. This is the default setting.
   - **Aggressive**. The wireless access point scans for attacks every second.
4. Optional: Click a policy name to display the policy rules that are stated next to the policy in the table. IDS/IPS policy rules are not configurable.
5. Optional: Clear check boxes for policies that you want to disable. By default, the check box next to Select Policy in the table heading is selected, and all IDS/IPS policies are enabled.
6. Click **Apply** to save your settings.

Configure Wireless Intrusion Detection and Prevention Mail Settings

For the IDS/IPS to send a notification according to the policy rule, you need to configure the email settings.

➤ To configure IDS/IPS email settings:

1. Select **Configuration > IDS/IPS Mail Settings**. The IDS/IPS Mail Settings screen displays:



IDS/IPS Mail Settings

IDS/IPS Mail Settings

Show as Mail Sender	
SMTP Server	
Port Number	25
This server requires authentication	□
User Name	
Password	
Send Notifications to Admin	
	(Ex:admin@yourdomain.com)

Figure 55.

2. Configure the settings as explained in the following table.

Table 25. IDS/IPS mail settings

Setting	Description	
Show as Mail Sender	A descriptive name of the sender for email identification purposes. For example, enter WNAP620-IDS-IPS@company.com.	
SMTP Server	The IP address or Internet name of the outgoing email SMTP server of your ISP.	
Port Number	The port number of the outgoing email SMTP server of your ISP. The default port number is 25.	
This server requires authentication	If the SMTP server requires authentication, select the **This server requires authentication** check box, and enter the user name and password.	
	User Name	The user name for SMTP server authentication.
	Password	The password for SMTP server authentication.
Send Notifications to Admin	The email address to which the notifications should be sent. Typically, this is the email address of the administrator.	

3. Click **Apply** to save your settings.

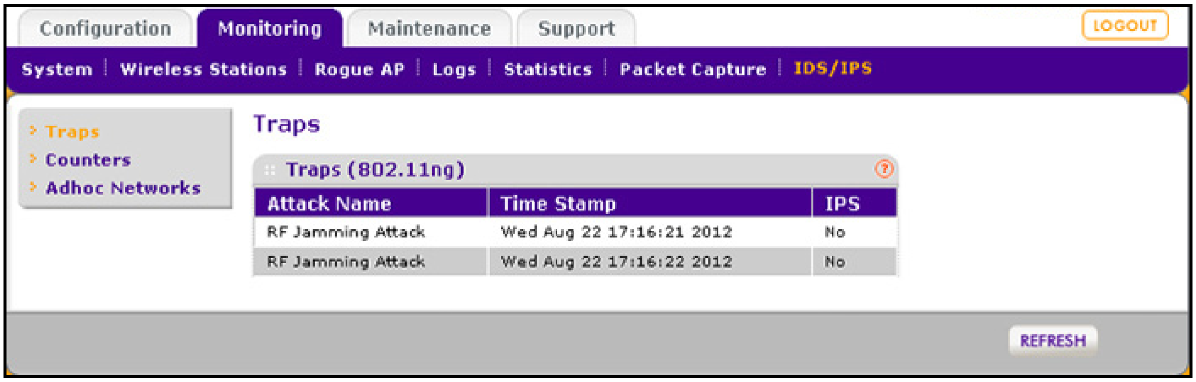
Monitor Traps, Counters, and Ad Hoc Networks

The IDS/IPS monitoring screens provide information about the most recent attacks, the number of occurrences per attack, and ad hoc networks. This information is read only.

Most Recent Attacks

➢ **To display the last 50 attacks against the wireless access point and its clients:**

Select **Monitoring > IPS/IDS > Traps**. The Traps screen displays.



Traps

Traps (802.11ng)

Attack Name	Time Stamp	IPS
RF Jamming Attack	Wed Aug 22 17:16:21 2012	No
RF Jamming Attack	Wed Aug 22 17:16:22 2012	No

Figure 56.

To update the information onscreen, click **Refresh**.

The following table explains the fields of the Traps screen:

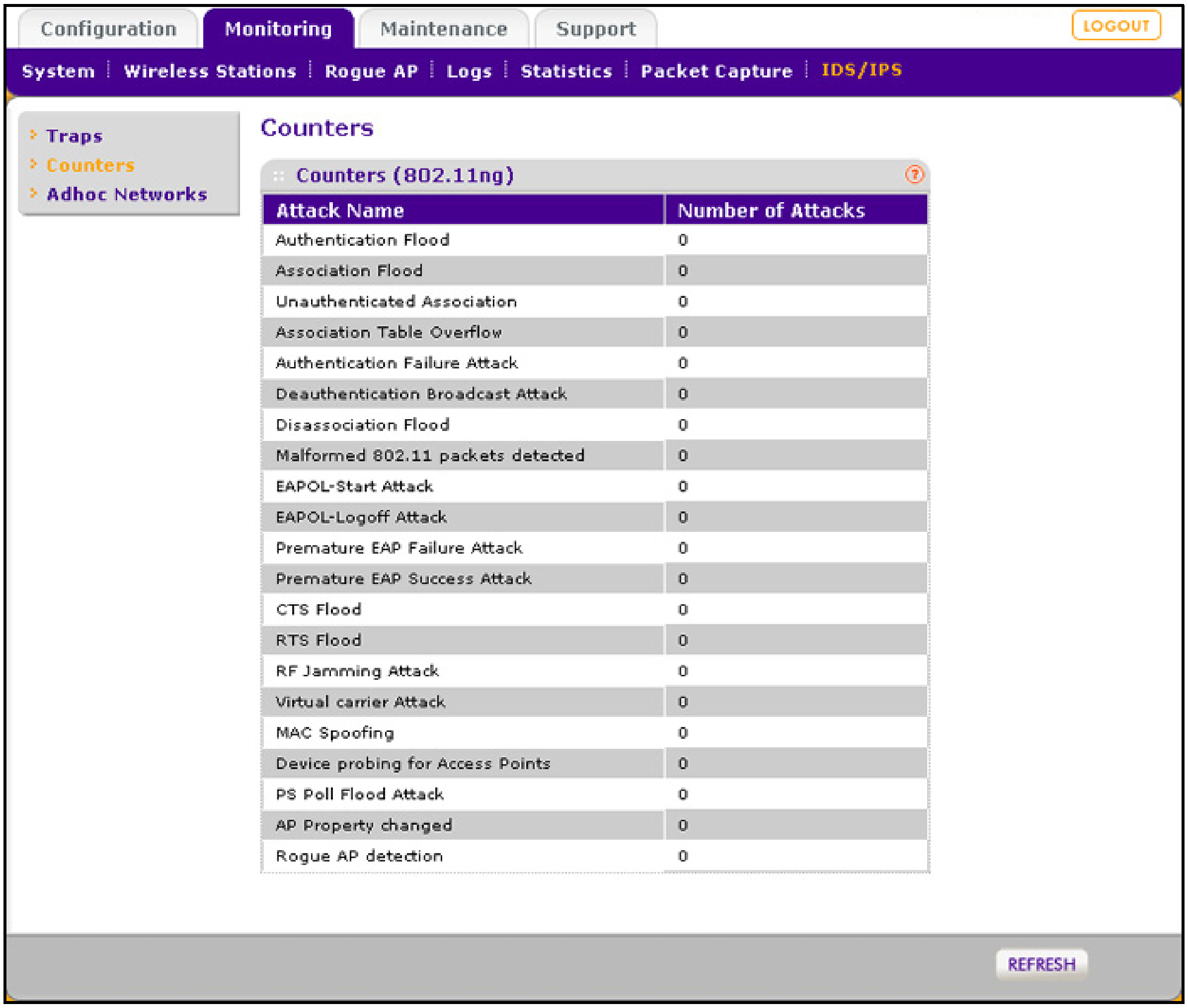
Table 26. Traps fields

Setting	Description
Attack Name	The name of the attack that corresponds to a policy in *Table 24* on page 89.
Time Stamp	The time that the attack occurred.
IPS	If the IPS has prevented the attack, the field displays Yes. If the IPS did not prevent the attack, or the IPS is not applicable to the attack, the field displays No.

Attack Counter

➢ **To display the number of occurrences per attacks:**

Select **Monitoring > IPS/IDS > Counters**. The Counters screen displays.



Counters

Counters (802.11ng)

Attack Name	Number of Attacks
Authentication Flood	0
Association Flood	0
Unauthenticated Association	0
Association Table Overflow	0
Authentication Failure Attack	0
Deauthentication Broadcast Attack	0
Disassociation Flood	0
Malformed 802.11 packets detected	0
EAPOL-Start Attack	0
EAPOL-Logoff Attack	0
Premature EAP Failure Attack	0
Premature EAP Success Attack	0
CTS Flood	0
RTS Flood	0
RF Jamming Attack	0
Virtual carrier Attack	0
MAC Spoofing	0
Device probing for Access Points	0
PS Poll Flood Attack	0
AP Property changed	0
Rogue AP detection	0

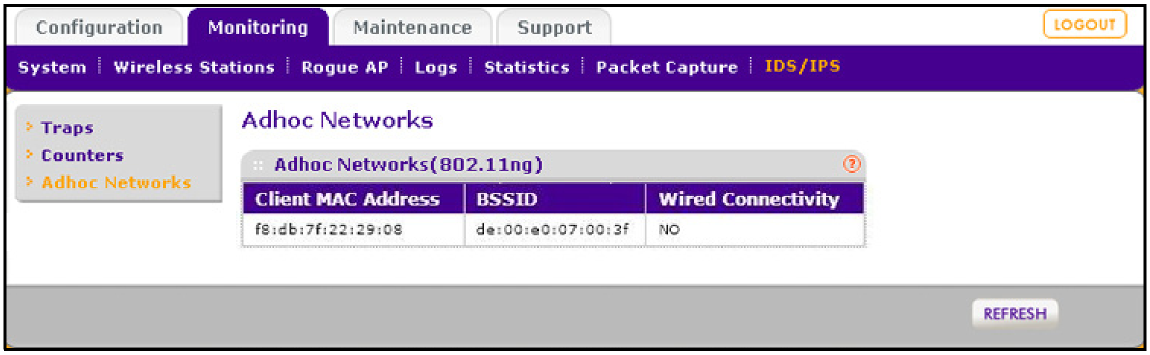
Figure 57.

To update the information onscreen, click **Refresh**.

Ad Hoc Networks

➢ **To display the ad hoc networks and their associated clients:**

Select **Monitoring > IPS/IDS > Adhoc Networks**. The Adhoc Network screen displays.



Adhoc Networks

Adhoc Networks(802.11ng)

Client MAC Address	BSSID	Wired Connectivity
f8:db:7f:22:29:08	de:00:e0:07:00:3f	NO

Figure 58.

To update the information onscreen, click **Refresh**.

The following table explains the fields of the Adhoc Networks screen:

Table 27. Ad hoc network fields

Setting	Description
Client MAC Address	The MAC address of the client that is connected to the ad hoc network.
BSSID	The BSSID of the ad hoc network. **Note:** A wireless access point that is connected to a wired network and a set of wireless stations is called a basic service set (BSS). The basic service set identifier (BSSID) differentiates one WLAN from another.
Wired Connectivity	If the ad hoc network has wired connectivity, the field displays YES. If the ad hoc network does not have wired connectivity, the field displays NO.

Advanced Configuration 5

This chapter describes how to configure the advanced features of the wireless access point. The chapter includes the following sections:

- *Configure IPv6 Settings and Optional DHCPv6 Server Settings*
- *Configure Spanning Tree Protocol, 802.1Q VLAN, and Link Layer Discovery Protocol*
- *Configure Hotspot Settings*
- *Configure Advanced Wireless Settings*
- *Configure Advanced Quality of Service Settings*
- *Configure Quality of Service Policies*
- *Configure Wireless Bridging*

Configure IPv6 Settings and Optional DHCPv6 Server Settings

The wireless access point supports IPv6:

- You can manage the wireless access point from an IPv6 address.
- The wireless access point can function as an IPv6 DHCP client.
- The DHCPv6 server of the wireless access point can allocate IPv6 addresses to its wireless clients, either through stateless or stateful allocation.

Configure the IPv6 Settings

Note: For information about how to configure the IPv4 settings, see *Configure the IPv4 Settings* on page 25.

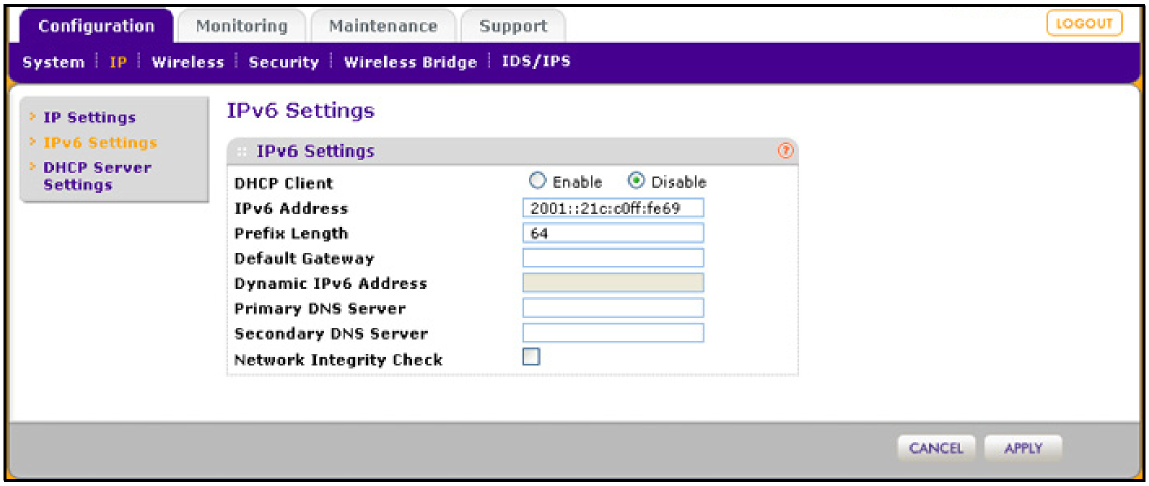
WARNING:

If you enable the DHCP client, the IP address of the wireless access point changes when you click Apply, causing you to lose your connection to the wireless access point. You then need to use the new IP address to reconnect to the wireless access point.

Tip: If you enable the DHCP client on the wireless access point, you can discover the new IP address of the wireless access point by accessing the DHCP server on your LAN, or by using a network IP address scanner application.

➤ To configure the IPv6 settings:

1. Select **Configuration > IP > IPv6 Settings**. The IP Settings screen displays:



IPv6 Settings

IPv6 Settings

DHCP Client	○ Enable ● Disable
IPv6 Address	2001::21c:c0ff:fe69
Prefix Length	64
Default Gateway	
Dynamic IPv6 Address	
Primary DNS Server	
Secondary DNS Server	
Network Integrity Check	□

Figure 59.

2. Configure the IPv6 settings as explained in the following table:

Table 28. IPv6 settings

Setting	Description
DHCP Client	By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCPv6 server on your LAN and you select the **Enable** radio button, the wireless access point receives its dynamic IPv6 address, prefix length, and default gateway settings automatically from the DHCPv6 server on your network when you connect the wireless access point to your LAN.
IPv6 Address	Enter the IP address of your wireless access point. The default IP address is **2001::21c:c0ff:fe69**. To change the address, enter an unused IPv6 address from the address range used on your LAN.
Prefix Length	Enter the prefix length for the IPv6 address. The default prefix length us 64.

Table 28. IPv6 settings (continued)

Setting	Description
Default Gateway	Enter the IPv6 address of the ISP gateway to which the wireless access point connects.
Dynamic IPv6 Address	The dynamic IPv6 address that is assigned by the DHCPv6 server on your network. This address does not overwrite the address in the IPv6 Address field.
Primary DNS Server	Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as www.netgear.com) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your wireless access point during login. If the ISP does not transfer an address, you need to obtain it from the ISP and enter it manually in this field.
Secondary DNS Server	
Network Integrity Check	Select this check box to validate that the upstream link is active before allowing wireless associations. Ensure that the default gateway is configured.

3. Click **Apply** to save your settings.

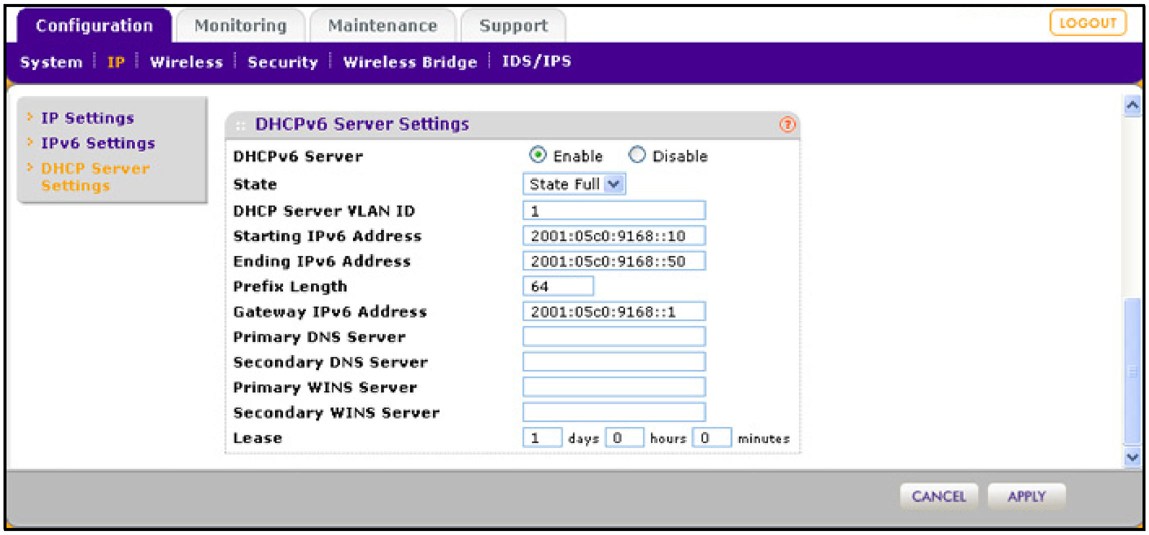
Configure the Optional DHCPv6 Server

The wireless access point provides a built-in DHCPv6 server for wireless clients only, which can be especially useful in small networks. When the DHCP server is enabled, the wireless access point provides preconfigured TCP/IP configurations to all connected wireless stations.

Note: For information about how to configure the DHCPv4 server, see *Configure the Optional DHCPv4 Server* on page 27.

➢ **To configure DHCPv6 server settings:**

1. Select **Configuration > IP > DHCP Server Settings**. The DHCP Server Settings screen displays. The following figure displays the DHCPv6 server settings only. For information about the DHCPv6 server settings, see *Configure the Optional DHCPv4 Server* on page 27.



DHCPv6 Server Settings

DHCPv6 Server ● Enable ○ Disable

State: State Full

DHCP Server VLAN ID: 1

Starting IPv6 Address: 2001:05c0:9168::10

Ending IPv6 Address: 2001:05c0:9168::50

Prefix Length: 64

Gateway IPv6 Address: 2001:05c0:9168::1

Primary DNS Server:

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Lease: 1 days 0 hours 0 minutes

Figure 60.

2. Configure the settings as explained in the following table:

Table 29. DHCP server settings for IPv6

Setting	Description
Select the DHCPv6 Server **Enable** radio button to enable the DHCP server. Use the default settings or specify the pool of IPv6 addresses to be assigned by setting the starting IPv6 address and ending IPv6 address. These addresses should be part of the same IP address subnet as the wireless access point's LAN IPv6 address.	
State	From the State drop-down list, select the DHCPv6 server option: • **Stateless**. The IPv6 clients in the LAN generate their own IP address by using a combination of locally available information and router advertisements, but receive DNS server information from the DHCPv6 server. **Note:** When you select the Stateless option, you do not need to configure any other DHCPv6 server settings fields. • **Stateful**. The IPv6 clients in the LAN obtain an interface IP address, configuration information such as DNS server information, and other parameters from the DHCPv6 server. The IP address is a dynamic address. **Note:** When you select the Stateful option, you need to configure all other DHCPv6 server settings fields.
DHCP Server VLAN ID	Enter the VLAN ID for the DHCP server. The VLAN ID range is from 1 to 4094. The default VLAN is 1.
Starting IPv6 Address	Enter the first address in the range of IPv6 addresses to be assigned to DHCP clients. The default address is 2001:05c0:9168::10.
Ending IPv6 Address	Enter the last address in the range of IPv6 addresses to be assigned to DHCP clients. The default address is 2001:05c0:9168::50.

Table 29. DHCP server settings for IPv6 (continued)

Setting	Description
Prefix Length	Enter the prefix length to be used by DHCP clients. The default length is 64.
Gateway IPv6 Address	Enter the IPv6 address of the default routing gateway to be used by DHCP clients. The default address is 2001:05c0:9168::1.
Primary DNS Address	Enter the IP address of the primary Domain Name System (DNS) server available to DHCP clients.
Secondary DNS Address	Enter the IP address of the secondary DNS server available to DHCP clients.
Primary WINS Server	Enter the IP address of the primary WINS server for the network, if there is any.
Secondary WINS Server	Enter the IP address of the secondary WINS server for the network, if there is any.
Lease	Enter the period that the DHCP server grants to DHCP clients to use the assigned IP addresses. The default time is one day.

3. Click **Apply** to save your settings.

Configure Spanning Tree Protocol, 802.1Q VLAN, and Link Layer Discovery Protocol

- *Configure STP and VLANs*
- *Configure Ethernet LLDP*

As part of the advanced system configuration, you can enable the Spanning Tree Protocol (STP), configure the VLANs, and enable Ethernet Link Layer Discovery Protocol (LLDP).

Configure STP and VLANs

STP provides network traffic optimization in locations where multiple wireless access points are active by preventing path redundancy. NETGEAR recommends that you enable STP if you have more than one active wireless access point at your location.

The 802.1Q VLAN protocol on the wireless access point logically separates traffic on the same physical network:

- **Untagged VLAN**. When the wireless access point sends frames that are associated with the untagged VLAN from its Ethernet interface, those frames are untagged. When the wireless access point receives untagged frames over its Ethernet interface, those frames are assigned to the untagged VLAN.

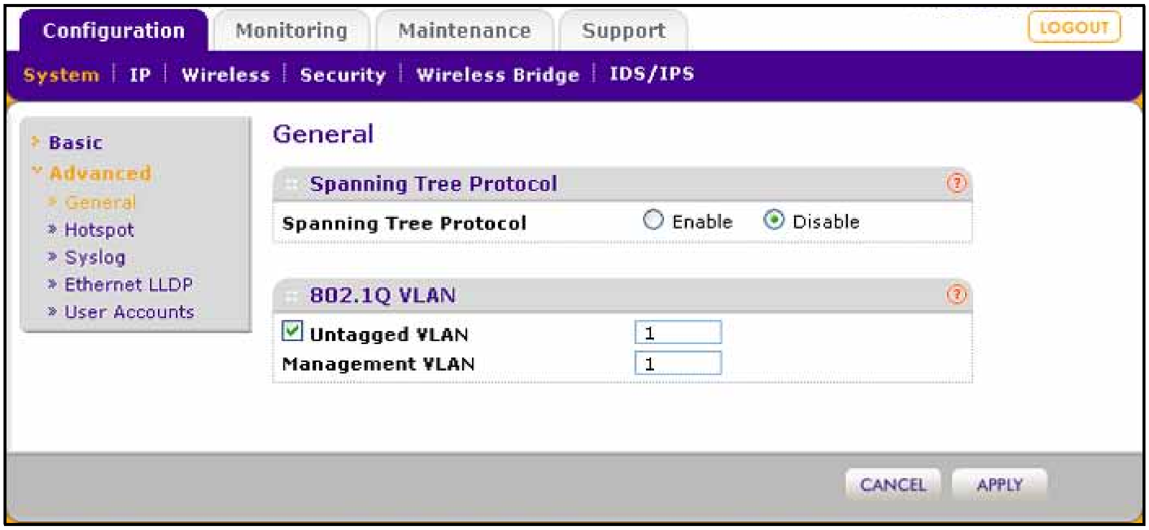
Note: Select the **Untagged VLAN** check box only if the hubs and switches on your LAN support the 802.1Q VLAN protocol. Likewise, change the untagged VLAN value only if the hubs and switches on your LAN support the 802.1Q VLAN protocol.

- **Tagged VLAN**. When you clear the Untagged VLAN check box, the wireless access point tags all frames that are sent from its Ethernet interface. Only incoming frames that are tagged with known VLAN IDs are accepted.
- **Management VLAN**. The management VLAN can be active only when the wireless access point functions as a point-to-point or point-to-multipoint bridge (see *Configure Wireless Bridging* on page 118). The management VLAN is used for managing traffic (Telnet, SNMP, and HTTP) to and from the wireless access point.

  Frames belonging to the management VLAN are not given any 802.1Q header when they are sent over the trunk. If a port is in a single VLAN, it can be untagged. However, if the port is a member of multiple VLANs, it needs to be tagged.

➢ To configure STP and VLANs:

1. Select **Configuring > System > Advanced > General**. The advanced General system settings screen displays:



General

Spanning Tree Protocol

Spanning Tree Protocol ○ Enable ● Disable

802.1Q VLAN

☑ Untagged VLAN 1

Management VLAN 1

Figure 61.

2. Specify the settings as explained in the following table:

Table 30. STP and VLAN settings

Setting	Description
Spanning Tree Protocol	
Spanning Tree Protocol	Select the **Enable** radio button to enable STP to prevent path redundancy. By default, the Disable radio button is selected.
802.1Q VLAN	
Untagged VLAN	Select the **Untagged VLAN** check box to configure one VLAN as an untagged VLAN. By default, the Untagged VLAN check box is selected. Specify a VLAN ID. The default VLAN ID is 1.
Management VLAN	Specify an ID for the VLAN from which the wireless access point can be managed. The default VLAN ID is 1. **Note:** If you configure the management VLAN ID as 0 (zero), the wireless access point can be managed over any VLAN, and frames that belong to the management VLAN are not tagged with an 802.1Q header when sent over the trunk.

WARNING:

Selecting the Untagged VLAN check box or changing the untagged VLAN value causes loss of IP connectivity if the hubs and switches on your LAN have not yet been configured with the corresponding VLAN.

3. Click **Apply** to save your settings.

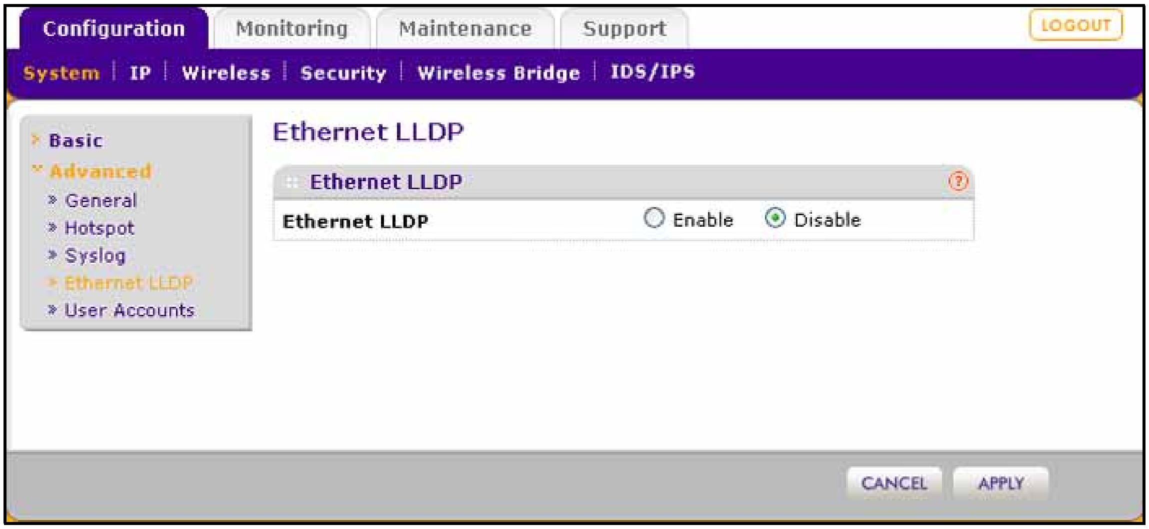
Configure Ethernet LLDP

Link Layer Discovery Protocol (LLDP), IEEE 802.1ab, is a management tool that delivers link-layer messages to adjacent network devices. For example, LLDP messages enable networking devices such as switches and management tools to discover the wireless access point in the network, and might indicate whether the wireless access point receives power through a PoE connection. LLDP is intervendor compatible.

By default, LLDP is enabled on the wireless access point.

➢ **To turn off LLDP:**

1. Select **Configuring > System > Advanced > Ethernet LLDP**. The Ethernet LLDP screen displays:



Ethernet LLDP ○ Enable ● Disable

Figure 62.

2. Select the **Disable** radio button. By default, the Enable radio button is selected.
3. Click **Apply** to save your settings.

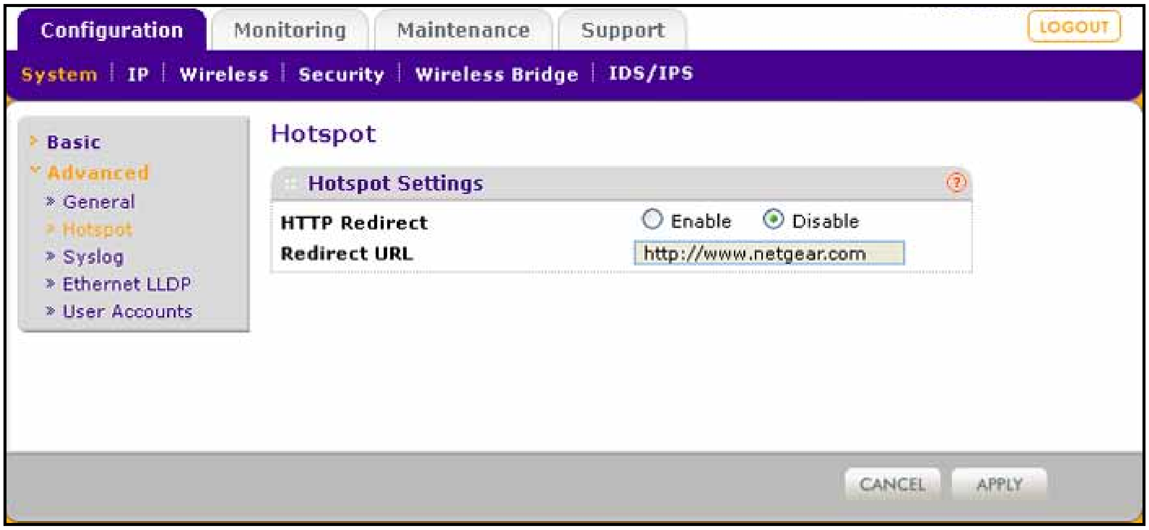
Configure Hotspot Settings

If the wireless access point functions as a public access point and you want it to capture and redirect all HTTP requests (over TCP, port 80), set up a hotspot server to redirect the requests to the specified URL and manage the clients. For example, you can redirect HTTP requests to a web server for authentication, timing control, or advertising. A hotel might want all wireless connections to go to its server to start a billing transaction.

Note: The redirection occurs only the first time that a wireless client opens a web browser.

➢ **To set up a hotspot server:**

1. Select **Configuration > System > Advanced > Hotspot**. The Hotspot screen displays:



Hotspot

Hotspot Settings

HTTP Redirect	○ Enable ● Disable
Redirect URL	http://www.netgear.com

Figure 63.

2. To enable HTTP redirection, select the **Enable** radio button. By default, the Disable radio button is selected.
3. In the Redirect URL field, enter the URL of the web server to which you wish to redirect HTTP requests.
4. Click **Apply** to save your settings. All HTTP requests are now redirected to the specified URL.

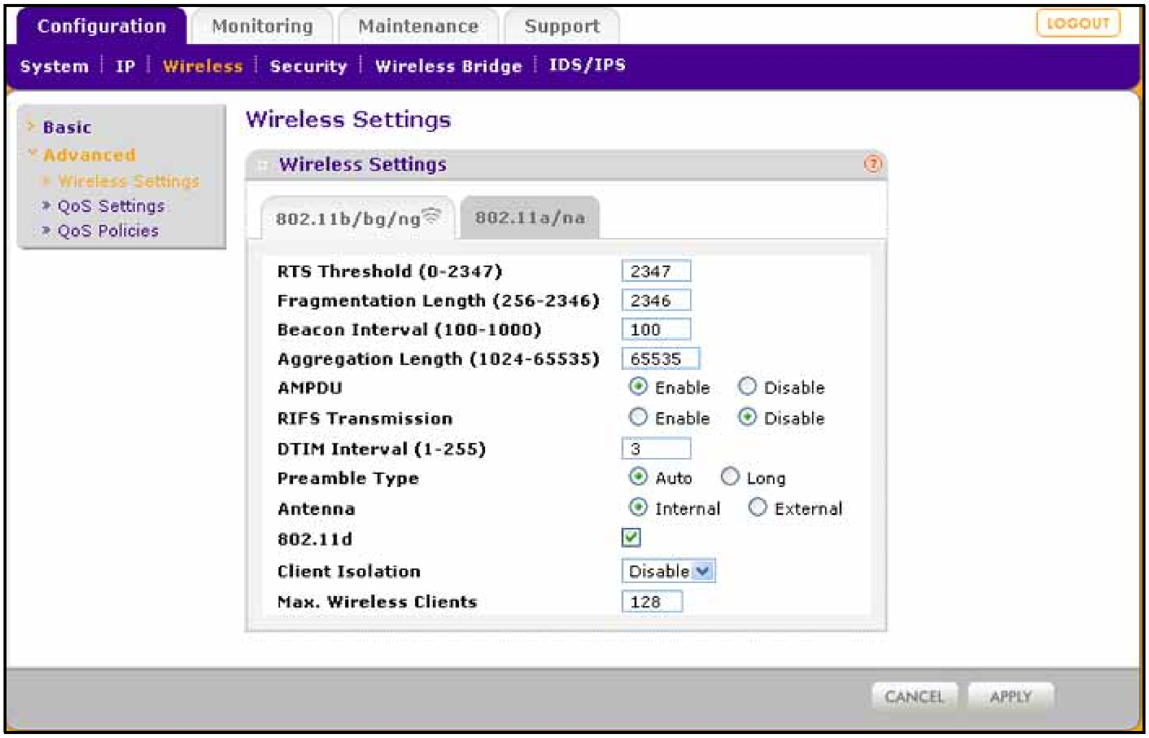
Configure Advanced Wireless Settings

Use the advanced Wireless Settings screen to configure and enable various WLAN settings for the 802.11b/bg/ng or 802.11a/na modes. You can configure the settings only for the active mode. (For information about how to change the wireless mode, see *Configure the Basic Wireless Settings* on page 28.)

The default WLAN settings normally work well. However, you can use the advanced settings to fine-tune the overall performance of the wireless access point for your specific environment.

➢ To configure advanced wireless settings:

1. Select **Configuration > Wireless > Advanced > Wireless Settings**. The advanced Wireless Settings screen displays. The following figure shows the 11ng settings, as indicated by the radio wave icon (📶) that is displayed next to ng:



RTS Threshold (0-2347): 2347
Fragmentation Length (256-2346): 2346
Beacon Interval (100-1000): 100
Aggregation Length (1024-65535): 65535
AMPDU: ● Enable ○ Disable
RIFS Transmission: ○ Enable ● Disable
DTIM Interval (1-255): 3
Preamble Type: ● Auto ○ Long
Antenna: ● Internal ○ External
802.11d: ☑
Client Isolation: Disable
Max. Wireless Clients: 128

Figure 64.

2. Optional: To configure advanced wireless settings for the 802.11a/na modes, click the **802.11a/na** tab.
3. Specify the settings as explained in the following table:

Table 31. Advanced wireless settings

Setting	Description
RTS Threshold (0–2347)	Enter the Request to Send (RTS) threshold. The default setting is 2347. If the packet size is equal to or less than the RTS threshold, the wireless access point uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism, and the data frame is transmitted immediately after the silence period. If the packet size is larger than the RTS threshold, the wireless access point uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting station sends an RTS packet to the receiving station and waits for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data.
Fragmentation Length (256–2346)	Enter the maximum packet size that is used for the fragmentation of data packets. Packets that are larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation length needs to be an even number. The default setting is 2346.

Table 31. Advanced wireless settings (continued)

Setting	Description
Beacon Interval (100–1000)	Enter the interval between 100 ms and 1000 ms for each beacon transmission, which allows the wireless access point to synchronize the wireless network. The default setting is 100.
Aggregation Length (1024–65535) **Note:** This setting does not apply to the 802.11a mode.	Enter the maximum length of aggregated MAC protocol data unit (A-MPDU) packets. Larger aggregation lengths could lead to better network performance. Aggregation is a mechanism used to achieve higher throughput. The default setting is 65535.
AMPDU **Note:** This setting does not apply to the 802.11b/bg modes and the 802.11a mode.	Select the **Enable** radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling the aggregated MAC protocol data unit (A-MPDU) could lead to better network performance. By default, the Enable radio button is selected.
RIFS Transmission **Note:** This setting does not apply to the 802.11b/bg modes and the 802.11a mode.	Select the **Enable** radio button to allow transmission of successive frames at different transmit powers. Enabling reduced interframe space (RIFS) could lead to better network performance. By default, the Disable radio button is selected.
DTIM Interval (1–255)	Enter the delivery traffic indication message (DTIM) interval, also referred to as the data beacon rate, which indicates the beacon delivery traffic indication message period in multiples of beacon intervals. This value needs to be between 1 and 255. The default setting is 3.
Preamble Type **Note:** This setting does not apply to the 802.11a/na modes.	Select one of the following radio buttons to specify the preamble type: • **Long**. A long transmit preamble might provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. • **Auto**. The Auto setting enables the wireless access point to handle both long and short preambles. The default setting is Auto.
Antenna **Note:** This setting does not apply to the 802.11a/na modes.	Select one of the following radio buttons to specify the antenna: • **Internal**. Enables the internal antenna. This is the default setting. • **External**. Enables an optional external antenna or antennas.
802.11d **Note:** This setting does not apply to the 802.11a/na modes.	Select this check box to enable support for additional regulatory domains that are not in the current standard; support includes the addition of a country information element to beacons, probe requests, and probe responses. This check box is selected by default.
Client Isolation	From the drop-down list, select one of the following options: • **Enable**. Communication between wireless clients that are associated to different virtual access points (VAPs) is blocked. • **Disable**. Communication between wireless clients that are associated to different VAPs is allowed. This is the default setting.
Max. Wireless Clients	Enter the maximum number of wireless clients that can simultaneously connect to the wireless access point at one time. The default setting is 128 clients.

4. Click **Apply** to save your settings.

Configure Advanced Quality of Service Settings

For most networks, the default Quality of Service (QoS) queue settings work well. For information about how to configure basic QoS, see *Configure Basic Wireless Quality of Service* on page 62.

You can specify the settings on multiple queues for increased throughput and better performance of differentiated wireless traffic such as Voice-over-IP (VoIP), other types of audio, video, and streaming media, as well as traditional IP data.

The advanced QoS options on the wireless access point are as follows:

- **AP EDCA parameters**. Specify the access point (AP) Enhanced Distributed Channel Access (EDCA) settings for different types of data transmitted from the wireless access point to wireless clients.
- **Station EDCA parameters**. Specify the station EDCA parameters for different types of data transmitted from the wireless clients to the wireless access point. If WMM is disabled, you cannot configure the Station EDCA parameters. (For information about how to enable WMM, see *Configure Basic Wireless Quality of Service* on page 62.)

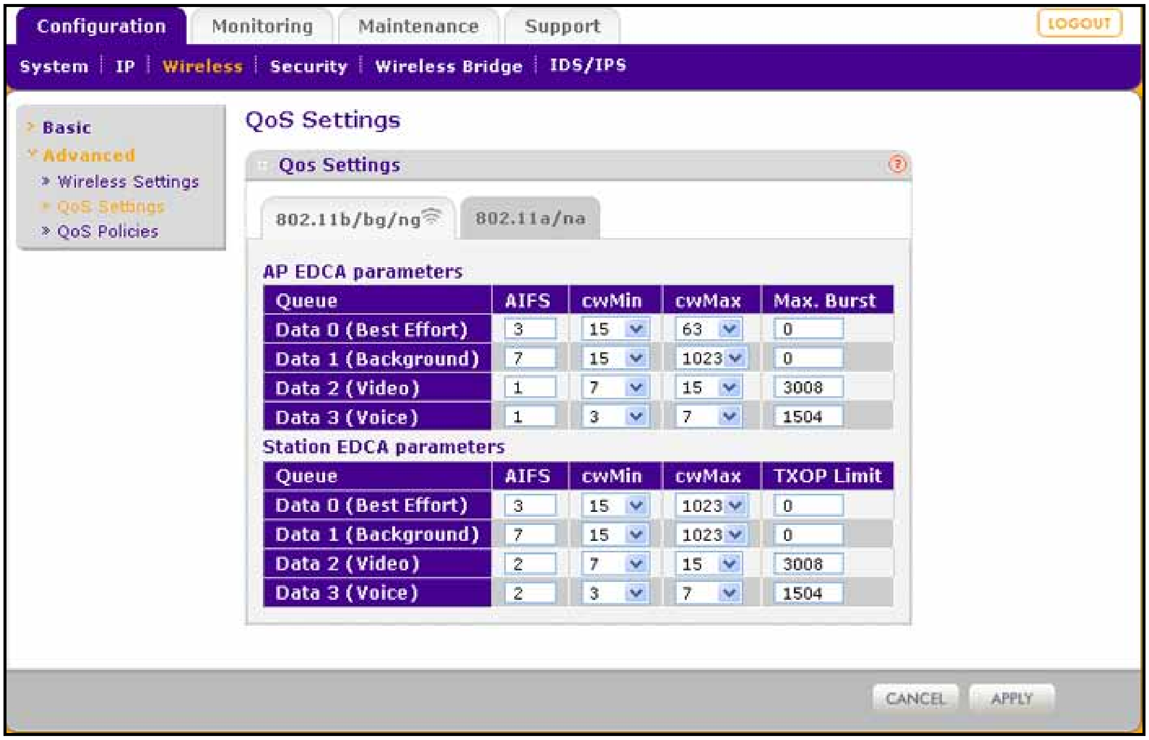
When you configure the EDCA settings, the wireless access point can leverage existing information in the IP packet header that is related to the Type of Service (ToS). The wireless access point examines the ToS field in the headers of all packets that it processes. Based on the value in a packet's ToS field, the wireless access point prioritizes the packet for transmission by assigning it to one of the queues. A different type of data is associated with each queue. You can configure how the wireless access point treats each queue.

The queues defined for different types of data transmitted from AP-to-station and station-to-AP are:

- **Data 0 (Best Effort)**. Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
- **Data 1 (Background)**. Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
- **Data 2 (Video)**. Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
- **Data 3 (Voice)**. Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.

➤ **To configure advanced QoS:**

1. Select **Configuration > Wireless > Advanced > QoS Settings**. The advanced QoS Settings screen displays:



QoS Settings

Qos Settings

802.11b/bg/ng | 802.11a/na

AP EDCA parameters

Queue	AIFS	cwMin	cwMax	Max. Burst
Data 0 (Best Effort)	3	15	63	0
Data 1 (Background)	7	15	1023	0
Data 2 (Video)	1	7	15	3008
Data 3 (Voice)	1	3	7	1504

Station EDCA parameters

Queue	AIFS	cwMin	cwMax	TXOP Limit
Data 0 (Best Effort)	3	15	1023	0
Data 1 (Background)	7	15	1023	0
Data 2 (Video)	2	7	15	3008
Data 3 (Voice)	2	3	7	1504

Figure 65.

2. Optional: To configure advanced QoS for the 802.11a/na modes, click the **802.11a/na** tab.
3. Specify the settings as explained in the following table:

Table 32. EDCA settings

Setting	Description
AP EDCA parameters	
AIFS	Enter the Arbitration Inter-Frame Spacing (AIFS) interval that specifies the wait time (in milliseconds) between data frames. A higher AIFS value means a higher priority for a queue. Valid values for AIFS are 0 through 8. The default values are Data 0: 3; Data 1: 7; Data 2: 1; Data 3: 1.
cwMin	Enter the minimum contention window (cwMin) value that specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for cwMin needs to be lower than the value for cwMax. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. The default values are Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.
cwMax	Enter the maximum contention window (cwMax) value that specifies the upper limit (in milliseconds) for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for cwMax needs to be higher than the value for cwMin. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. The default values are Data 0: 63; Data 1: 1023; Data 2: 15; Data 3: 7.

Table 32. EDCA settings (continued)

Setting	Description
Max. Burst	Enter the maximum burst value that specifies the maximum burst length (in microseconds) allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Decreasing this value increases the priority of the queue. Valid values for maximum burst length are all multiples of 32 between 0 and 8192, inclusive of 0 and 8192. The default values are Data 0: 0; Data 1: 0; Data 2: 3008; Data 3: 1504.
Station EDCA parameters	
AIFS	Enter the Arbitration Inter-Frame Spacing (AIFS) interval that specifies the wait time (in milliseconds) between data frames. A higher AIFS value means a higher priority for a queue. Valid values for AIFS are 0 through 8. The default values are Data 0: 3; Data 1: 7; Data 2: 2; Data 3: 2.
cwMin	Enter the minimum contention window (cwMin) value that specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for cwMin needs to be lower than the value for cwMax. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. The default values are Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.
cwMax	Enter the maximum contention window (cwMax) value that specifies the upper limit (in milliseconds) for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for cwMax needs to be higher than the value for cwMin. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. The default values are Data 0: 1023; Data 1: 1023; Data 2: 15; Data 3: 7.
TXOP Limit	Enter the transmission opportunity (TXOP) value that specifies the time interval (in microseconds) in which a client station can initiate transmissions on the wireless medium (WM). Decreasing this value increases the priority of the queue. Valid values for TXOP Limit are all multiples of 32 between 0 and 8192, inclusive of 0 and 8192. The default values are Data 0: 0; Data 1: 0; Data 2: 3008; Data 3: 1504.

4. Click **Apply** to save your settings.

Configure Quality of Service Policies

The wireless access point lets you configure and apply QoS policies to wireless clients. In each QoS policy, you can specify multiple classifications (match clauses) and apply traffic to eight priority queues based on the following information in the Layer 2, Layer 3, Layer 3 IP headers, and Layer 4:

- IP precedence. Indicates the IP Type of Service (ToS) or precedence in the IP headers.
- IP DSCP. Indicates the Differentiated Services Code Point (DSCP) marking in the IP header.
- IP protocol 119. Indicates the IP protocol field in the IP header with value 119.
- 802.1P. Indicates the 3-bit Class of Service (CoS) field in the class header.
- IP protocol. Indicates the protocol field in the IP header.

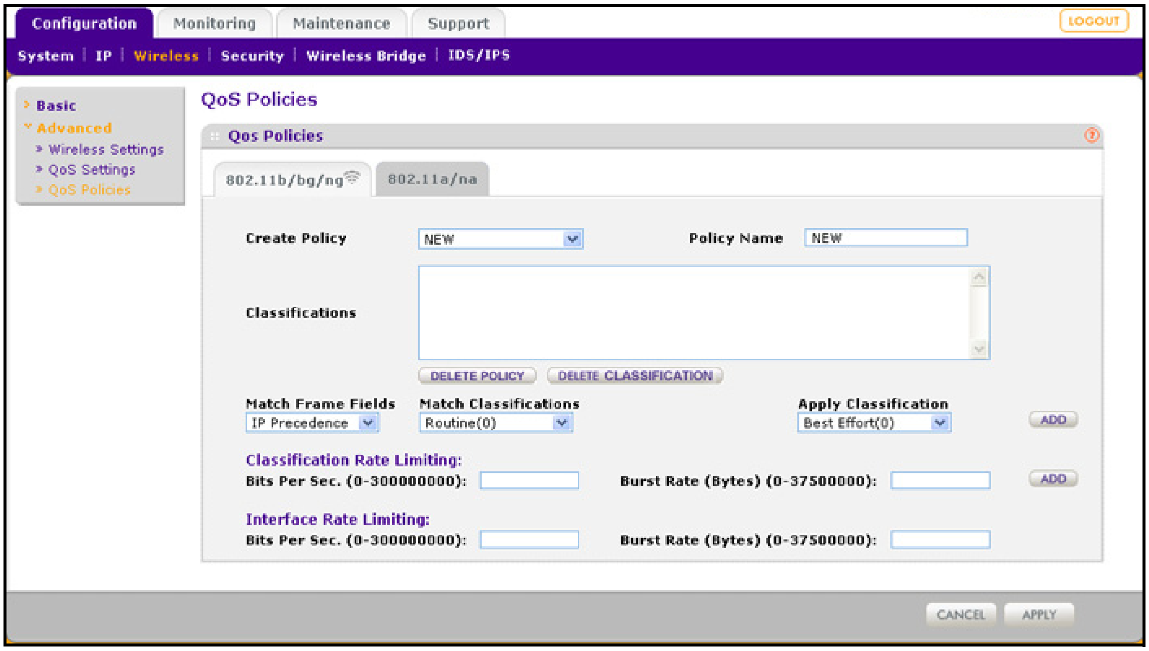
- EtherType. Indicates the EtherType field in Ethernet-II frame header.
- Source MAC. Indicates the source MAC address in Ethernet-II frame header.
- Destination MAC. Indicates the destination MAC address in Ethernet-II frame header.
- Source IP. Indicates the source IP address in the IP header.
- Destination IP. Indicates the destination IP address in the IP header.
- Source port. Indicates the source port number in the port header.
- Destination port. Indicates the destination port number in the port header.

For each classification in a QoS policy, you can configure rate limiting by specifying the maximum bit rate and maximum burst rate. Packets that exceed the maximum bit rate are retained in the traffic queue and are processed when transmission falls below the maximum bit rate again. You can also configure the overall maximum bit rate and maximum burst rate for the entire wireless interface.

You can configure up to eight QoS policies.

➢ To configure a new QoS policy:

1. Select **Configuration > Wireless > Advanced > QoS Policies**. The advanced QoS Policies screen displays:



Create Policy: NEW
Policy Name: NEW
Classifications:
Match Frame Fields: IP Precedence
Match Classifications: Routine(0)
Apply Classification: Best Effort(0)

Classification Rate Limiting:
Bits Per Sec. (0-300000000):
Burst Rate (Bytes) (0-37500000):

Interface Rate Limiting:
Bits Per Sec. (0-300000000):
Burst Rate (Bytes) (0-37500000):

Figure 66.

2. Optional: To configure the QoS Policies screen for the 802.11a/na modes, click the **802.11a/na** tab.
3. From the Create Policy drop-down list, select **NEW**. If you have not created any QoS policies, NEW is the only selection possible.
4. In the Policy Name field, enter a name for the new QoS policy.
5. Specify a classification for the QoS policy as explained in the following table.

Note: *Depending on your selection from the Match Frame Fields drop-down list, Match Classifications appears either as a drop-down list from which you need to make a selection or a field in which you need to enter information.*

Table 33. QoS classification settings

Setting	Description	
Match Frame Fields and Match Classifications	IP DCSP	From the Match Classifications drop-down list, select the DSCP traffic class against which the information in the IP header needs to be matched: • **Routine(0)** • **Priority(1)** • **Immediate(2)** • **Flash(3)** • **Flash Override(4)** • **Critic/CCP(5)** • **Inter Control(6)** • **Network Control(7)**
	IP Precedence	From the Match Classifications drop-down list, select the DSCP marking against which the information in the IP header needs to be matched: • **Best Effort** • **Assured Forwarding - Class 1 Low** • **Assured Forwarding - Class 1 Medium** • **Assured Forwarding - Class 1 High** • **Assured Forwarding - Class 2 Low** • **Assured Forwarding - Class 2 Medium** • **Assured Forwarding - Class 2 High** • **Assured Forwarding - Class 3 Low** • **Assured Forwarding - Class 3 Medium** • **Assured Forwarding - Class 3 High** • **Assured Forwarding - Class 4 Low** • **Assured Forwarding - Class 4 Medium** • **Assured Forwarding - Class 4 High** • **Class Selector 1** • **Class Selector 2** • **Class Selector 3** • **Class Selector 4** • **Class Selector 5** • **Class Selector 6** • **Class Selector 7** • **Expedited Forwarding**
	IP Protocol119	Traffic is matched against value 119 in the IP protocol field in the IP header.

Table 33. QoS classification settings (continued)

Setting	Description	
Match Frame Fields and Match Classifications (continued)	802.1P	From the Match Classifications drop-down list, select the CoS priority value against which the information in the IP header needs to be matched: • **Routine(0)** • **Priority(1)** • **Immediate(2)** • **Flash(3)** • **Flash Override(4)** • **Critic/CCP(5)** • **Inter Control(6)** • **Network Control(7)**
	IP Protocol	In the Match Classifications field, enter the IP protocol value against which the information in the IP header needs to be matched. A list of protocol values is available at *http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml*.
	Ether Type	In the Match Classifications field, enter the Ether type value against which the information in the IP header needs to be matched. A list of Ether type values is available at *http://standards.ieee.org/develop/regauth/ethertype/eth.txt*.
	Source MAC	In the Match Classifications field, select or enter the source MAC address against which the information in the IP header needs to be matched. To select the MAC address of a wireless client that is connected to the wireless access point: 1. Select the radio button to the left of the Match Classifications drop-down list. 2. From the drop-down list, select a MAC address. To enter a MAC address: 1. Select the radio button to the right of the Match Classifications drop-down list. 2. In the field to the right of the radio button, enter a MAC address.
	Destination MAC	In the Match Classifications field, select or enter the destination MAC address against which the information in the IP header needs to be matched. To select the MAC address of a wireless client that is connected to the wireless access point: 1. Select the radio button to the left of the Match Classifications drop-down list. 2. From the drop-down list, select a MAC address. To enter a MAC address: 1. Select the radio button to the right of the Match Classifications drop-down list. 2. In the field to the right of the radio button, enter a MAC address.

Table 33. QoS classification settings (continued)

Setting	Description	
Match Frame Fields and Match Classifications (continued)	Source IP	In the Match Classifications field, enter the source IP address against which the information in the IP header needs to be matched.
	Destination IP	In the Match Classifications field, enter the destination IP address against which the information in the IP header needs to be matched.
	Source Port	The Match Classifications field is separated into two sections. In the left section, enter the source port number, and optionally, in the right section, enter the associated IP address against which the information in the IP header needs to be matched.
	Destination Port	The Match Classifications field is separated into two sections. In the left section, enter the destination port number, and optionally, in the right section, enter the associated IP address against which the information in the IP header needs to be matched.
Apply Classification	From the Apply Classification drop-down list, select the traffic class that needs to be applied to the packets that match the selection in the Match Classifications field: • **Best Effort(0)** • **Background(1)** • **Spare(2)** • **Excellent(3)** • **Control Load(4)** • **Video < 100 ms Latency(5)** • **Voice < 10 ms Latency(6)** • **Network Control(7)**	

6. Optional: Specify rate limiting for the classification as explained in the following table:

Table 34. Classification rate limiting settings

Setting	Description	
Classification Rate Limiting	Bits Per Sec.	Enter a value between 0 and 300,000,000 bps to specify the maximum data rate up to which packets that match the classification are queued for transmission and sent immediately over the wireless interface. This value applies only to traffic that matches the classification. **Note:** When the maximum rate is exceeded, packets are retained in the queue and sent when the transmission falls below the maximum rate again.
	Burst Rate (Bytes)	Enter a value between 0 and 37,500,000 bytes to specify the maximum amount of data that can be transmitted in a burst for packets that match the classification. This value applies only to traffic that matches the classification.

7. Click **Add** to add the classification to the Classifications field.
8. To add another classification to the QoS policy, repeat *Step 5*, *Step 6*, and *Step 7*.
9. Click **Apply** to save your settings. The QoS policy is saved.

Note: Rate limiting for the wireless interface is an optional setting that applies to all traffic on the wireless interface. Unlike classification rate limiting, which you can specify for each classification, rate limiting for the wireless interface needs to be specified only once.

➢ To specify rate limiting for the wireless interface:

1. Specify rate limiting for the entire wireless interface as explained in the following table:

Table 35. Wireless interface rate limiting settings

Setting	Description	
Interface Rate Limiting	Bits Per Sec.	Enter a value between 0 and 300,000,000 bps to specify the maximum data rate up to which packets are queued for transmission and sent immediately over the wireless interface. This value applies to all traffic on the wireless interface. **Note:** When the maximum rate is exceeded, packets are retained in the queue and sent when the transmission falls below the maximum rate again.
	Burst Rate (Bytes)	Enter a value between 0 and 37,500,000 bytes to specify the maximum amount of data that can be transmitted in a burst over the wireless interface. This value applies to all traffic on the wireless interface.

2. Click **Apply** to save your settings.

➢ To modify a QoS policy:

1. From the Create Policy drop-down list, select the policy that you want to modify.
2. To delete a classification, select it in the Classification field, and click **Delete Classification**.
3. To add a classification, follow *Step 5* through *Step 7* in the procedure to configure a new QoS policy. You can also change the name of the policy.
4. Click **Apply** to save your settings.

➢ To delete a QoS policy:

1. From the Create Policy drop-down list, select the policy that you want to delete.
2. Click **Delete Policy**.
3. Click **Apply** to save your settings.

Configure Wireless Bridging

The wireless access point supports a wireless distributing system (WDS) that lets you build large bridged wireless networks. You can select from the following wireless access point modes:

- **Wireless point-to-point bridge**. In this mode, the wireless access point can communicate with another bridge-mode wireless station and, as an option, also with wireless clients. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see *Configure a Point-to-Point Wireless Network* on page 118.
- **Wireless point-to-multipoint bridge**. In this mode, the wireless access point is the master for a group of bridge-mode wireless stations. As an option, the wireless access point can also communicate with wireless clients. You can configure up to four profiles.

  The other bridge-mode wireless stations need to be set to point-to-point bridge mode, using the MAC address of the master wireless access point. Rather than communicating directly with each other, all other bridge-mode wireless stations send their traffic to the master wireless access point. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see *Configure a Point-to-Multipoint Wireless Network* on page 122.
- **Repeating the wireless signal**. In this mode, this wireless access point repeats the wireless signal, does not support communication with wireless clients, and sends all traffic to a remote access point. In this mode, wireless clients cannot associate with the wireless access point. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see *Configure the Wireless Access Point to Repeat the Wireless Signal Using Point-to-Multipoint Bridge Mode* on page 126.

Note: You cannot configure wireless bridging when automatic channel selection is enabled. On the basic Wireless Settings screen, make sure that Auto is not selected from the Channel / Frequency drop-down list (see *Configure the Basic Wireless Settings* on page 28).

Configure a Point-to-Point Wireless Network

In point-to-point bridge mode, the wireless access point communicates with another bridge-mode wireless station. Use wireless security to protect this communication. The following figure shows an example in which two wireless access points (APs) function in point-to-point bridge mode:

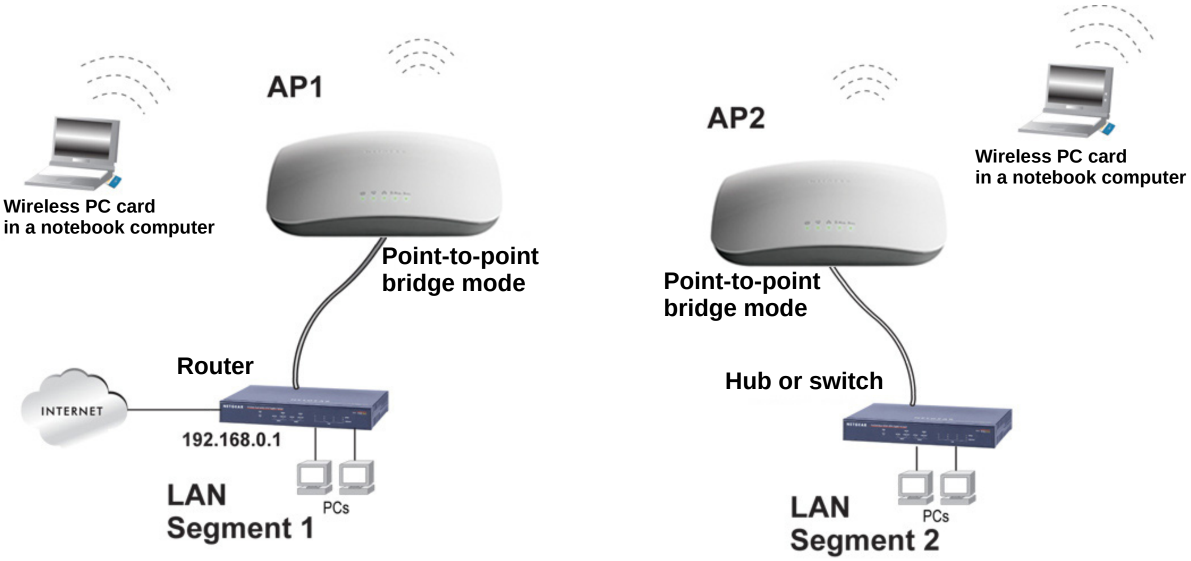
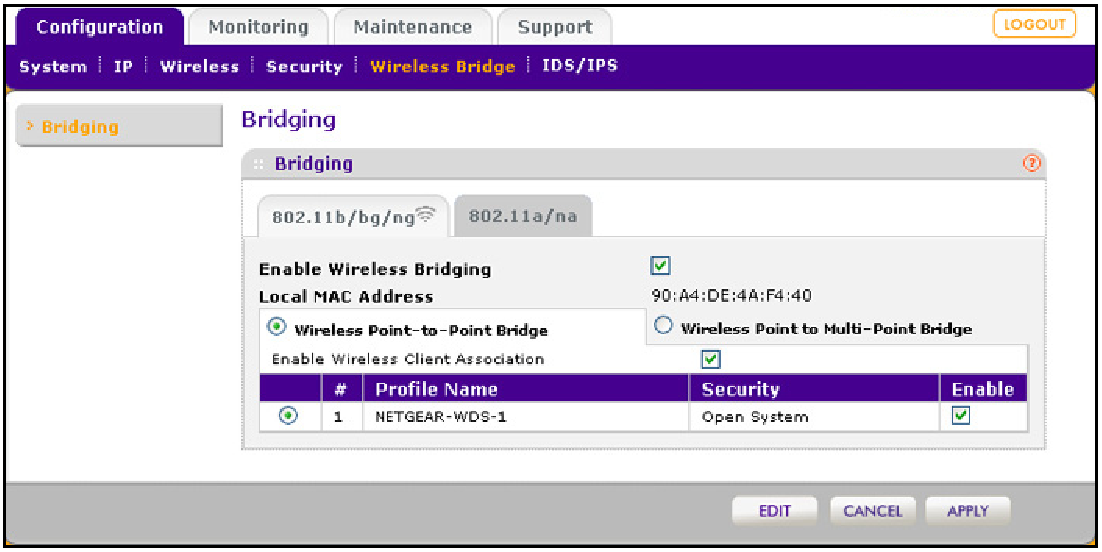

AP1
Wireless PC card in a notebook computer
Point-to-point bridge mode
Router
INTERNET
192.168.0.1
LAN Segment 1
PCs
AP2
Wireless PC card in a notebook computer
Point-to-point bridge mode
Hub or switch
LAN Segment 2
PCs

Figure 67.

➢ To configure a point-to-point wireless network:

1. Configure the wireless access point (AP1 on LAN Segment 1 in the previous figure) as a point-to-point bridge:
   - a. Select **Configuration > Wireless Bridge**. The Bridging screen displays (see the following figure).
   - b. Optional: To display the Bridging screen for the 802.11a/na modes, click the **802.11a/na** tab.
   - c. Select the **Enable Wireless Bridging** check box. The Local MAC Address field is a nonconfigurable field that shows the MAC address of the wireless access point.
   - d. Select the **Wireless Point-to-Point Bridge** radio button. The screen adjusts.



Enable Wireless Bridging ☑

Local MAC Address 90:A4:DE:4A:F4:40

● Wireless Point-to-Point Bridge ○ Wireless Point to Multi-Point Bridge

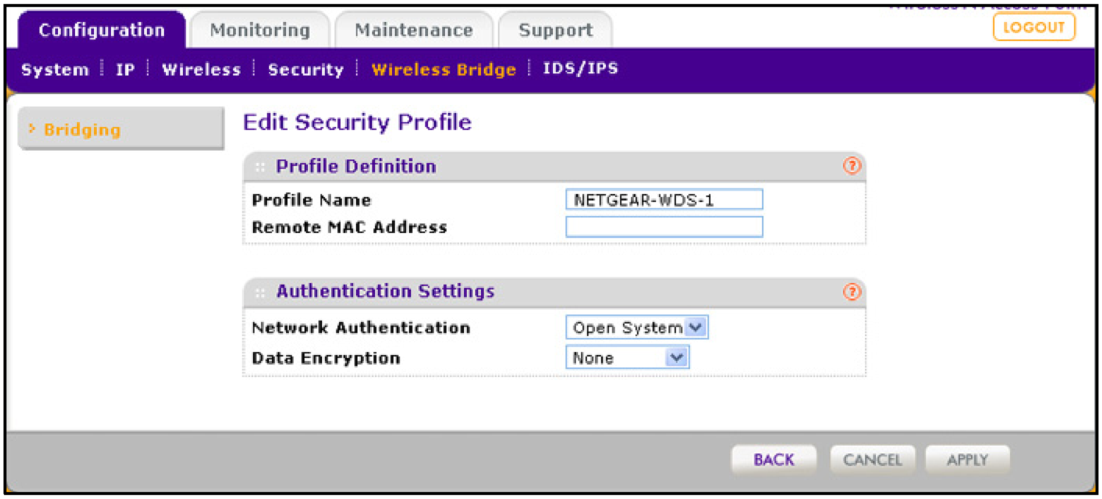
Enable Wireless Client Association ☑

	#	Profile Name	Security	Enable
●	1	NETGEAR-WDS-1	Open System	☑

Figure 68.

e. If you want to enable wireless client association while the wireless access point functions as a point-to-point bridge, select the **Enable Wireless Client Association** check box.

f. Click **Edit** to configure the security profile settings. The Edit Security Profile screen displays:



Edit Security Profile

Profile Definition

Profile Name: NETGEAR-WDS-1

Remote MAC Address:

Authentication Settings

Network Authentication: Open System

Data Encryption: None

Figure 69.

g. Specify the settings as explained in the following table:

Table 36. Point-to-point bridge profile and authentication settings

Setting	Description
Profile Definition	
Profile Name	Enter a profile name that is easy to remember. The default name is NETGEAR-WDS-1.
Remote MAC Address	Enter the MAC address of the remote wireless access point (the MAC address of AP2 on LAN Segment 1 in *Figure 67* on page 119).
Authentication Settings	
Network Authentication and Data Encryption	From the Network Authentication drop-down list, select **Open System**, **WPA-PSK**, or **WPA2-PSK**. Your selection determines the options that the Data Encryption drop-down list provides, and whether the WPA Passphrase (Network Key) field displays.

Table 36. Point-to-point bridge profile and authentication settings (continued)

Setting	Description	
Network Authentication and Data Encryption (continued)	Open System	Although you can use the bridge communication without any authentication and encryption, NETGEAR recommends that you use WEP if you do select an open system. From the Data Encryption drop-down list, select one of the following: • **None**. No authentication and encryption. • **64-bit WEP**. Standard WEP encryption, using 40/64-bit encryption. • **128-bit WEP**. Standard WEP encryption, using 104/128-bit encryption. • **152-bit WEP**. Proprietary WEP encryption mode, using 128+24 bit encryption. This mode functions only with other wireless stations that support this mode.
	WPA-PSK	**TKIP** (Temporal Key Integrity Protocol) is the standard encryption method used with WPA-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive).
	WPA2-PSK	**AES** (Advanced Encryption Standard) is the standard encryption method used with WPA2-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). **Note:** NETGEAR recommends WPA2-PSK authentication with AES encryption if you want to use the 11n rates and speed.

h. Click **Apply** to save your security profile settings. The Bridging screen displays again.

i. If the correct profile name and security option are displayed in the table, select the check box in the Enable column.

j. Click **Apply** on the Bridging screen to save your point-to-point bridge settings.

2. Configure a second wireless access point (AP2) on LAN Segment 2 (see *Figure 67* on page 119) in point-to-point bridge mode.

   AP1 needs to have AP2's MAC address in its Remote MAC Address field, and AP2 needs to have AP1's MAC address in its Remote MAC Address field.

3. Verify the following settings for both wireless access points:
   - Both wireless access points are configured to operate in the same LAN network address range as the LAN devices.
   - Both wireless access points use the same channel, authentication mode, and security settings.

4. Verify connectivity across the LAN 1 and LAN 2.

A computer on either LAN segment should be able to connect to the Internet or share files and printers of any other computers or servers connected to LAN Segment 1 or LAN Segment 2.

Configure a Point-to-Multipoint Wireless Network

In a point-to-multipoint bridge, the wireless access point is the master for a group of bridge-mode wireless access points. All traffic is sent to the master rather than to the other wireless access points. Use wireless security to protect this communication.

For each wireless access point that you want the master to be able to connect to, you need to configure a security profile with a unique name and the MAC address of the wireless access point. You can configure up to four such security profiles (NETGEAR-WDS-1, NETGEAR-WDS-2, and so on).

The following figure shows an example in which AP1 functions in point-to-multipoint bridge mode and AP2 and AP3 function in point-to-point bridge mode:

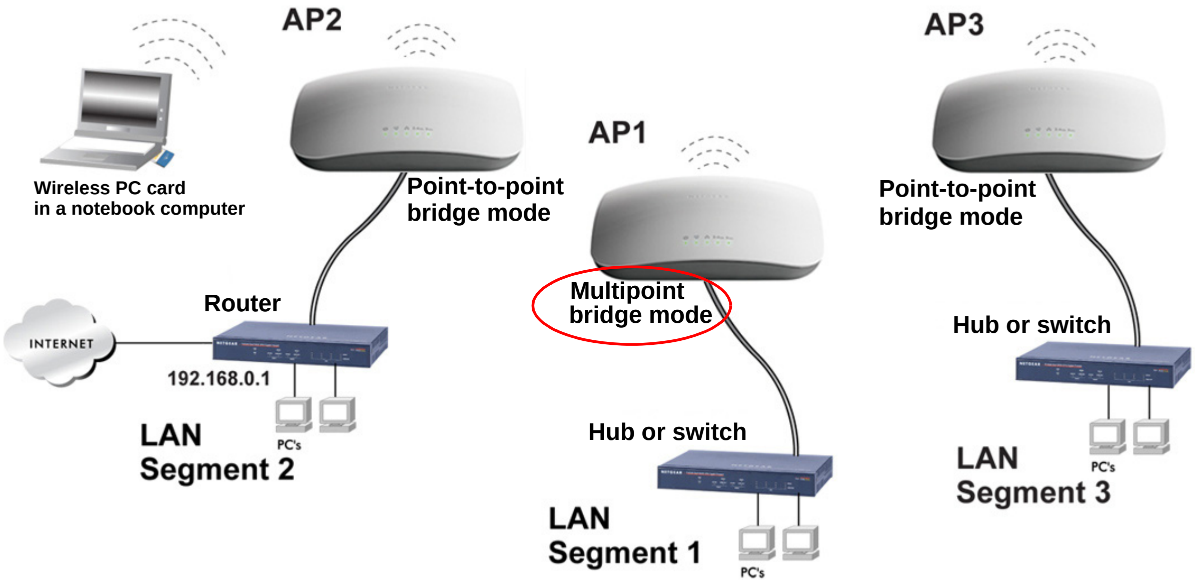
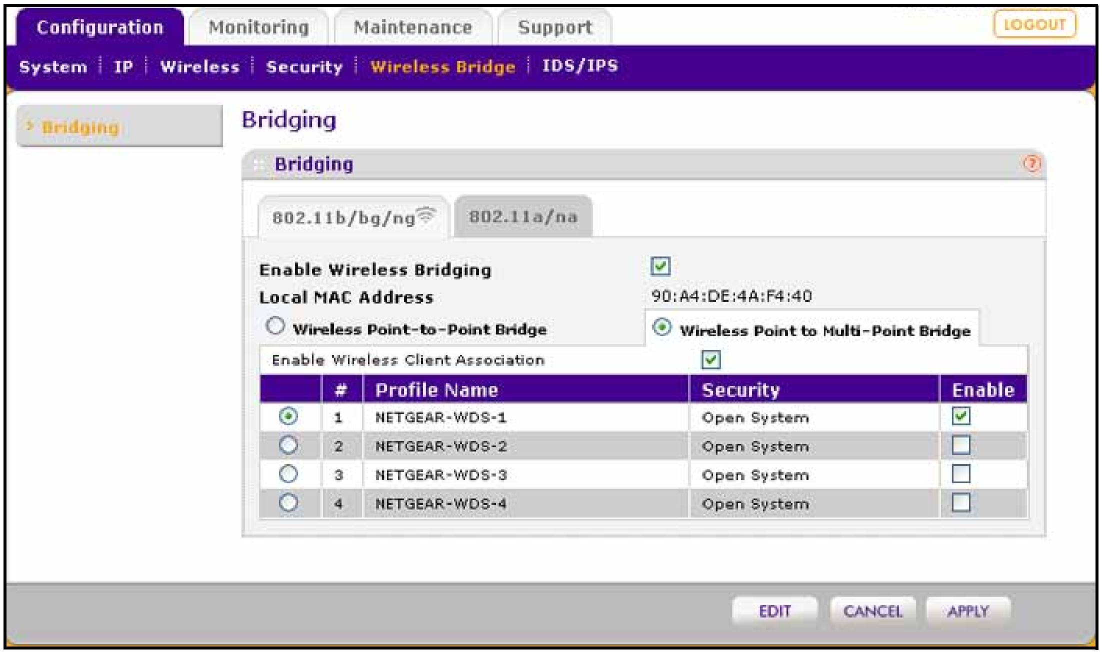


Figure 70.

➤ **To configure a point-to-multipoint wireless network:**

1. Configure the security profiles on the wireless access point (AP1 on LAN Segment 1 in the previous figure):
   a. Select **Configuration > Wireless Bridge**. The Bridging screen displays. (The following figure shows the screen after you have completed *Step d*.)



Bridging

Bridging

Enable Wireless Bridging ☑

Local MAC Address 90:A4:DE:4A:F4:40

○ Wireless Point-to-Point Bridge ● Wireless Point to Multi-Point Bridge

Enable Wireless Client Association ☑

	#	Profile Name	Security	Enable
●	1	NETGEAR-WDS-1	Open System	☑
○	2	NETGEAR-WDS-2	Open System	□
○	3	NETGEAR-WDS-3	Open System	□
○	4	NETGEAR-WDS-4	Open System	□

Figure 71.

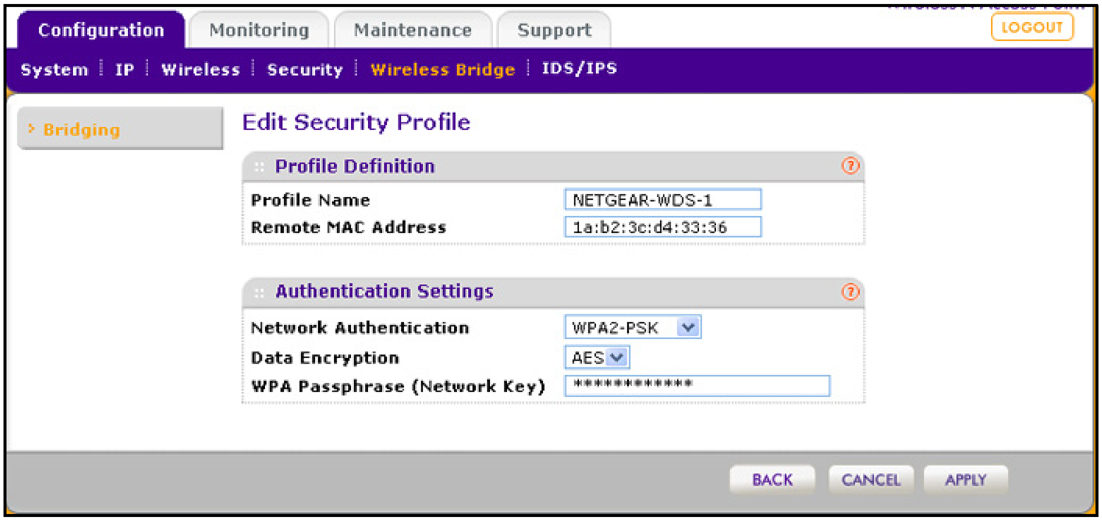
b. Optional: To display the Bridging screen for the 802.11a/na modes, click the **802.11a/na** tab.

c. Select the **Enable Wireless Bridging** check box. The Local MAC Address field is a nonconfigurable field that shows the MAC address of the wireless access point.

d. Select the **Wireless Point-to-Multi-Point Bridge** radio button. The screen adjusts.

e. The profile table shows four security profiles. Choose a security profile to edit by selecting the corresponding radio button to the left of the profile.

f. Click **Edit** to configure the selected security profile settings. The Edit Security Profile screen displays for the selected security profile. (The following figure contains an example.)



Edit Security Profile

Profile Definition

Profile Name: NETGEAR-WDS-1

Remote MAC Address: 1a:b2:3c:d4:33:36

Authentication Settings

Network Authentication: WPA2-PSK

Data Encryption: AES

WPA Passphrase (Network Key): *************

Figure 72.

g. Specify the settings as explained in the following table:

Table 37. Point-to-multipoint bridge profile and authentication settings

Setting	Description	
Profile Definition		
Profile Name	Enter a profile name that is easy to remember. The default names for the four security profiles are NETGEAR-WDS-1, NETGEAR-WDS-2, NETGEAR-WDS-3, and NETGEAR-WDS-4.	
Remote MAC Address	Enter the MAC address of the remote wireless access point (the MAC address of AP2 or AP 3 on LAN Segment 1 in *Figure 70* on page 122).	
Authentication Settings		
Network Authentication and Data Encryption	From the Network Authentication drop-down list, select **Open System**, **WPA-PSK**, or **WPA2-PSK**. Your selection determines the options that the Data Encryption drop-down list provides, and whether the WPA Passphrase (Network Key) field displays.	
	Open System	Although you can use the bridge communication without any authentication and encryption, NETGEAR recommends that you use WEP if you do select an open system. From the Data Encryption drop-down list, select one of the following: • **None**. No authentication and encryption. • **64-bit WEP**. Standard WEP encryption, using 40/64-bit encryption. • **128-bit WEP**. Standard WEP encryption, using 104/128-bit encryption. • **152-bit WEP**. Proprietary WEP encryption mode, using 128+24 bit encryption. This mode functions only with other wireless stations that support this mode.
	WPA-PSK	**TKIP** (Temporal Key Integrity Protocol) is the standard encryption method used with WPA-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive).
	WPA2-PSK	**AES** (Advanced Encryption Standard) is the standard encryption method used with WPA2-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). **Note:** NETGEAR recommends WPA2-PSK authentication with AES encryption if you want to use the 11n rates and speed.

h. Click **Apply** to save your security profile settings. The Bridging screen displays again.

i. Repeat *Step c* through *Step h* for any other security profile that you want to edit.

For example, first configure security profile NETGEAR-WDS-1 with the MAC address of AP2, and then configure security profile NETGEAR-WDS-2 with the MAC address of AP3 (see *Figure 70* on page 122).

2. Activate the wireless access point (AP1 on LAN Segment 1 in *Figure 70* on page 122) as a point-to-multipoint bridge (that is, it is the master in the wireless network):
   - a. On the Bridging screen, select the **Enable Wireless Bridging** check box.
   - b. Select the **Wireless Point-to-Multi-Point Bridge** radio button.
   - c. Select the **Enable Wireless Client Association** check box to enable wireless client association.

Note: If you do not select the Enable Wireless Client Association check box, the wireless access point does not function in point-to-multipoint bridge but in repeater mode.

   - d. If the correct profile names and security options are displayed in the table, select the check boxes in the Enable column for all security profiles that you want to enable.
   - e. Click **Apply** on the Bridging screen to activate your point-to-multipoint bridge settings.
3. Configure AP2 on LAN Segment 2 (see *Figure 70* on page 122) in point-to-point bridge mode with the remote MAC address of AP1.
4. Configure AP3 on LAN Segment 3 (see *Figure 70* on page 122) in point-to-point bridge mode with the remote MAC address of AP1.
5. Verify the following for all wireless access points:
   - Only AP1 on LAN Segment 1 is configured in point-to-multipoint bridge mode, and all others APs are configured in point-to-point bridge mode.
   - AP2 and AP3 (the point-to-point APs) have AP1’s MAC address in their Remote MAC Address field.
   - All APs are on the same LAN, that is, the LAN IP addresses of all APs are in the same network as the LAN devices.
   - If you use DHCP, all wireless access points can obtain IP addresses automatically (as DHCP clients). For more information, see *Configure the Optional DHCPv4 Server* on page 27 or *Configure the Optional DHCPv6 Server* on page 101.
   - All wireless access points use the same channel, authentication mode, and security settings.
6. Verify connectivity across the LANs:

   A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other devices or servers connected to any of the three LAN segments.

Note: You can extend this multipoint bridging configuration by adding additional wireless access points that are configured in point-to-point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Configure the Wireless Access Point to Repeat the Wireless Signal Using Point-to-Multipoint Bridge Mode

You can configure the wireless access point to repeat the wireless signal, without communication with other wireless clients. All traffic is sent to the remote or downstream wireless access point. You can configure up to four security profiles to enable the wireless access point to repeat the wireless signal for four remote wireless access points. Each security profile requires a unique name and needs to include the MAC address of the remote wireless access point. You can configure up to four such security profiles (NETGEAR-WDS-1, NETGEAR-WDS-2, and so on).

The following figure shows an example in which AP1, AP2, and AP3 repeat the wireless signal in point-to-multipoint bridge mode. AP2 requires a security profile for AP1 and another one for AP3:

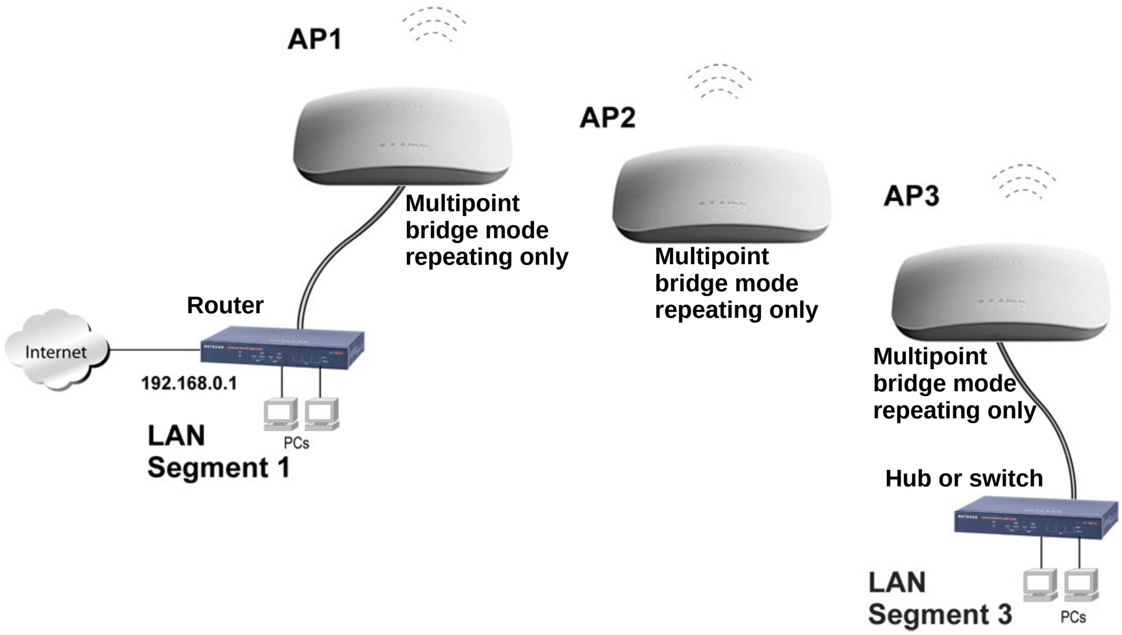

AP1
AP2
AP3
Multipoint bridge mode repeating only
Multipoint bridge mode repeating only
Multipoint bridge mode repeating only
Router
Internet
192.168.0.1
LAN Segment 1
PCs
Hub or switch
LAN Segment 3
PCs

Figure 73.

➤ **To configure the wireless access point to repeat the wireless signal:**

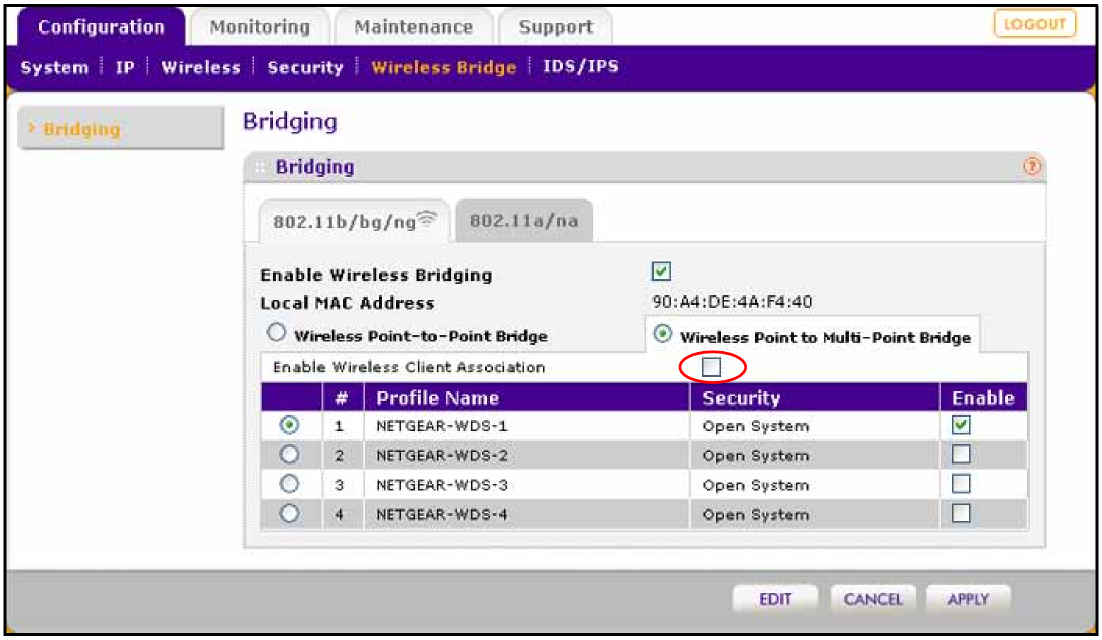
1. Configure the security profiles on the wireless access point (AP2 in the previous figure):

   a. Select **Configuration > Wireless Bridge**. The Bridging screen displays (see the following figure).

   b. Optional: To display the Bridging screen for the 802.11a/na modes, click the **802.11a/na** tab.

   c. Select the **Enable Wireless Bridging** check box. The Local MAC Address field is a nonconfigurable field that shows the MAC address of the wireless access point.

   d. Select the **Wireless Point-to-Multi-Point Bridge** radio button. The screen adjusts.



Enable Wireless Bridging ☑

Local MAC Address 90:A4:DE:4A:F4:40

○ Wireless Point-to-Point Bridge ● Wireless Point to Multi-Point Bridge

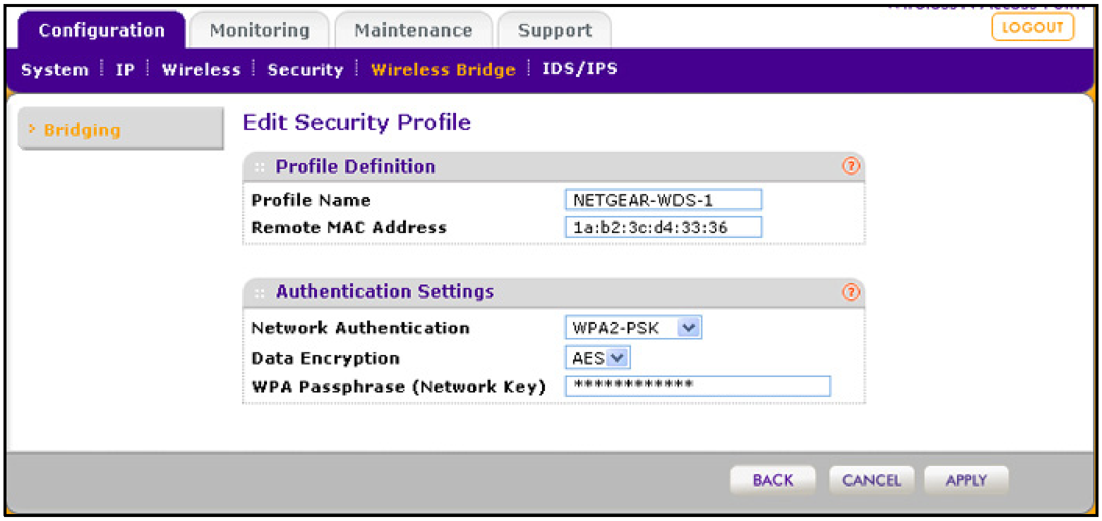
Enable Wireless Client Association □

	#	Profile Name	Security	Enable
●	1	NETGEAR-WDS-1	Open System	☑
○	2	NETGEAR-WDS-2	Open System	□
○	3	NETGEAR-WDS-3	Open System	□
○	4	NETGEAR-WDS-4	Open System	□

Figure 74.

   e. The profile table shows four security profiles. Choose a security profile to edit by selecting the corresponding radio button to the left of the profile.

   f. Click **Edit** to configure the selected security profile settings. The Edit Security Profile screen displays for the selected security profile. (The following figure contains an example.)



Edit Security Profile

Profile Definition

Profile Name: NETGEAR-WDS-1

Remote MAC Address: 1a:b2:3c:d4:33:36

Authentication Settings

Network Authentication: WPA2-PSK

Data Encryption: AES

WPA Passphrase (Network Key): ************

Figure 75.

g. Specify the settings as explained in the following table:

Table 38. Wireless signal repeating profile and authentication settings

Setting	Description	
Profile Definition		
Profile Name	Enter a profile name that is easy to remember. The default names for the four security profiles are NETGEAR-WDS-1, NETGEAR-WDS-2, NETGEAR-WDS-3, and NETGEAR-WDS-4.	
Remote MAC Address	Enter the MAC address of the remote wireless access point (the MAC address of AP1 or AP3 in *Figure 73* on page 126).	
Authentication Settings		
Network Authentication and Data Encryption	From the Network Authentication drop-down list, select **Open System**, **WPA-PSK**, or **WPA2-PSK**. Your selection determines the options that the Data Encryption drop-down list provides, and whether the WPA Passphrase (Network Key) field displays.	
	Open System	Although you can use the bridge communication without any authentication and encryption, NETGEAR recommends that you use WEP if you do select an open system. From the Data Encryption drop-down list, select one of the following: • **None**. No authentication and encryption. • **64-bit WEP**. Standard WEP encryption, using 40/64-bit encryption. • **128-bit WEP**. Standard WEP encryption, using 104/128-bit encryption. • **152-bit WEP**. Proprietary WEP encryption mode, using 128+24 bit encryption. This mode functions only with other wireless stations that support this mode.

Table 38. Wireless signal repeating profile and authentication settings (continued)

Setting	Description	
Network Authentication and Data Encryption (continued)	WPA-PSK	**TKIP** (Temporal Key Integrity Protocol) is the standard encryption method used with WPA-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive).
	WPA2-PSK	**AES** (Advanced Encryption Standard) is the standard encryption method used with WPA2-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). **Note:** NETGEAR recommends WPA2-PSK authentication with AES encryption if you want to use the 11n rates and speed.

h. Click **Apply** to save your security profile settings. The Bridging screen displays again.

i. Repeat *Step e* through *Step h* for any other security profile that you want to edit.

For example, first configure security profile NETGEAR-WDS-1 with the MAC address of AP1, and then configure security profile NETGEAR-WDS-2 with the MAC address of AP3 (see *Figure 73* on page 126).

2. Activate repeater mode on the wireless access point (AP2 in *Figure 73* on page 126):

   a. On the Bridging screen, select the **Enable Wireless Bridging** check box.

   b. Select the **Wireless Point-to-Multi-Point Bridge** radio button.

   c. Clear the **Enable Wireless Client Association** check box to disable wireless client association (see the red circle in *Figure 74* on page 127).

Note: If you do not clear the Enable Wireless Client Association check box, the wireless access point functions in regular point-to-multipoint bridge mode.

   d. If the correct profile names and security options are displayed in the table, select the check boxes in the Enable column for all security profiles that you want to enable.

   e. Click **Apply** on the Bridging screen to activate your repeater settings.

3. Configure AP1 on LAN Segment 1 (see *Figure 73* on page 126) in repeater mode with the remote MAC address of AP2.

4. Configure AP3 on LAN Segment 3 (see *Figure 73* on page 126) in repeater mode with the remote MAC address of AP2.

5. Verify the following for all wireless access points:
    - All APs are on the same LAN, that is, the LAN IP addresses of all APs are in the same network as the LAN devices.
    - If you use DHCP, all wireless access points can obtain IP addresses automatically (as DHCP clients). For more information, see *Configure the Optional DHCPv4 Server* on page 27 or *Configure the Optional DHCPv6 Server* on page 101.
    - All wireless access points use the same channel, authentication mode, and security settings.
6. Verify connectivity across the LANs:

    A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other devices or servers connected to any of the two LAN segments.

Note: You can extend repetition of the wireless signal by adding up to two more wireless access points that are configured in point-to-multipoint bridge mode without client association. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

6. Troubleshooting

6

This chapter provides information about troubleshooting the wireless access point. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the wireless access point on?

  Go to *Basic Functioning* on page 132.

- Have I connected the wireless access point correctly?

  Go to *Basic Functioning* on page 132.

- I cannot access the Internet or the LAN.

  Go to *You Cannot Access the Internet or the LAN from a Wireless-Capable Computer* on page 134.

- I cannot access the wireless access point from a browser.

  Go to *You Cannot Configure the Wireless Access Point from a Browser* on page 134.

- A time-out occurs.

  Go to *When You Enter a URL or IP Address a Time-Out Error Occurs* on page 135.

- I have problems with the LAN connection.

  Go to *Troubleshoot a TCP/IP Network Using the Ping Utility* on page 135.

- I cannot remember the wireless access point’s configuration password.

  Go to *Change the Administrator Password* on page 74.

- I want to clear the configuration and start over again.

  Go to *Restore the Wireless Access Point to the Factory Default Settings* on page 71.

- The date or time is not correct.

  Go to *Problems with Date and Time* on page 137.

The wireless access point provides a packet capture tool that enables you to perform problem diagnoses. For information about how to use this tool, see *Use the Packet Capture Tool* on page 138.

Basic Functioning

- *Verify the Correct Sequence of Events at Startup*
- *No LEDs Are Lit on the Wireless Access Point*
- *The Active LED or the LAN LED Is Not Lit*
- *The WLAN LED Does Not Light Up*

Note: For descriptions of the LEDs, see *Top Panel* on page 11.

Verify the Correct Sequence of Events at Startup

➢ **After you turn on power to the wireless access point, check that the following sequence of events occurs:**

- The Power/Test LED is first steady amber, then goes off, and then blinks green before turning steady green after about 45 seconds.
- The Active LED is lit or blinks green when there is Ethernet traffic.
- The LAN LED indicates the LAN speed: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps.
- The WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready.

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

No LEDs Are Lit on the Wireless Access Point

It takes a few seconds for the Power LED to light up. Wait a minute and check the Power LED status on the wireless access point. If the wireless access point has no power:

➢ **If you use a PoE switch to provide power to the wireless access point, check these items:**

- Make sure that the Ethernet cable between the wireless access point and the PoE switch is correctly connected at both ends.
- Make sure that the power cord of the PoE switch is plugged into a working power outlet or power strip.
- Make sure that your PoE switch is functioning normally.

➢ **If you use a power cord to provide power to the wireless access point, check these items:**

- Make sure that the power cord is connected to the wireless access point.
- Make sure that the power adapter is connected to a functioning power outlet. If it is in a power strip, make sure that the power strip is turned on. If it is plugged directly into the wall, verify that it is not a switched outlet.
- Make sure that you are using the correct NETGEAR power adapter that is supplied with your wireless access point.

The Active LED or the LAN LED Is Not Lit

There is a hardware connection problem.

➢ **Check these items:**

- Make sure that the cable connectors are securely plugged in at the wireless access point and the network device—hub, (PoE) switch, or router.
- Make sure that the connected device is turned on.
- Make sure that the correct cable is used. Use a standard Category 5 Ethernet patch cable. If the network device has Auto Uplink (MDI/MDIX) ports, you can use either a crossover cable or a normal patch cable.

The WLAN LED Does Not Light Up

The wireless access point’s antenna is not working.

➢ **Check these items:**

- If the WLAN LED remains off, either disconnect the cable to the PoE switch and then reconnect it again, or disconnect the adapter from its power source and then plug it in again.
- Make sure that optional external antennas are tightly connected to the wireless access point.

Contact NETGEAR technical support if the WLAN LED remains off.

You Cannot Access the Internet or the LAN from a Wireless-Capable Computer

There is a configuration problem.

➤ **Check these items:**

- You might not have restarted the computer with the wireless adapter to allow TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter might not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up correctly for that network. In Windows, the usual setting for Network Properties is to obtain an IP address automatically.
- The wireless access point's default values might not work with your network. Check the wireless access point's default configuration against the configuration of other devices in your network.
- Make sure that the SSID, network authentication, and data encryption settings of the computer with the wireless adapter are the same as those of the wireless access point.
- Ping the IP address of the wireless access point to verify that there is a wireless connection between the computer with the wireless adapter and the wireless access point. If the ping fails, check the network configuration (for the wireless access point, see *Configure the IPv4 Settings* on page 25).
- Ping the default gateway to verify that there is a path from the computer with the wireless adapter to the default gateway. If the ping fails, check the network configuration or call the Internet service provider (ISP).

You Cannot Configure the Wireless Access Point from a Browser

➤ **Check these items:**

- The wireless access point is correctly installed, it is powered on, and LAN connections are okay. Check that the Active LED and LAN LED are on to verify that the Ethernet connection is okay.
- If your computer uses a fixed (static) IP address, ensure that it is using an IP address in the range of the wireless access point. The wireless access point's default IP address is 192.168.0.100, and its subnet mask is 255.255.255.0 with DHCP disabled. Make sure that your network configuration settings are correct.
- If you are using the NetBIOS name of the wireless access point to connect, ensure that your computer and the wireless access point are on the same network segment or that there is a WINS server on your network.
- If your computer is set to obtain an IP address automatically (DHCP client), restart it.

- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser, clearing the cache, deleting the cookies, and launching the browser again.
- Make sure that 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 wireless access point does not save changes you have made in the web management interface, check the following:**

- When entering configuration settings, be sure to click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

When You Enter a URL or IP Address a Time-Out Error Occurs

A number of things could be causing this.

➢ **Try the following troubleshooting steps:**

- Check whether other computers on the LAN work correctly. If they do, ensure that your computer’s TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses of the wireless access point (see *Configure the IPv4 Settings* on page 25).
- If the computer is configured correctly but still not working, ensure that the wireless access point is connected and turned on. Access it and check its settings. If you cannot connect to the wireless access point, check the LAN and power connections.
- If the wireless access point is configured correctly, check your Internet connection (for example, your cable modem) to make sure that it is working correctly.

Troubleshoot a TCP/IP Network Using the Ping Utility

- *Test the LAN Path to Your Wireless Access Point*
- *Test the Path from Your Computer to a Remote Device*

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. You can easily troubleshoot a TCP/IP network by using the ping utility in your computer.

Test the LAN Path to Your Wireless Access Point

You can ping the wireless access point from your computer to verify that the LAN path to your wireless access point is set up correctly.

➢ **To ping the wireless access point from a computer running Windows 95 or later:**

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the field provided, type **`ping`** followed by the IP address of the wireless access point, as in this example:

   ```
   ping 192.168.0.100
   ```

3. Click **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 that the Active LED and LAN LED are on. If one or both of these LEDs are off, follow the instructions in *The Active LED or the LAN LED Is Not Lit* on page 133.
     - 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 wireless access point.
   - Wrong network configuration:
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
     - Verify that the IP address for your wireless access point and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After verifying that the LAN path works correctly, test the path from your computer to a remote device.

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the Windows Run window, type:

   ping -n 10 *<IP address>*

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

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

- Check that your computer has the IP address of your router listed as the default wireless access point. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer’s Network Control Panel. Verify that the IP address of the router is listed as the default wireless access point.
- Check to see that the network address of your computer (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 computer, enter that host name as the account name in the basis General system settings screen (see *Configure Basic General System Settings and Time Settings* on page 23).

Problems with Date and Time

The Time Settings screen that is accessible through the Configuration > System > Basic > Time menu choices displays the current date and time of day. The wireless access point uses the Network Time Protocol (NTP) to obtain the current time from a network time server on the Internet that you specify in the Time Settings screen (see *Configure Basic General System Settings and Time Settings* on page 23). Each entry on the Logs screen is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date and time shown is Fri Dec 31 00:00:00 1999 or a similar incorrect date and time. Cause: The wireless access point has not yet successfully reached the network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the wireless access point, wait at least 5 minutes and check the date and time again.
- The day is correct or one day ahead or behind, and the hours are ahead or behind. Cause: You have selected an incorrect time zone for your area. Specify the correct time zone in the basic General system settings screen (see *Configure Basic General System Settings and Time Settings* on page 23).

Use the Packet Capture Tool

You can capture wireless packets to analyze traffic patterns with a network traffic analyzer tool. The captured packet flow can show if traffic is flowing correctly to its destinations or if packets are dropped. There is a limit to the size of the packet flow that you can capture in a file.

➤ **To capture packets:**

1. Select **Monitoring > Packet Capture**. The Packet Capture screen displays:

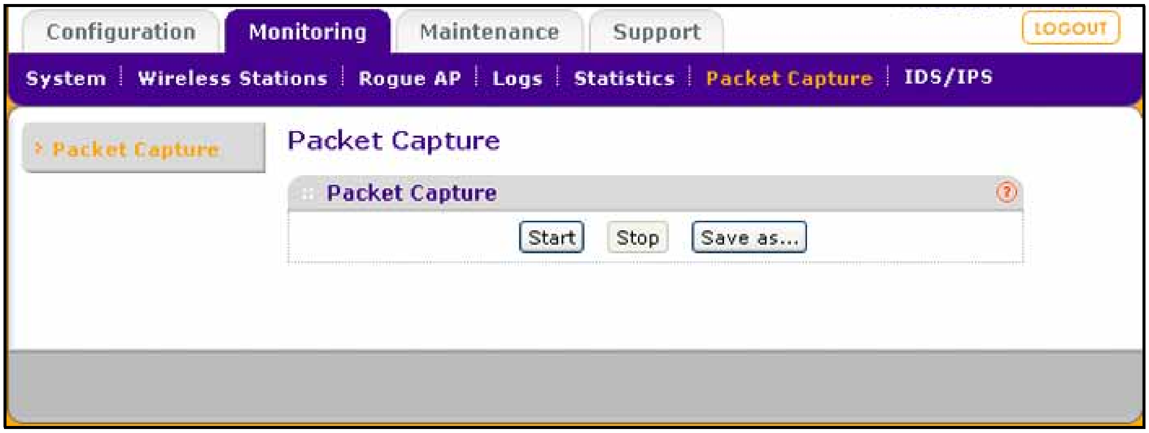


Figure 76.

2. Click **Start** to start capturing wireless packets leaving or entering the wireless access point on the active operating channel. Depending on which interface is enabled, packets on the 2.4 GHz interface or 5 GHz interface are captured. Normal functioning of the wireless access point is not affected during the packet capture process.

   If any previously captured packets exist, you are prompted to delete them, and only then can you capture new packets.

3. Click **Stop** to stop capturing packets.
4. Click **Save as** to save the pacture.pcap file on your computer or to a disk drive.

Supplemental Information

A

This appendix provides factory default settings and technical specifications for the ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620. The appendix includes the following sections:

- *Technical Specifications*
- *Factory Default Settings*

Technical Specifications

Table 39. Technical specifications

Feature	Description
802.11b/bg/ng wireless specifications	
802.11b data rates	1, 2, 5.5, and 11 Mbps, and auto-rate capable
802.11bg data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable
802.11ng MCS index and data rates	Data rates for a 20 MHz channel width and an automatic guard interval: 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps, 16 / 21.7 Mbps, 17 / 43.3 Mbps, 18 / 65 Mbps, 19 / 86.7 Mbps, 20 / 130.7 Mbps, 21 / 173.3 Mbps, 22 / 195 Mbps, 23 / 216.7 Mbps, and auto-rate capable
	Data rates for a 20 MHz channel width and a long guard interval (800 ms): 0 / 6.5 Mbps, 1 / 13 Mbps, 2 / 19.5 Mbps, 3 / 26 Mbps, 4 / 39 Mbps, 5 / 52 Mbps, 6 / 58.5 Mbps, 7 / 65 Mbps, 8 / 13 Mbps, 9 / 26 Mbps, 10 / 39 Mbps, 11 / 52 Mbps, 12 / 78 Mbps, 13 / 104 Mbps, 14 / 117 Mbps, 15 / 130 Mbps, 16 / 19.5 Mbps, 17 / 39 Mbps, 18 / 58.5 Mbps, 19 / 78 Mbps, 20 / 117 Mbps, 21 / 156 Mbps, 22 / 175.5 Mbps, 23 / 195 Mbps, and auto-rate capable
	Data rates for a 40 MHz channel width and an automatic guard interval: 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, 16 / 45 Mbps, 17 / 90 Mbps, 18 / 135 Mbps, 19 / 180 Mbps, 20 / 270 Mbps, 21 / 360 Mbps, 22 / 405 Mbps, 23 / 450 Mbps, and auto-rate capable

Table 39. Technical specifications (continued)

Feature	Description
802.11ng MCS index and data rates (continued)	Data rates for a 40 MHz channel width and a long guard interval (800 ms): 0 / 13.5 Mbps, 1 / 27 Mbps, 2 / 40.5 Mbps, 3 / 54 Mbps, 4 / 81 Mbps, 5 / 108 Mbps, 6 / 121.5 Mbps, 7 / 135 Mbps, 8 / 27 Mbps, 9 / 54 Mbps, 10 / 81 Mbps, 11 / 108 Mbps, 12 / 162 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, 16 / 40.5 Mbps, 17 / 81 Mbps, 18 / 121.5 Mbps, 19 / 162 Mbps, 20 / 243 Mbps, 21 / 324 Mbps, 22 / 364.5 Mbps, 23 / 405 Mbps, and auto-rate capable
802.11b/bg/ng operating frequencies	• 2.412–2.462 GHz (US) • 2.457–2.462 GHz (Spain) • 2.410–2.484 GHz (Japan 11b) • 2.410–2.472 GHz (Japan 11ng) • 2.457–2.472 GHz (France) • 2.412–2.472 GHz (Europe ETSI) • 2.412–2.472 GHz (China)
802.11 b/bg/ng encryption	• 64-bit, 128-bit, and 52-bit WEP • AES • TKIP
802.11a/na wireless specifications	
802.11a data rates	6, 9, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable
802.11na data rates	Data rates for a 20 MHz channel width and an automatic guard interval: 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps, 16 / 21.7 Mbps, 17 / 43.3 Mbps, 18 / 65 Mbps, 19 / 86.7 Mbps, 20 / 130.7 Mbps, 21 / 173.3 Mbps, 22 / 195 Mbps, 23 / 216.7 Mbps, and auto-rate capable
	Data rates for a 20 MHz channel width and a long guard interval (800 ms): 0 / 6.5 Mbps, 1 / 13 Mbps, 2 / 19.5 Mbps, 3 / 26 Mbps, 4 / 39 Mbps, 5 / 52 Mbps, 6 / 58.5 Mbps, 7 / 65 Mbps, 8 / 13 Mbps, 9 / 26 Mbps, 10 / 39 Mbps, 11 / 52 Mbps, 12 / 78 Mbps, 13 / 104 Mbps, 14 / 117 Mbps, 15 / 130 Mbps, 16 / 19.5 Mbps, 17 / 39 Mbps, 18 / 58.5 Mbps, 19 / 78 Mbps, 20 / 117 Mbps, 21 / 156 Mbps, 22 / 175.5 Mbps, 23 / 195 Mbps, and auto-rate capable
	Data rates for a 40 MHz channel width and an automatic guard interval: 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, 16 / 45 Mbps, 17 / 90 Mbps, 18 / 135 Mbps, 19 / 180 Mbps, 20 / 270 Mbps, 21 / 360 Mbps, 22 / 405 Mbps, 23 / 450 Mbps, and auto-rate capable
	Data rates for a 40 MHz channel width and a long guard interval (800 ms): 0 / 13.5 Mbps, 1 / 27 Mbps, 2 / 40.5 Mbps, 3 / 54 Mbps, 4 / 81 Mbps, 5 / 108 Mbps, 6 / 121.5 Mbps, 7 / 135 Mbps, 8 / 27 Mbps, 9 / 54 Mbps, 10 / 81 Mbps, 11 / 108 Mbps, 12 / 162 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, 16 / 40.5 Mbps, 17 / 81 Mbps, 18 / 121.5 Mbps, 19 / 162 Mbps, 20 / 243 Mbps, 21 / 324 Mbps, 22 / 364.5 Mbps, 23 / 405 Mbps, and auto-rate capable

Table 39. Technical specifications (continued)

Feature	Description
802.11a/na operating frequencies	• 5.180–5.240 GHz (US, lower frequencies) • 5.260–5.320 GHz (US, middle frequencies) • 5.180–5240 GHz (CE [EU], lower frequencies) • 5.260–5.320 GHz (CE [EU], middle frequencies) • 5.500–5.680 GHz (CE [EU], upper frequencies)
802.11 a/na encryption	• 64-bit, 128-bit, and 52-bit WEP • AES • TKIP
Management and Other Specifications	
Network management	• Remote configuration and management through the web management interface, through SNMP, or through Telnet or SSH with the command-line interface (CLI). • SNMP management supports SNMP MIB I, MIB II, 802.11 MIB and proprietary configuration MIB.
Maximum clients	Limited by the amount of wireless network traffic generated by each node; a maximum of 128 clients is supported.
Status LEDs	• Power/Test LED • Link speed LED • Ethernet LAN • Wireless LAN (2.4 GHz and 5 GHz)
Electrical and Physical Specifications	
Power adapter	12 VDC, 1A; plug is localized to country of sale
Physical specifications	• Dimensions (h x w x d): 253.75 x 253.75 x 54.76 mm (10.0 x 10.0 x 2.16 in.) • Weight: 1.5 kg (3.31 lb)
Environmental specifications	Operating temperature: 0 to 55°C (32 to 131°F) Operating humidity: 10–9%, noncondensing
Compliance **Note:** For more information about compliance, see *Appendix C, Notification of Compliance*.	
Electromagnetic compliance	• FCC Part 15 SubPart B • FCC Part 15 SubPart C • FCC Part 15 SubPart E • CE • C-TICK

Factory Default Settings

You can use the Reset button located on the rear of the wireless access point to reset all settings to their factory defaults. This is called a hard reset.

To perform a hard reset, use a sharp object to press and hold the **Reset** button for approximately 5 seconds (until the Test LED blinks rapidly). This returns the wireless access point to the factory configuration settings that are shown in the following table.

Note: Pressing the Reset button for a shorter period of time simply causes the wireless access point to reboot.

Table 40. Default configuration settings

Feature		Description
Login for management and configuration		
	LAN IPv4 management address	192.168.0.100
	Subnet mask for IPv4 management address	255.255.255.0
	LAN IPv6 management address	2001::21c:c0ff:fe69
	Prefix length for IPv6 management address	64
	Required static IPv4 address for management computer	192.168.0.210 and 255.255.255.0
	User name (case-sensitive) for login	admin
	Login password (case-sensitive) for login	password
LAN and management features		
	DHCPv4 client	Disabled
	DHCPv6 client	Disabled
	Untagged VLAN	Enabled, VLAN ID 1
	Management VLAN	VLAN ID 1
	SNMP	Disabled
	Syslog	Disabled
	Spanning Tree Protocol (STP)	Disabled
	Link Layer Discovery Protocol (LLDP)	Enabled
	Secure Shell (SSH)	Enabled

Table 40. Default configuration settings (continued)

Feature			Description
	Hotspot		Disabled
	Secure Telnet		Disabled
	Time zone		USA-Pacific
	NTP client		Enabled
	Custom NTP server		Disabled
	Port speed		10/100/1000
	Ethernet MAC address		See bottom label
DHCP server			
	IPv4	DHCPv4 server	Disabled
		DHCPv4 server VLAN ID	1
		DHCPv4 server IP range start address	192.168.0.2
		DHCPv4 server IP range start address	192.168.0.50
		DHCPv4 server subnet mask	255.255.255.0
		DHCPv4 server gateway IPv4 address	192.168.0.1
		DHCPv4 server IP address lease for clients	1 day
	IPv6	DHCPv6 server	Disabled
		DHCPv6 server state	Stateful
		DHCPv6 server VLAN ID	1
		DHCPv6 server IP range start address	2001:05c0:9168::10
		DHCPv6 server IP range start address	2001:05c0:9168::50
		DHCPv6 server prefix length	64
		DHCPv6 server gateway IPv4 address	2001:05c0:9168::1
		DHCPv6 server IP address lease for clients	1 day
Radio and wireless settings			
	Operating mode		Access point, infrastructure mode
	Wireless access point name		netgearxxxxxx, where xxxxxx are the last 6 digits of the wireless access point MAC address
	Country and region		Varies by region
	Wireless communication		2.4 GHz radio enabled 5 GHz radio disabled

Table 40. Default configuration settings (continued)

Feature		Description
	Wireless mode	11ng
	Wireless network name (SSID)	NETGEAR_11ng
	Broadcast network name SSID	Enabled
	802.11ng radio frequency channel	Auto
	MCS index/data rate (transmission speed)	Best **Note:** Maximum wireless signal rate derived from IEEE Standard 802.11 specifications. Actual throughput will vary. Network conditions and environmental factors, including volume of network traffic, building materials and construction, and network overhead, lower actual data throughput rate.
	Channel width	20 MHz
	Guard interval	Auto
	Output power	Full
	Wireless on/off (radio scheduling)	Disabled
	RTS threshold	2347
	Fragmentation length	2346
	Beacon interval	100
	Aggregation length	65535
	AMPDU	Enabled
	RIFS transmission	Disabled
	DTIM interval	3
	Preamble type	Auto
	Antenna	Internal
	802.11d	Enabled
	Client isolation	Disabled
	Maximum wireless clients	128
	Wi-Fi Multimedia (WMM)	Enabled
	WMM powersave	Enabled
	AP EDCA parameters (QoS settings)	See *Table 32* on page 111.
	Station EDCA parameters (QoS settings)	

Table 40. Default configuration settings (continued)

Feature		Description
	QoS policies	None
	Wireless bridging	Disabled
Default wireless profile and profile security		
	Profile name	NETGEAR
	Profile state	Enabled
	Wireless network name (SSID)	NETGEAR_11ng
	Broadcast wireless network name (SSID)	Enabled
	Network authentication	Open system (no authentication)
	Data encryption	None
	Wireless client security separation	Disabled
	VLAN ID	1
Wireless security features		
	Rogue AP detection	Disabled
	Rogue AP detection policy	Moderate
	MAC authentication	Disabled
	RADIUS servers	None
	RADIUS authentication port number	1812
	RADIUS shared secret	sharedsecret
	RADIUS accounting port number	1813
	RADIUS reauthentication time	3600 seconds
	RADIUS update of the global key	1800 seconds
	IDS/IPS	Disabled
	IDS/IPS policies	Preconfigured policies (see *Table 24* on page 89), all disabled
	IDS/IPS detection policy	Moderate
	IDS/IPS mail settings	Blank

Command-Line Reference

B

The wireless access point can be configured through either the command-line interface (CLI), a web browser, or a MIB browser.

The CLI allows viewing and modification of the configuration from a terminal or computer through a Telnet or SSH connection.

```
Keyword                                  Description
------------------------------------------------------------------------------
|-backup-configuration                 --Backup configuration
|
|-config>                              --Configuration setting
| |-apname                             --Access point name
| |-country                            --Country/region
| |
| |-dhcpv4>                            --DHCPv4 server
| | |-dns-server                       --DNS server
| | |-gateway                          --Default gateway
| | |-ip-address                       --IP range
| | |-lease-time                       --Lease time
| | |-status                           --Status
| | |-vlan-id                          --Vlan-id
| | |-subnet-mask                      --Subnet mask
| | |-wins-server                      --WINS server
| |
| |-dhcpv6>                            --DHCPv6 server
| | |-dns-server                       --DNS server
| | |-gateway                          --Default gateway
| | |-ip-address                       --IP range
| | |-prefixlen                        --Prefixlen of IP
| | |-status                           --Status
| | |-vlan-id                          --Vlan-id
| | |-state                            --State
| | |-wins-server                      --WINS server
| |
| |-http-redirect                      --Enable HTTP redirection
| |-http-redirect-url                  --HTTP redirection URL
| |
| |-ids-ips-mail>                      --IDS/IPS mail settings
| | |-mail-sender                      --Administrator/superuser mail address
| | |-smtp-server                      --SMTP server address & port
| | |-smtp-server-authentication       --SMTP server status
| | |-username                         --Username of the Administrator/superuser
| | |-password                         --Password of the Administrator/superuser
| | |-send-notifications               --Administrator/superuser mail address
| |
| |-interface>                         --Select wireless lan interface
| | |-wlan>                            --Wireless LAN interface setting
| | | |-2.4GHz>                        --2.4 GHz wireless LAN interface setting
| | | | |-aggregation-length           --Aggregated packet size
| | | | |-ampdu                        --Aggregated MAC Protocol Data Unit
| | | | |-beacon-interval              --Wireless beacon period in TU(1024 us)
| | | | |-channel                      --Wireless channel (depends on country and wireless mode)
| | | | |-channelwidth                 --Wireless channel width
| | | | |-dtim-interval                --Wireless DTIM period in beacon interval
| | | | |-fragmentation-length         --Wireless fragmentation threshold(even only)
| | | | |-guardinterval                --Interval (from interference from other transmissions)
| | | | |-knownap-add                  --Add known access point
| | | | |-knownap-del                  --Delete known access point
| | | | |-macacl-add                   --Add wireless access control (ACL)
| | | | |-macacl-database              --Delete wireless access control (ACL) database
| | | | |-macacl-del                   --Delete wireless access control (ACL)
| | | | |-mcsrate                      --Transmit data rate
| | | | |-mode                         --Enable wireless access control (ACL)
| | | | |-operation-mode               --Wireless operation mode
| | | | |-power                        --Wireless transmit power
| | | | |-preamble                     --Wireless preamble (only effect on 802.11b rates)
| | | | |-radio                        --Enable wireless radio
| | | | |-rate                         --Wireless transmission date rate
| | | | |-rifs-transmission            --Enable successive frame transmission at different
| | | | |                                transmit powers
| | | | |-rogue-ap-detection           --Enable rogue access point detection
| | | | |-rts-threshold                --Wireless RTS/CTS threshold
| | | | |-11dSupport                   --IEEE802.11d status
| | | | |-client-isolation             --Client isolation status
| | | | |-create-qos-policy            --Create QoS (Quality of service) policy
| | | | |-create-qos-classification    --Create Qos (Quality of service) classification
| | | | |-delete-qos-policy            --Delete QoS (Quality of service) policy
| | | | |-delete-qos-classification    --Delete Qos (Quality of service) classification
| | | | |
| | | | |-security-profile>            --Create security profile
| | | | | |-1>                         --1st security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-2>                         --2nd security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-3>                         --3rd security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-4>                         --4th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicyv--Delete outgoing QoS policy
| | | | | |
| | | | | |-5>                         --5th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-6>                         --6th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-7>                         --7th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-8>                         --8th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | |
| | | | |-ids-ips-profile>
| | | | | |-ips-status                 --IDS/IPS (Intrusion detection & prevention system) status
| | | | | |-ips-detection-policy       --IDS/IPS (Intrusion detection & prevention system)
| | | | | |                              policies
| | | | | |-attack-status>                       --IDS/IPS attack configurations
| | | | | | |-EAPOL-logoff-attack                --EAPOL logoff attack status
| | | | | | |-EAPOL-start-attack                 --EAPOL start attack status
| | | | | | |-adhoc-network-detected             --ADHOC network detected attack status
| | | | | | |-adhoc-nw-wired-connectivity        --ADHOC network wired connectivity attack status
| | | | | | |-ap-property-change                 --AP property change attack status
| | | | | | |-association-flood                  --Association flood attack status
| | | | | | |-association-table-overflow         --Association table overflow attack status
| | | | | | |-authentication-failure-attack      --Authentication failure attack status
| | | | | | |-authentication-flood               --Authentication flood attack status
| | | | | | |-cts-flood                          --CTS flood attack status
| | | | | | |-rts-flood                          --RTS flood attack status
| | | | | | |-deauthentication-broadcast-attack  --Deauthentication broadcast attack status
| | | | | | |-device-probing-for-AP              --Device probing for AP attack status
| | | | | | |-disassociation-flood               --Disassociation flood attack status
| | | | | | |-known-client-association-Adhoc-nw  --Known client association ADHOC network attack
| | | | | | |                                      status
| | | | | | |-mac-spoofing                       --MAC spoofing attack status
| | | | | | |-malformed-802.11-packet-detection  --Malformed IEEE802.11 packet detection attack
| | | | | | |                                      status
| | | | | | |-premature-EAP-failure-attack       --Premature EAP failure attack status
| | | | | | |-premature-EAP-success-attack       --Premature EAP success attack status
| | | | | | |-ps-poll-flood-attack               --PS POLL flood attack status
| | | | | | |-rf-jamming-attack                  --RF jamming attack status
| | | | | | |-rogue-ap-detection                 --Rogue AP detection attack status
| | | | | | |-unauthenticated-association        --Unauthenticated-association attack status
| | | | | | |-virtual-carrier-attack             --Virtual carrier attack status
| | | | |
| | | | |-wireless-bridge>             --Wireless bridge setting
| | | | | |-security-profile>          --Create security profile
| | | | | | |-1>                       --1st security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-mac             --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | |
| | | | | | |-2>                       --2nd security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-mac             --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | |
| | | | | | |-3>                       --3rd security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-ma              --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | |
| | | | | | |-4>                       --4th security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-mac             --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | |
| | | | | |
| | | | |
| | | | |-wmm>                         --WMM settings
| | | | | |-ap-data0-best-effort       --Access point best effort voice data
| | | | | |-ap-data1-background        --Access point low-priority data
| | | | | |-ap-data2-video             --Access point video data
| | | | | |-ap-data3-voice             --Access point voice data
| | | | | |-powersave
| | | | | |-station-data0-best-effort  --Station best effort voice data
| | | | | |-station-data1-background   --Station low-priority data
| | | | | |-station-data2-video        --Station video data
| | | | | |-station-data3-voice        --Station voice data
| | | | | |-support                    --Support
| | | | |
| | | |
| | | |-5GHz>                          --5.0 GHz wireless LAN interface setting
| | | | |-aggregation-length           --Aggregated packet size
| | | | |-ampdu                        --Aggregated MAC Protocol Data Unit
| | | | |-beacon-interval              --Wireless beacon period in TU(1024 us)
| | | | |-channel                      --Wireless channel (depends on country and wireless mode)
| | | | |-channelwidth                 --Wireless channel width
| | | | |-dtim-interval                --Wireless DTIM period in beacon interval
| | | | |-fragmentation-length         --Wireless fragmentation threshold(even only)
| | | | |-guardinterval                --Interval (from interference from other transmissions)
| | | | |-knownap-add                  --Add known access point
| | | | |-knownap-del                  --Delete known access point
| | | | |-macacl-add                   --Add wireless access control (ACL)
| | | | |-macacl-database              --Delete wireless access control (ACL) database
| | | | |-macacl-del                   --Delete wireless access control (ACL)
| | | | |-mcsrate                      --Transmit data rate
| | | | |-mode                         --Enable wireless access control (ACL)
| | | | |-operation-mode               --Wireless operation mode
| | | | |-power                        --Wireless transmit power
| | | | |-preamble                     --Wireless preamble (only effect on 802.11b rates)
| | | | |-radio                        --Enable wireless radio
| | | | |-rate                         --Wireless transmission date rate
| | | | |-rifs-transmission            --Enable successive frame transmission at different
| | | | |                                transmit powers
| | | | |-rogue-ap-detection           --Enable rogue access point detection
| | | | |-rts-threshold                --Wireless RTS/CTS threshold
| | | | |-11dSupport                   --IEEE802.11d status
| | | | |-client-isolation             --Client isolation status
| | | | |-create-qos-policy            --Create QoS (Quality of service) policy
| | | | |-create-qos-classification    --Create Qos (Quality of service) classification
| | | | |-delete-qos-policy            --Delete QoS (Quality of service) policy
| | | | |-delete-qos-classification    --Delete Qos (Quality of service) classification
| | | | |
| | | | |-security-profile>            --Create security profile
| | | | | |-1>                         --1st security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-2>                         --2nd security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-3>                         --3rd security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-4>                         --4th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-5>                         --5th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-6>                         --6th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-7>                         --7th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | | |-8>                         --8th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1                     --Wireless wep key 1
| | | | | | |-key2                     --Wireless wep key 2
| | | | | | |-key3                     --Wireless wep key 3
| | | | | | |-key4                     --Wireless wep key 4
| | | | | | |-keyno                    --Key number
| | | | | | |-name                     --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid                     --Network name (1-32 chars)
| | | | | | |-status                   --Profile status
| | | | | | |-vlan-id                  --VLAN id
| | | | | | |-wep-pass-phras           --Wireless wep passphrase key
| | | | | | |-wepkeytype               --Wireless wep key type
| | | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |
| | | | |
| | | | |-ids-ips-profile>
| | | | | |-ips-status                 --IDS/IPS (Intrusion detection & prevention system) status
| | | | | |-ips-detection-policy       --IDS/IPS (Intrusion detection & prevention system
| | | | | |                              policies
| | | | | |-attack-status>             --IDS/IPS attack configurations
| | | | | | |-EAPOL-logoff-attack      --EAPOL logoff attack status
| | | | | | |-EAPOL-start-attack       --EAPOL start attack status
| | | | | | |-adhoc-network-detected   --ADHOC network detected attack status
| | | | | | |-adhoc-nw-wired-connectivity        --ADHOC network wired connectivity attack status
| | | | | | |-ap-property-change                 --AP property change attack status
| | | | | | |-association-flood                  --Association flood attack status
| | | | | | |-association-table-overflow         --Association table overflow attack status
| | | | | | |-authentication-failure-attack      --Authentication failure attack status
| | | | | | |-authentication-flood               --Authentication flood attack status
| | | | | | |-cts-flood                          --CTS flood attack status
| | | | | | |-rts-flood                          --RTS flood attack status
| | | | | | |-deauthentication-broadcast-attack  --Deauthentication broadcast attack status
| | | | | | |-device-probing-for-AP              --Device probing for AP attack status
| | | | | | |-disassociation-flood               --Disassociation flood attack status
| | | | | | |-known-client-association-Adhoc-nw  --Known client association ADHOC network attack
| | | | | | |                                      status
| | | | | | |-mac-spoofing                       --MAC spoofing attack status
| | | | | | |-malformed-802.11-packet-detection  --Malformed IEEE802.11 packet detection attack
| | | | | | |                                      status
| | | | | | |-premature-EAP-failure-attack       --Premature EAP failure attack status
| | | | | | |-premature-EAP-success-attack       --Premature EAP success attack status
| | | | | | |-ps-poll-flood-attack               --PS POLL flood attack status
| | | | | | |-rf-jamming-attack                  --RF jamming attack status
| | | | | | |-rogue-ap-detection                 --Rogue AP detection attack status
| | | | | | |-unauthenticated-association        --Unauthenticated-association attack status
| | | | | | |-virtual-carrier-attack             --Virtual carrier attack status
| | | | | |
| | | | |
| | | | |-wireless-bridge>             --Wireless bridge setting
| | | | | |-security-profile>          --Create security profile
| | | | | | |-1>                       --1st security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-mac             --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | |
| | | | | | |-2>                       --2nd security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-mac             --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | | |
| | | | | | |-3>                       --3rd security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-mac             --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | | |
| | | | | | |-4>                       --4th security profile
| | | | | | | |-authentication         --Authentication type
| | | | | | | |-encryption             --Data encryption
| | | | | | | |-name                   --Profile name
| | | | | | | |-presharedkey           --Preshared key
| | | | | | | |-remote-mac             --Remote MAC
| | | | | | | |-status                 --Profile status
| | | | | | | |-wep-pass-phrase        --Wireless wep passphrase key
| | | | | | | |-wepkey                 --Wireless wep key
| | | | | | | |-wepkeytype             --Wireless wep key type
| | | | | | | |
| | | | | | |
| | | | |
| | | | |-wmm>                         --WMM settings
| | | | | |-ap-data0-best-effort       --Access point best effort voice data
| | | | | |-ap-data1-background        --Access point low-priority data
| | | | | |-ap-data2-video             --Access point video data
| | | | | |-ap-data3-voice             --Access point voice data
| | | | | |-powersave
| | | | | |-station-data0-best-effort  --Station best effort voice data
| | | | | |-station-data1-background   --Station low-priority data
| | | | | |-station-data2-video        --Station video data
| | | | | |-station-data3-voice        --Station voice data
| | | | | |-support                    --???
| | | | |
| | | |
| | |
| |
| |-ipv4>                              --Set host IPv4
| | |-address                          --Host IPv4 address
| | |-default-gateway                  --IPv4 address of default gateway
| | |-dhcp-client                      --Enable dhcpv4 client
| | |-dns-server                       --IPv4 address of DNS server
| | |-network-integrity-check
| |
| |-ipv6>                              --Set host IPv6
| | |-address                          --Host IPv6 address
| | |-default-gateway                  --IPv6 address of default gateway
| | |-dhcp-client                      --Enable dhcpv6 client
| | |-dns-server                       --IPv6 address of DNS server
| | |-network-integrity-check
| |
| |-log>                               --Syslog setting
| | |-syslog-status                    --Enable syslog client
| | |-syslog-server-ip                 --Syslog server IP address
| | |-syslog-server-port               --Syslog server port number
| |
| |-lldp-status                        --Enable/Disable LLDP
| |
| |-radiusv4>                                     --Radiusv4 settings
| | |-accounting-server-primary                   --Primary accounting server
| | |-accounting-server-primary-port              --Primary accounting server port
| | |-accounting-server-primary-sharedsecret      --Primary accounting server shared secret
| | |-accounting-server-secondary                 --Secondary accounting server
| | |-accounting-server-secondary-port            --Secondary accounting server port
| | |-accounting-server-secondary-sharedsecret    --Secondary accounting server shared secret
| | |-authentication-server-primary               --Primary authentication server
| | |-authentication-server-primary-port          --Primary system accounting server shared secret
| | |-authentication-server-primary-sharedsecret  --Primary authentication server shared secret
| | |-authentication-server-secondary             --Secondary authentication server
| | |-authentication-server-secondary-port        --Secondary authentication server port
| | |-authentication-server-secondary-sharedsecret--Secondary authentication server shared secret
| | |-reauthentication-time
| | |-update-global-key
| | |-update-global-key-interval
| |
| |-radiusv6>                                     --Radiusv4 settings
| | |-accounting-server-primary                   --Primary accounting server
| | |-accounting-server-primary-port              --Primary accounting server port
| | |-accounting-server-primary-sharedsecret      --Primary accounting server shared secret
| | |-accounting-server-secondary                 --Secondary accounting server
| | |-accounting-server-secondary-port            --Secondary accounting server port
| | |-accounting-server-secondary-sharedsecret    --Secondary accounting server shared secret
| | |-authentication-server-primary               --Primary authentication server
| | |-authentication-server-primary-port          --Primary system accounting server shared secret
| | |-authentication-server-primary-sharedsecret  --Primary authentication server shared secret
| | |-authentication-server-secondary             --Secondary authentication server
| | |-authentication-server-secondary-port        --Secondary authentication server port
| | |-authentication-server-secondary-sharedsecret--Secondary authentication server shared secret
| | |-reauthentication-time
| | |-update-global-key
| | |-update-global-key-interval
| |
| |-remote>                            --Remote access settings
| | |-ssh                              --Enable remote access via SSH
| | |-telnet                           --Enable remote access via Telnet
| |
| |-snmp>                              --SNMP settings
| | |-description                      --SNMP system description
| | |-read-community                   --SNMP ReadCommunity
| | |-snmp-status                      --SNMP status
| | |-trap-community                   --SNMP ReadCommunity
| | |-trap-server                      --SNMP TrapServer IP address
| | |-write-community                  --SNMP WriteCommunity
| |
| |-spanning-tree                      --Enable spanning tree protocol
| |
| |-time>                              --Time Setting
| | |-custom-ntp-server                --Custom NTP server host name
| | |-ntp-client                       --NTP client host name
| | |-ntp-server                       --NTP server host name
| | |-time-zone                        --Time zone
| |
| |-vlan>                              --VLAN settings
| | |-management-vlan                  --VLAN management-id
| | |-untagged-vlan                    --Untagged VLAN-id
| | |-untagged-vlan-status             --Untagged vlan status
| |
|
|-exit                                 --Logout from CLI
|-file                                 --
|-firmware-upgrade                     --Upload new system firmware file from httpd server
|-firmware-upgrade-tftp                --Upload new system firmware file from tftpd server
|-password                             --System password
|-reboot                               --System reboot
|-restore-configuration                --Restore system configuration
|-restore-default-password             --Restore default system password
|-restore-factory-default              --Restore default system configurations
|-show>                                --Show system settings
| |-configuration                      --Show system configuration
| |-interface>                         --Show wireless lan interface
| | |-eth>                             --Ethernet interface
| | | |-statistics                     --Show ethernet statistics
| | |
| | |-wlan>                            --Wlan interface settings
| | | |-2.4GHz>                        --2.4GHz wlan interface settings
| | | | |-configuration                --Interface configuration
| | | | |-statistics                   --Interface statistics
| | | | |-stationlist                  --Station list
| | | | |-trusted-stationlist          --Trusted station list
| | | | |-knownaplist                  --Known access point list
| | | | |-unknownaplist                --Unknown access point list
| | | | |-ids-ips-statistics           --IDS/IPS statistics
| | | | |-ids-ips-thresholds           --IDS/IPS thresholds
| | | | |-ids-ips-traps                --IDS/IPS trap list
| | | | |-qos-policies                 --QoS policy list
| | | |
| | | |-5GHz>                          --5GHz wlan interface settings
| | | | |-configuration                --Interface configuration
| | | | |-statistics                   --Interface statistics
| | | | |-stationlist                  --Station list
| | | | |-trusted-stationlist          --Trusted station list
| | | | |-knownaplist                  --Known access point list
| | | | |-unknownaplist                --Unknown access point list
| | | | |-ids-ips-statistics           --IDS/IPS statistics
| | | | |-ids-ips-thresholds           --IDS/IPS thresholds
| | | | |-ids-ips-traps                --IDS/IPS trap list
| | | | |-qos-policies                 --QoS policy list
| | | |
| | |
| |
| |-log>                              --System log
| |-system                           --System setting
| |-time                             --System time settings
| |
```

Notification of Compliance

C

NETGEAR Dual Band - Wireless

Regulatory Compliance Information

This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe - EU Declaration of Conformity

CE (!)

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4 GHz), EN301 489-17, EN301 893 (5 GHz), EN60950-1

For complete DoC please visit the NETGEAR EU Declarations of Conformity website at *http://support.netgear.com/app/answers/detail/a_id/11621/*.

EDOC in Languages of the European Community

Language	**Statement**
Cesky [Czech]	*NETGEAR* Inc. tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *NETGEAR Inc.* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *NETGEAR Inc.*, dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *NETGEAR Inc.* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *NETGEAR Inc.*, declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]	Por medio de la presente *NETGEAR Inc.* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *NETGEAR Inc.* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *NETGEAR Inc.* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *NETGEAR Inc.* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *NETGEAR Inc.* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *NETGEAR Inc.* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *NETGEAR Inc.* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *NETGEAR Inc.*, jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *NETGEAR Inc.* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym NETGEAR Inc. oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*NETGEAR Inc.* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	NETGEAR Inc. izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*NETGEAR Inc.* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*NETGEAR Inc.* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *NETGEAR Inc.* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Íslenska [Icelandic]	Hér með lýsir *NETGEAR Inc.* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*NETGEAR Inc.* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure (Radiation Exposure Statement)

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 23 cm between the radiator and your body.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, NETGEAR, Inc., 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the ProSafe Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620 complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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 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 methods:

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

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

- This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
- For operation within 5.15 ~ 5.25GHz frequency range, it is restricted to indoor environment. This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
- For products available in the USA market, only channel 1 ~ 11 can be operated. Selection of other channels is not possible.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 23 cm between the radiator & your body.

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) this device must accept any interference received, including interference that may cause undesired operation.

This device has been designed to operate with an antenna having a maximum gain of 6.29dB. Antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

IMPORTANT NOTE: Radiation Exposure Statement

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 23 cm between the radiator and your body.

Caution

The device for operation in the band 5150 - 5250 MHz is only for indoor usage to reduce the potential for harmful interference to co-channel mobile satellite systems.

High power radars are allocated as primary users (that is, priority users) of the bands 5250 - 5350 MHz and 5650 - 5850 MHz and these radars could cause interference and/or damage to LE-LAN devices.

Industrie Canada

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes:

(1) le dispositif ne doit pas produire de brouillage préjudiciable, et

(2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Ce dispositif a été conçu pour fonctionner avec une antenne ayant un gain maximal de dB 6.29. Une antenne à gain plus élevé est strictement interdite par les règlements d'Industrie Canada. L'impédance d'antenne requise est de 50 ohms.

Conformément à la réglementation d'Industrie Canada, le présent émetteur radio peutfonctionner avec une antenne d'un type et d'un gain maximal (ou inférieur) approuvé pourl'émetteur par Industrie Canada. Dans le but de réduire les risques de brouillage radioélectriqueà l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que lapuissance isotrope rayonnée équivalente (p.i.r.e.) ne dépasse pas l'intensité nécessaire àl'établissement d'une communication satisfaisante.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 23 cm de distance entre la source de rayonnement et votre corps.

Avertissement

Les dispositifs fonctionnant dans la bande 5150 - 5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

De plus, les utilisateurs devraient aussi être avisés que les utilisateurs de radars de haute puissance sont désignés utilisateurs principaux (c.-à-d., qu'ils ont la priorité) pour les bandes 5250 - 5350 MHz et 5650 - 5850 MHz et que ces radars pourraient causer du brouillage et/ou des dommages aux dispositifs LAN-EL.

Detachable Antenna Usage

This device has been designed to operate with a Dipole antenna with a maximum gain of 5dBi. An antenna having a higher gain is strictly prohibited per regulations of Industry Canada. The required antenna impedance is 50 ohms.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (IC: 4054A-12200202 / Model: WNDAP620) has been approved by Industry Canada to operate with the antenna type, maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this user's manual, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

Ce dispositif a ete concu pour fonctionner avec une antenne ayant un gain maximal de Dipole antenna avec 5dBi. Une antenne a gain plus eleve est strictement interdite par les reglements d'Industrie Canada. L'impedance d'antenne requise est de 50 ohms.

Conformement a la reglementation d'Industrie Canada, le present emetteur radio peutfonctionner avec une antenne d'un type et d'un gain maximal (ou inferieur) approuve pourl'emetteur par Industrie Canada. Dans le but de reduire les risques de brouillage radioelectriquea l'intention des autres utilisateurs, il faut choisir le type d'antenne et son gain de sorte que lapuissance isotrope rayonnee equivalente (p.i.r.e.) ne depasse pas l'intensite necessaire al'etablissement d'une communication satisfaisante.

Le present emetteur radio (IC: 4054A-12200202 / Model: WNDAP620) a ete approuve par Industrie Canada pour fonctionner avec les types d'antenne enumeres ci-dessous et ayant un gain admissible maximal et l'impedance requise pour chaque type d'antenne. Les types d'antenne non inclus dans cette liste, ou dont le gain est superieur au gain maximal indique, sont strictement interdits pour l'exploitation de l'emetteur.

Index