NETGEAR

ProSafe Dual Band Wireless-N Access Point WNDAP360

Reference Manual

350 East Plumeria Drive
San Jose, CA 95134
USA

May 4, 2011
202-10826-01
v1.0

©2011 NETGEAR, Inc. All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of NETGEAR, Inc.

Technical Support

Thank you for choosing NETGEAR. To register your product, get the latest product updates, get support online, or for more information about the topics covered in this manual, visit the support website at *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/app/answers/detail/a_id/984*.

Trademarks

NETGEAR, the NETGEAR logo, and Connect with Innovation are trademarks and/or registered trademarks of NETGEAR, Inc. and/or its subsidiaries in the United States and/or other countries. Information is subject to change without notice. Other brand and product names are registered trademarks or trademarks of their respective holders. © 2011 NETGEAR, Inc. All rights reserved.

Statement of Conditions

To improve internal design, operational function, and/or reliability, NETGEAR reserves the right to make changes to the products described in this document without notice. NETGEAR does not assume any liability that may occur due to the use, or application of, the product(s) or circuit layout(s) described herein.

Revision History

Publication Part Number	Version	Publish Date	Comments
202-10826-01	v1.0	May 4, 2011	First publication

Contents

Chapter 1 Introduction

About the ProSafe Dual Band Wireless-N Access Point WNDAP360 6
What Is In the Box? 7
System Requirements 7
Key Features and Standards 8
Supported Standards and Conventions 8
Key Features 9
802.11b/g/n and 802.11a/n Standards–Based Wireless Networking . . . 10
Autosensing Ethernet Connections with Auto Uplink 10
Hardware Description 11
Top Panel 11
Rear Panel 12
Bottom Panel with Product Label 13

Chapter 2 Installation and Basic Configuration

What You Need before You Begin 14
Wireless Equipment Placement and Range Guidelines 14
Ethernet Cabling Requirements 15
LAN Configuration Requirements 15
Computer Hardware Requirements 15
Install and Configure the Wireless Access Point 15
Connect the Wireless Access Point to Computer 16
Log In to the Wireless Access Point 17
Configure Basic General System Settings and Time Settings 19
Configure IP Settings and Optional DHCP Server Settings 21
Configure Basic Wireless Settings 23
Operating Frequency (Channel) Guidelines 29
Test Basic Wireless Connectivity 30
Mount the Wireless Access Point 30
Ceiling Installation 31
Wall Installation 33
Desk Installation 35

Chapter 3 Wireless Configuration and Security

Wireless Data Security Options 36
Security Profiles 38
Before You Change the SSID, WEP, and WPA Settings 39
Configure and Enable Security Profiles 42
Configure RADIUS Server Settings 51

Restrict Wireless Access by MAC Address 53
Schedule the Wireless Radio to Be Turned Off 55
Configure Basic Wireless Quality of Service 56

Chapter 4 Management

Enable Remote Management. 58
SNMP Management 59
Secure Shell and Telnet Management 60
Upgrade the Wireless Access Point Software 61
Manage the Configuration File or Reset to Factory Defaults 64
Save the Configuration 64
Restore the Configuration. 65
Restore the Wireless Access Point to the Factory Default Settings 66
Reboot the Wireless Access Point without Restoring the Default Configuration 67
Change the Administrator Password 68
Enable the Syslog Server 69
Monitor the Wireless Access Point. 69
View System Information 70
Monitor Wireless Stations. 72
View the Activity Log 75
Traffic Statistics 75
Enable Rogue AP Detection and Monitor Access Points 77
Enable and Configure Rogue AP Detection 77
View and Save Access Point Lists 79

Chapter 5 Advanced Configuration

Spanning Tree Protocol and 802.1Q VLAN 81
Hotspot Settings 83
Configure Advanced Wireless Settings 84
Configure Advanced QoS Settings. 86
Configure Wireless Bridging 89
Configure a Point-to-Point Wireless Network 90
Configure a Point-to-Multipoint Wireless Network 93
Configure the Wireless Access Point to Repeat the Wireless Signal Using Point-to-Multipoint Bridge Mode 98

Chapter 6 Troubleshooting

Basic Functioning 104
No LEDs Are Lit on the Wireless Access Point 104
The Active LED or the LAN LED Is Not Lit 105
The WLAN LED Does Not Light Up 105
You Cannot Access the Internet or the LAN from a Wireless-Capable Computer 105
You Cannot Configure the Wireless Access Point from a Browser 106
When You Enter a URL or IP Address a Time-Out Error Occurs. 107

Troubleshooting a TCP/IP Network Using the Ping Utility 107
Testing the LAN Path to Your Wireless Access Point 107
Testing the Path from Your Computer to a Remote Device 108
Problems with Date and Time 108
Use the Packet Capture Tool 109

Appendix A Supplemental Information

Technical Specifications 110
Factory Default Settings 112

Appendix B Command-Line Reference

Appendix C Notification of Compliance

Index

Introduction

1

This chapter introduces the NETGEAR® ProSafe™ Dual Band Wireless-N Access Point WNAP360 and describes some of the key features. This chapter includes the following sections:

- *About the ProSafe Dual Band Wireless-N Access Point WNDAP360*
- *What Is In the Box?*
- *System Requirements*
- *Key Features and Standards*
- *Hardware Description*

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

About the ProSafe Dual Band Wireless-N Access Point WNDAP360

The ProSafe Dual Band Wireless-N Access Point WNDAP360 is the basic building block of a wireless LAN infrastructure. It provides 2.4 GHz 802.11b/g/n and 5 GHz 802.11a/n connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

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 of about a 500-foot radius. The ProSafe Dual Band Wireless-N Access Point WNDAP360 can support a small group of users—typically 10 to 32 users per radio—in a range of several hundred feet, with a maximum of 64 supported clients.

The ProSafe Dual Band Wireless-N Access Point WNDAP360 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 seamless connection to the network.

The autosensing capability of the ProSafe Dual Band Wireless-N Access Point WNDAP360 allows packet transmission at up to 300 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.

What Is In the Box?

The product package should contain the following items:

- ProSafe Dual Band Wireless-N Access Point WNDAP360
- Power adapter and cord (12 VCD, 1.0A)
- Straight-through Category 5 Ethernet cable
- *ProSafe Dual Band Wireless-N Access Point WNDAP360 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.

Refer to the NETGEAR website at *http://kbserver.netgear.com/main.asp* for the telephone number of customer support in your area. You should keep the *Installation Guide*, along with the original packing materials, and use the packing materials to repack the wireless access point if you need to return it for repair.

To qualify for product updates and product warranty, NETGEAR encourages you to register on the NETGEAR website at *http://my.netgear.com/registration/login.aspx*.

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 Web browser for configuration, such as Microsoft Internet Explorer 6.0 or later, or Mozilla 1.5 or later
- At least one computer with the TCP/IP protocol installed
- An 802.11a/n or 802.11b/g/n-compliant device, such as the NETGEAR® RangeMax™ Wireless-N Dual Band USB Adapter WNDA3100v2.

Key Features and Standards

The ProSafe Dual Band Wireless-N Access Point WNDAP360 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 ProSafe Dual Band Wireless-N Access Point WNDAP360 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.
- **Full WPA and WPA2 support**. 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 preshared key authentication is without the overhead of RADIUS servers but with all of 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 eight SSIDs 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 client support**. DHCP provides a dynamic IP address to PCs and other devices upon request. The wireless access point can act as a client and obtain information from your DHCP server; it can also act as a DHCP server and provide network information for wireless clients.
- **SNMP Support**. Support for Simple Network Management Protocol (SNMP) Management Information Base (MIB) management.
- **802.1Q VLAN (virtual LAN) support**. A network of computers that behave as if they are connected to the same network even though they might actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user and host management, bandwidth allocation, and resource optimization.

Key Features

The ProSafe Dual Band Wireless-N Access Point WNDAP360 provides solid functionality, including the following features:

- **Dual Band Concurrent**. The wireless access point can operate in both the 2.4 GHz band and the 5 GHz band concurrently.

  The choice of bands is reflected in the protocol standard supported, as well as the administration screens that are displayed.

- **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 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.
  - **Repeating the wireless signal**. In this mode, the wireless access point does not function as an access point for clients but functions only in point-to-*multi*point 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.
- **Hotspot settings**. You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify.
- **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.
- **Rogue AP detection**. The Rogue AP filtering feature ensures that unknown APs are not given access to any part of the LAN.
- **Access control**. The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the wireless access point to gain access to your 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 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 via the Ethernet interface. A Secure Shell (SSH) client is required.
- **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.

- **Power over Ethernet**. Power can be supplied to the wireless access point over the Ethernet port from any 802.3af-compliant midspan or end-span source.
- **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.
- **Wi-FI Multimedia (WMM) support**. 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.
- **Quality of Service (QoS) support**. You can 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 feature allows you to prioritize traffic, such as voice and video traffic, so that packets do not get dropped.
- **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 ProSafe Dual Band Wireless-N Access Point WNDAP360 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. Additionally, the wireless access point supports the following wireless features:

- Aggregation support
- Reduced InterFrame spacing support
- 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 ProSafe Dual Band Wireless-N Access Point WNDAP360 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 ProSafe Dual Band Wireless-N Access Point WNDAP360.

Top Panel

The ProSafe Dual Band Wireless-N Access Point WNDAP360 LEDs are described in the following figure and table:

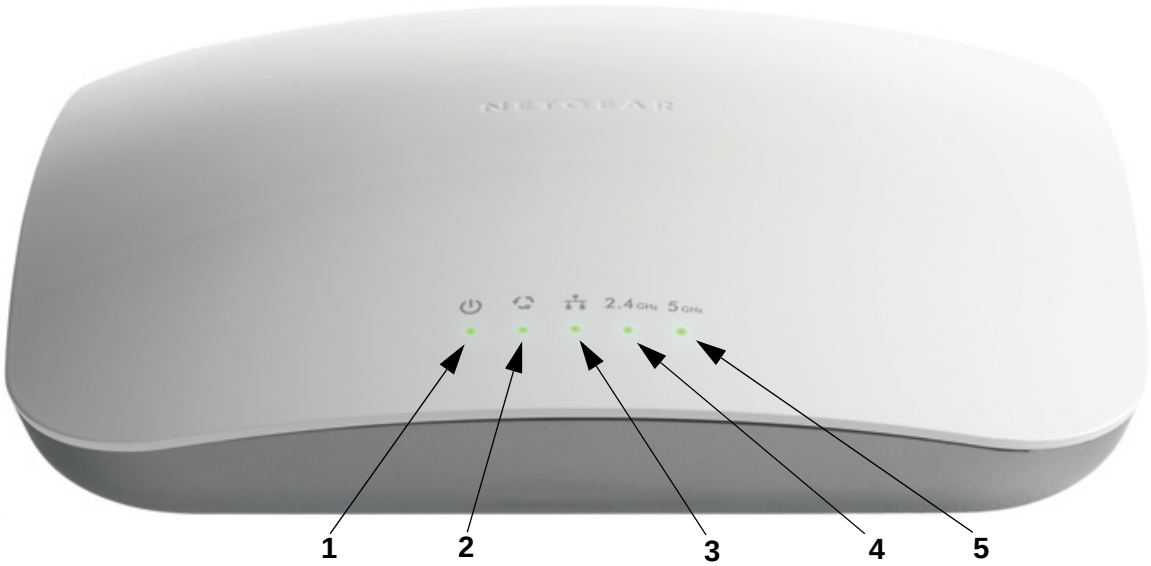


Figure 1.

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

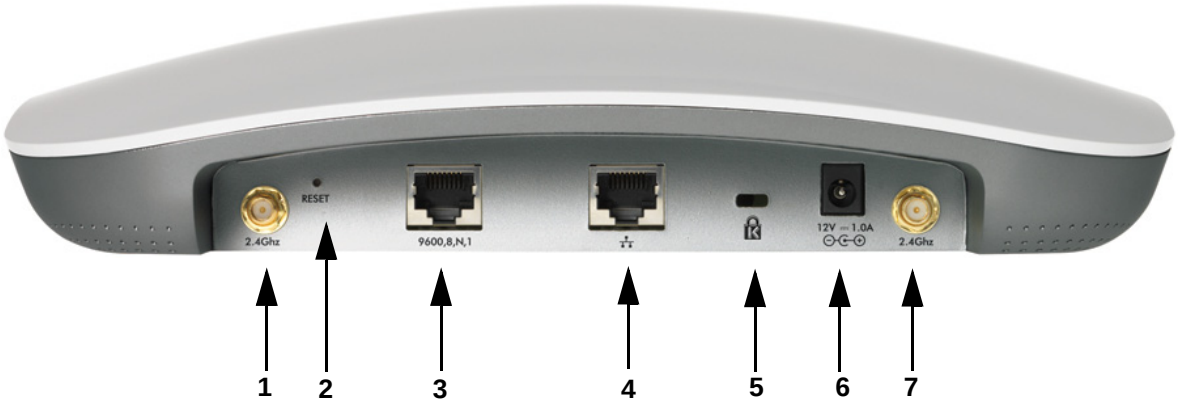


Figure 2.

The rear panel functions of the ProSafe Dual Band Wireless-N Access Point WNDAP360 are described in the following list:

1. 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 66.
3. 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.
4. 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.
5. Cable security lock receptacle for an optional lock.
6. Power socket for a 12 VDC, 1A power adapter.
7. Reverse SMA connector for an optional 2.4-GHz antenna.

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:

Figure 3.

Installation and Basic Configuration

2

This chapter describes how to install and configure your access point for wireless connectivity to your LAN. This basic configuration will enable computers with 2.4 GHz 802.11b/g/n or 5 GHz 802.11 a/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*

Note: In this chapter and in all further chapters, the WNDAP360 is referred to as the wireless access point.

What You Need before You Begin

You need to consider the following guidelines and requirements before you can set up your wireless access point. See also *System Requirements* on page 7.

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 notebook 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 wirelessly connect to the wireless access point. For complete performance specifications, see *Appendix A, Supplemental Information*.

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

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, 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 WNDAP360 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.

Computer Hardware Requirements

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.

Install and Configure the Wireless Access Point

Before installing the wireless access point, make sure that your Ethernet network is up and working. You will be connecting the wireless access point to the Ethernet network. Then computers with 802.11b/g/n or 802.11a/n wireless adapters will be able to communicate with the Ethernet network.

In order for this to work correctly, verify that you have met all of the system requirements, shown in *System Requirements* on page 7.

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

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

Connect the Wireless Access Point to 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).

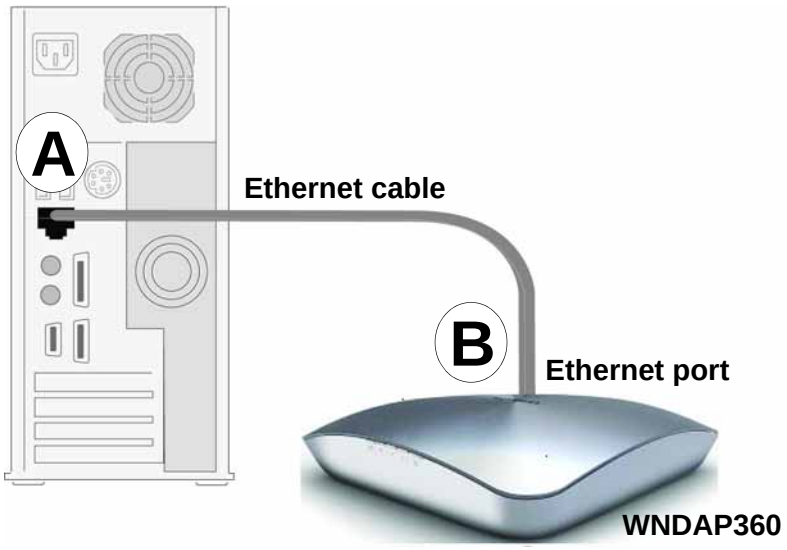


Figure 4.

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 will not need to use the power adapter to power the wireless access point. This 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 http://192.168.0.100. The wireless access point is set, by default, for the DHCP client to be disabled.

➢ **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 **http://192.168.0.100** into your browser. The Login screen opens:

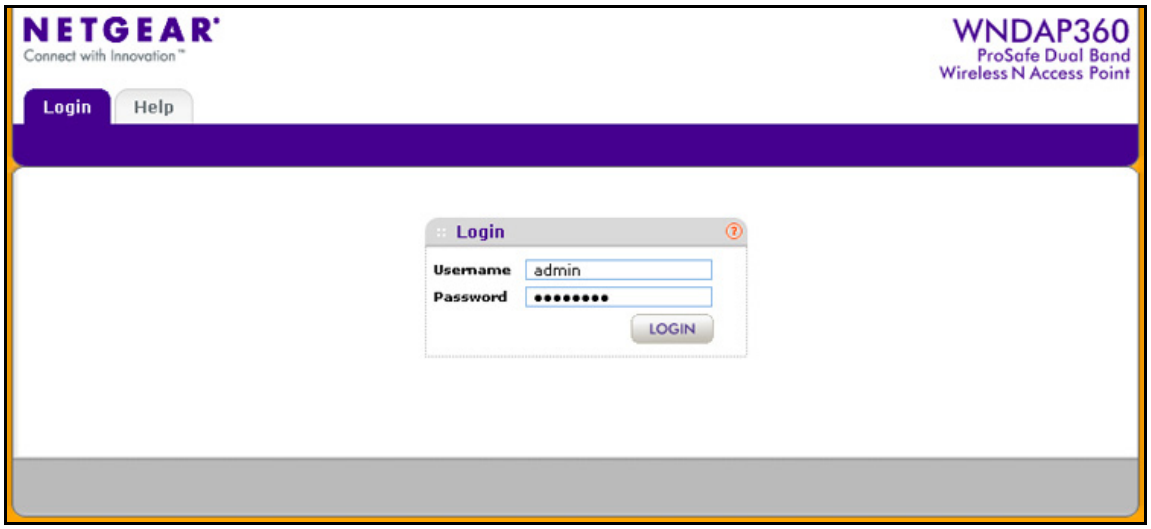


Figure 5.

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 8* on page 19.

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 6.

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 7.

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:

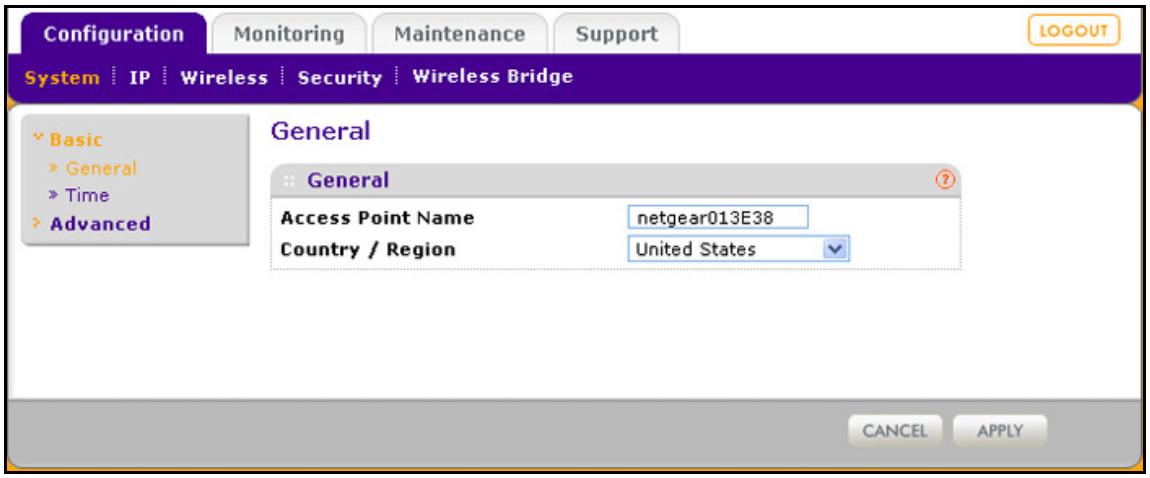


Figure 8.

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

Table 2. Basic General System Settings

Field	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 netgearxxxxxx, where xxxxxxx 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:

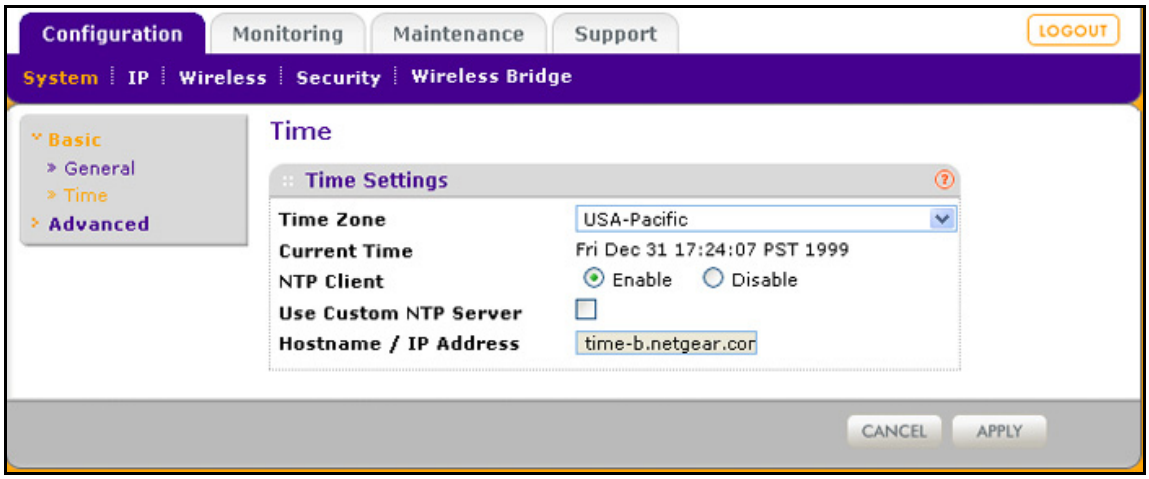


Figure 9.

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

Table 3. Time System Settings

Field	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.	
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 to 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 IP Settings and Optional DHCP Server Settings

➢ **To configure the IP settings:**

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

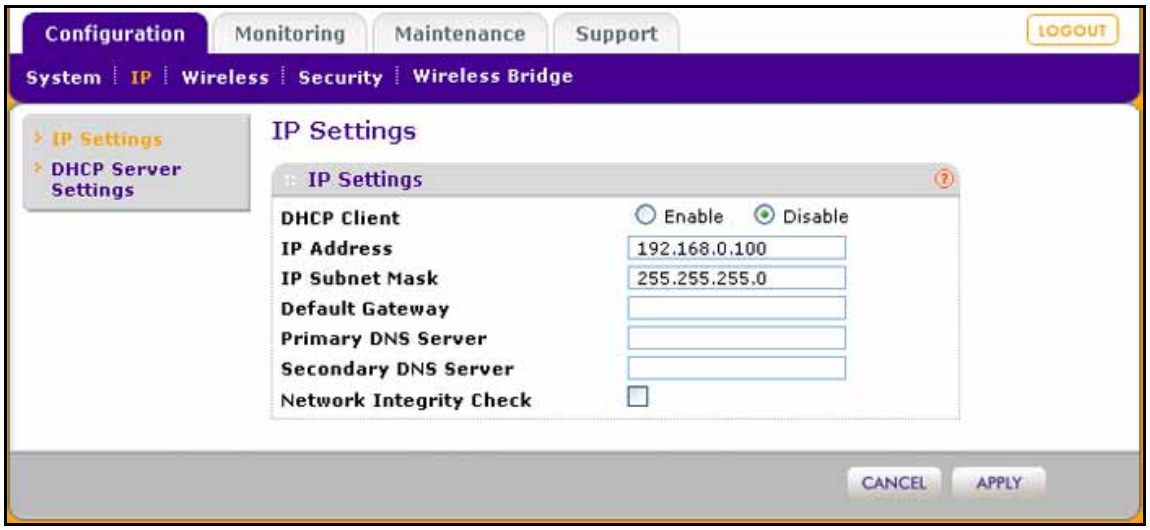


Figure 10.

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

Table 4. IP Settings

Field	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 will receive 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's router to which the wireless access point will connect.
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.

The wireless access point provides a built-in DHCP 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.

➢ **To configure DHCP server settings:**

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

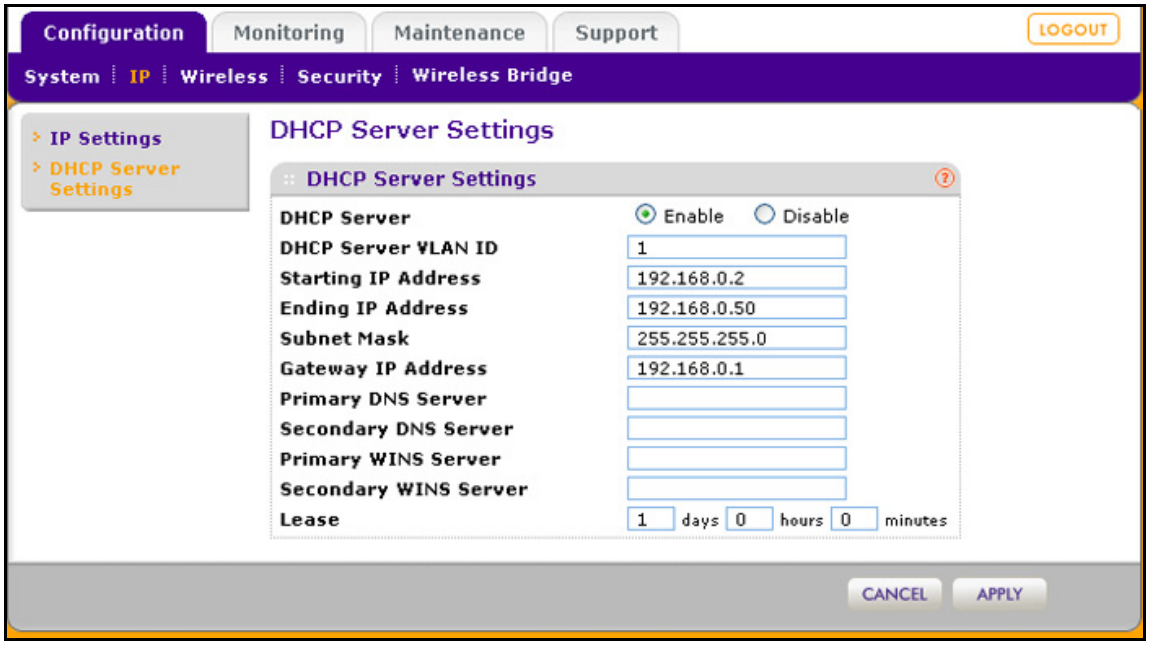


Figure 11.

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

Table 5. DHCP Server Settings

Field	Description
Select the **DHCP Server** check box to enable the DHCP server. Use the default settings or specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless access point's LAN IP address.	
DHCP Server VLAN ID	Enter the DHCP server VLAN ID. The VLAN ID range is between 1 and 4094.
Starting IP Address	Enter the first address in the range of IP addresses to be assigned to DHCP clients. The default address is 192.168.1.02.
Ending IP Address	Enter the last address in the range of IP 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 IP Address	Enter the IP address of the default routing gateway to be used by DHCP clients. The default address is 192.168.0.1.

Table 5. DHCP Server Settings (Continued)

Field	Description
Primary DNS Address	Enter the IP address of the primary Domain Name Server (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.
Secondary WINS Server	Enter the IP address of the secondary WINS server for the network.
Lease	Enter the period that the DHCP server grants to DHCP clients to use the assigned IP addresses. The default time is 1 day.

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

Configure Basic Wireless Settings

For proper compliance and compatibility between similar products in your coverage area, you need to correctly configure the 802.11b/g/n and 802.11a/n wireless adapter settings, including the operating channel and country. You also need to correctly 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 will 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.)

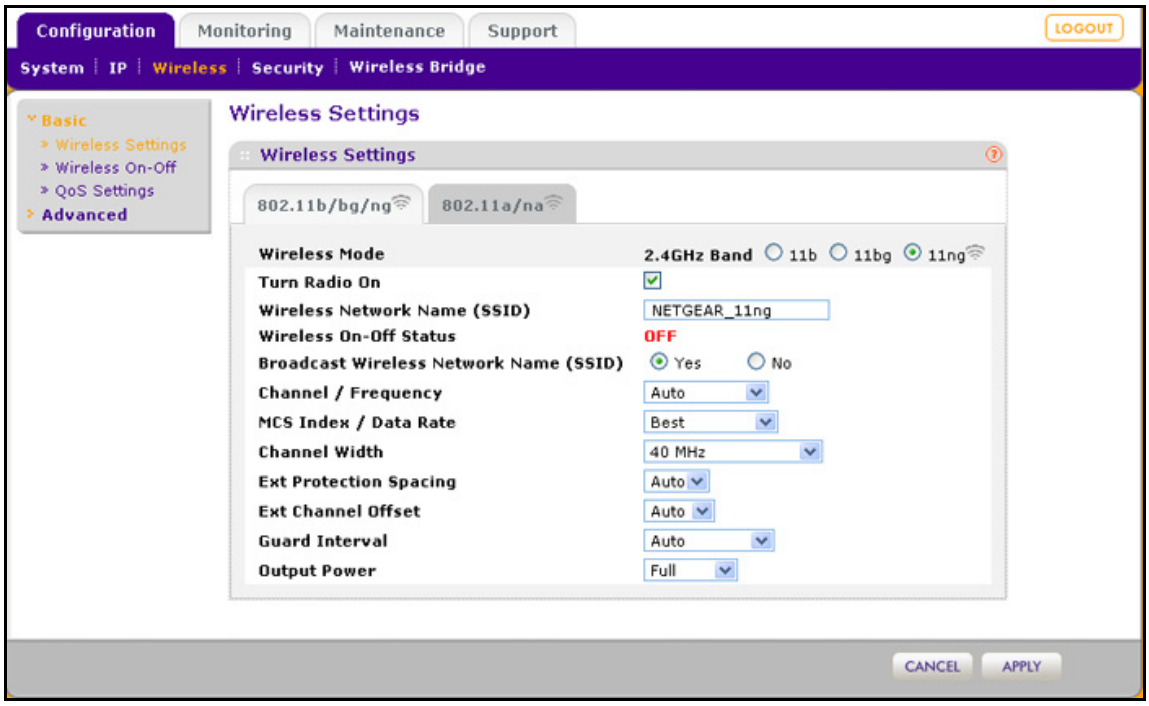


Figure 12.

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, button, and drop-down list onscreen are masked out.

3. Turn on the radio by selecting the **Turn Radio On** check box. A popup 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

Field	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 will not get a wireless connection to the wireless access point.	
Scheduler Status	This is a nonconfigurable field that show the status of the wireless scheduler. For more information, see *Schedule the Wireless Radio to Be Turned Off* on page 55.	
Broadcast Wireless Network Name (SSID)	Select the **Yes** radio button to enable the wireless access point to broadcasts 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 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). Should this happen, you might want to experiment with different channels to see which is the best. For more information, see *Operating Frequency (Channel) Guidelines* on page 29. **Note:** For more information about available channels and frequencies, see *Technical Specifications* in Appendix A.	
11ng mode only **Note:** For most networks, the default settings will 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* in Appendix A.
	Channel Width	From the drop-down list, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, or 40 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz.
	Ext Protection Spacing	When you select a channel width of Dynamic 20/40 MHz or 40 MHz, you also need to select protection spacing for the extension channel from the Ext Protection Spacing drop-down list. In addition to the default value Auto, you can also select a value of 20 or 25. **Note:** This field is not applicable when the channel width is set to 20 MHz.

Table 6. Basic 2.4-GHz Band Wireless Settings (Continued)

Field	Descriptions	
11ng mode only (continued)	Ext Channel Offset	When you select a channel width of Dynamic 20/40 MHz or 40 MHz, you also need to select the offset for the extension channel from the Ext Channel Offset drop-down list. In addition to the default value Auto, you can also select Upper or Lower. **Note:** This field is not applicable when the channel width is set to 20 MHz.
	Guard Interval	From the drop-down list, select the guard interval to protect transmissions from interference. In addition to the default value Auto, you can also select Long - 800 ns. Some legacy devices can operate only with a long guard interval.
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* in Appendix A.
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: The radio wave icon ( ) displays next to the enabled wireless mode.

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.)

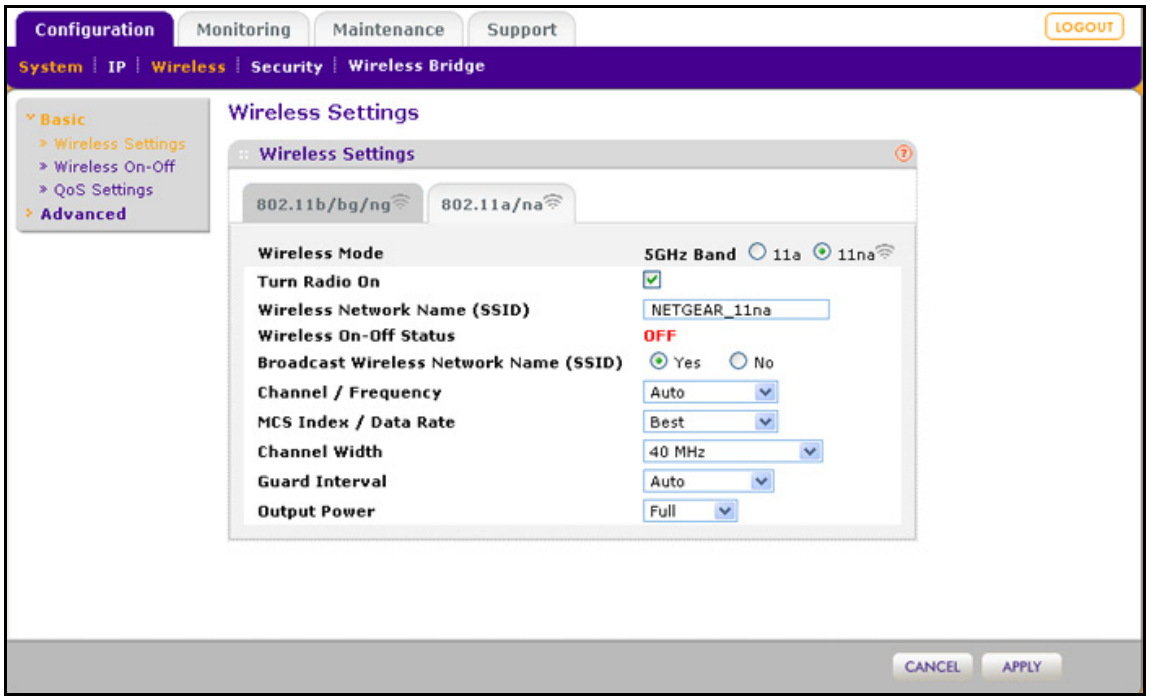


Figure 13.

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, button, and drop-down list onscreen are masked out.

3. Turn on the radio by selecting the **Turn Radio On** check box. A popup 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

Field	Descriptions	
Wireless Network Name (SSID)	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 will not get a wireless connection to the wireless access point.	
Scheduler Status	This is a nonconfigurable field that show the status of the wireless scheduler. For more information, see *Schedule the Wireless Radio to Be Turned Off* on page 55.	
Broadcast Wireless Network Name (SSID)	Select the **Yes** radio button to enable the wireless access point to broadcasts 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 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). Should this happen, 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* in Appendix A.	
11na mode only **Note:** For most networks, the default settings will 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 11na mode, see *Factory Default Settings* in Appendix A.
	Channel Width	From the drop-down list, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, or 40 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. In addition to the default value Auto, you can also select Long - 800 ns. Some legacy devices can operate only with a long guard interval.

Table 7. Basic 5-GHz Band Wireless Settings (Continued)

Field	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* in Appendix A.
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: The radio wave icon ( ) displays next to the selected radio mode.

Operating Frequency (Channel) Guidelines

You should not need to change the operating frequency (channel) unless you notice interference problems, or are setting up the wireless access point near another wireless access point. 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 are using 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, 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 can happen only when the wireless access points use the same SSID. The WNDAP360 wireless access point functions in infrastructure mode by default.

Note: For information about how to configure advanced wireless settings, see *Configure Advanced Wireless Settings* on page 84.

Test Basic Wireless Connectivity

After you have configured the wireless access point as explained in the previous sections, test your computers 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 and 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, and 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*.

WARNING!

Before you deploy the wireless access point in your network, set up wireless security and other wireless features as described in *Chapter 3, Wireless Configuration and Security*.

In addition to wireless security and other wireless features, before you deploy the wireless access point in your network, configure any additional features as described in *Chapter 4, Management* 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

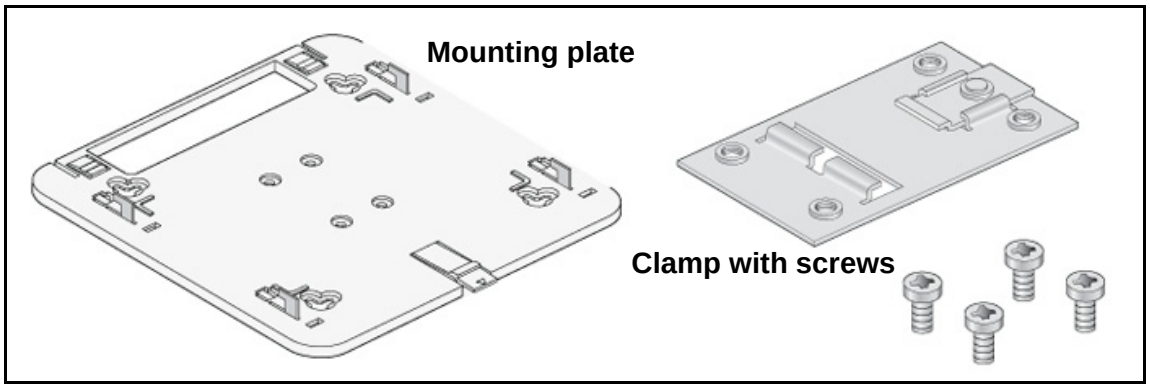
This section includes the following subsections:

- *Ceiling Installation* on this page
- *Wall Installation*
- *Desk Installation*

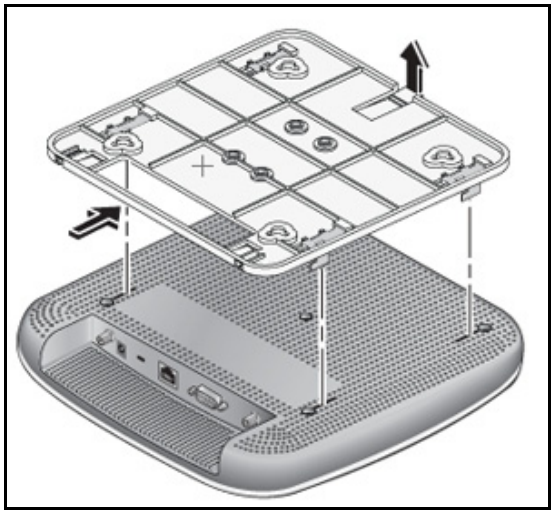
Ceiling Installation

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

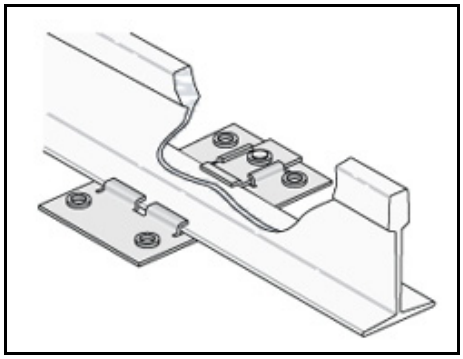
1. Verify the package content of the ceiling installation kit.



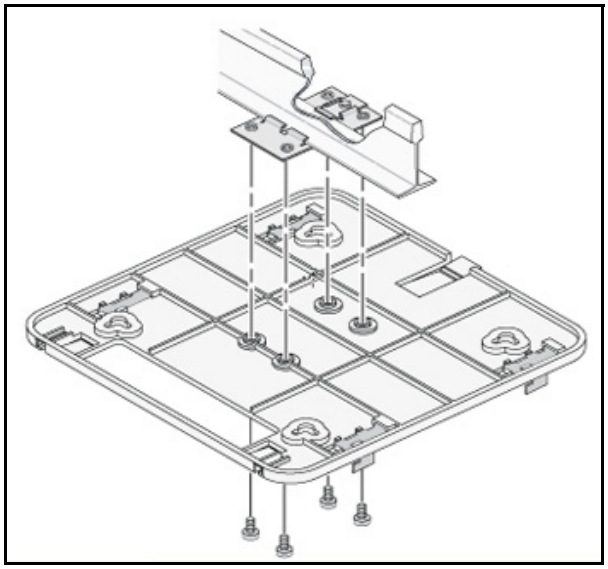
2. Detach the mounting plate from the wireless access point.



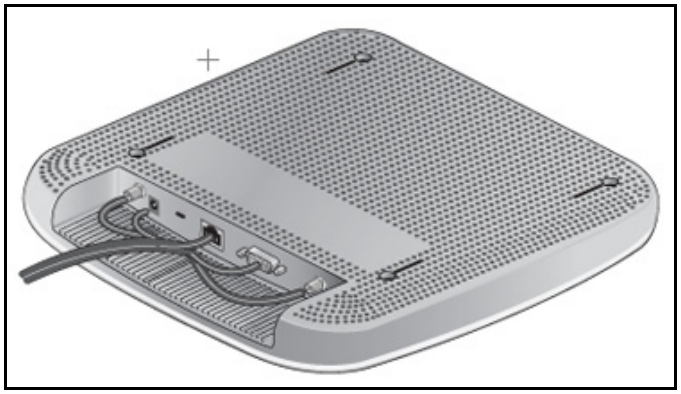
3. Attach the clamp to the ceiling rail.



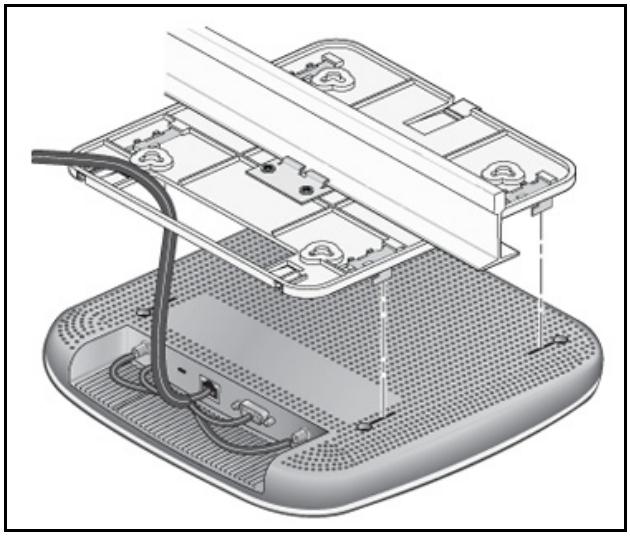
4. Attach the mounting plate to the clamp.



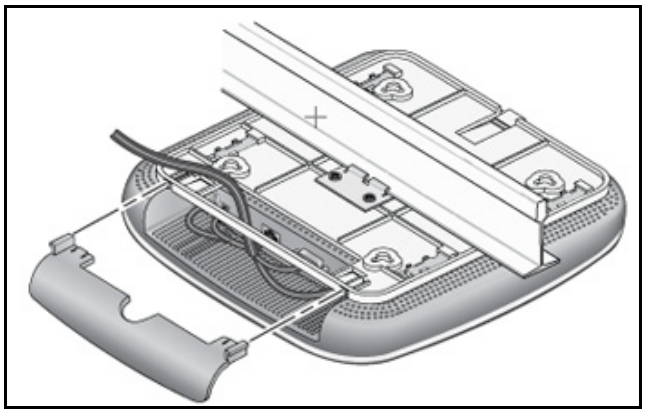
5. Connect the cables to the wireless access point.



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



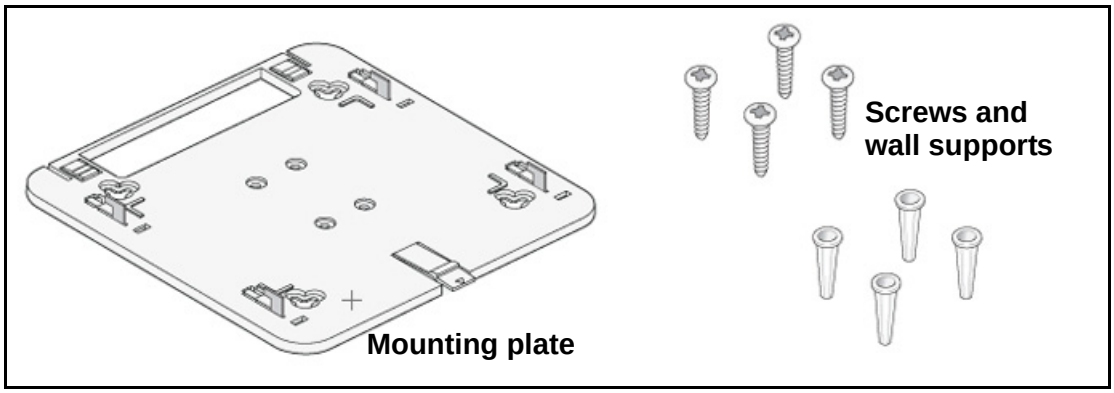
7. Attach the cover to the wireless access point.



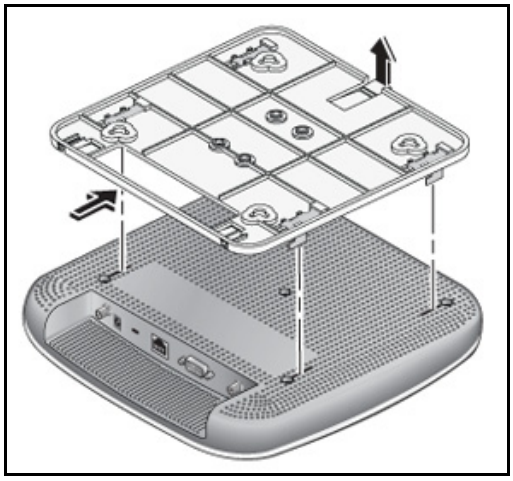
Wall Installation

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

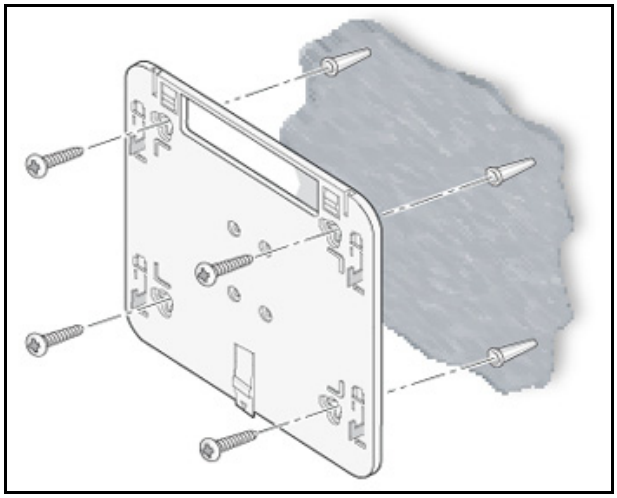
1. Verify the package content of the wall installation kit.



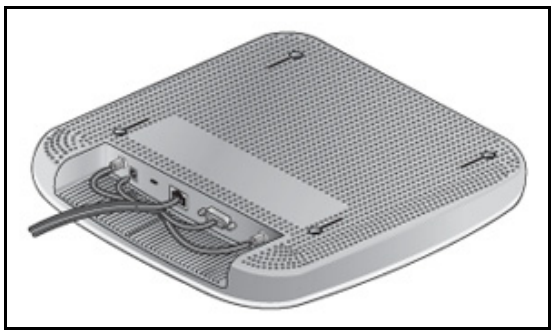
2. Detach the mounting plate from the wireless access point.



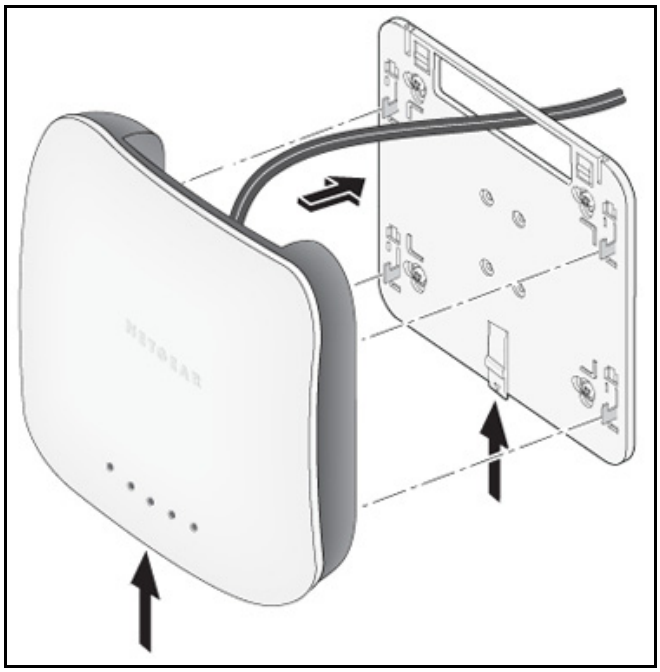
3. Attach the mounting plate to the wall.



4. Connect the cables to the wireless access point.



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

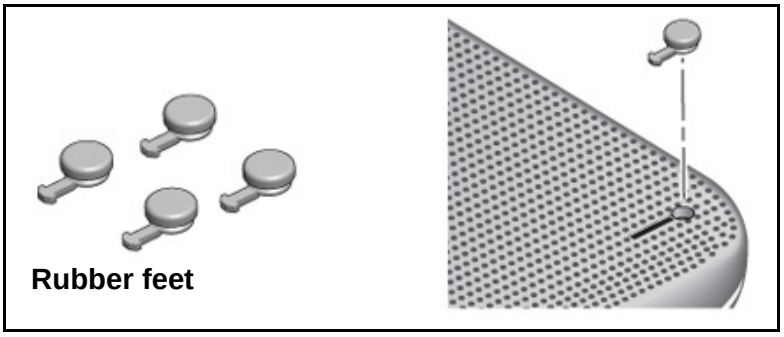


6. Attach the cover to the wireless access point.

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 your ProSafe Dual Band Wireless-N Access Point WNDAP360. This 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 should work with an Ethernet LAN connection, and wireless connectivity should have been verified before you set up wireless security and additional wireless features. In planning your wireless network, consider the level of security required.

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 will 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.

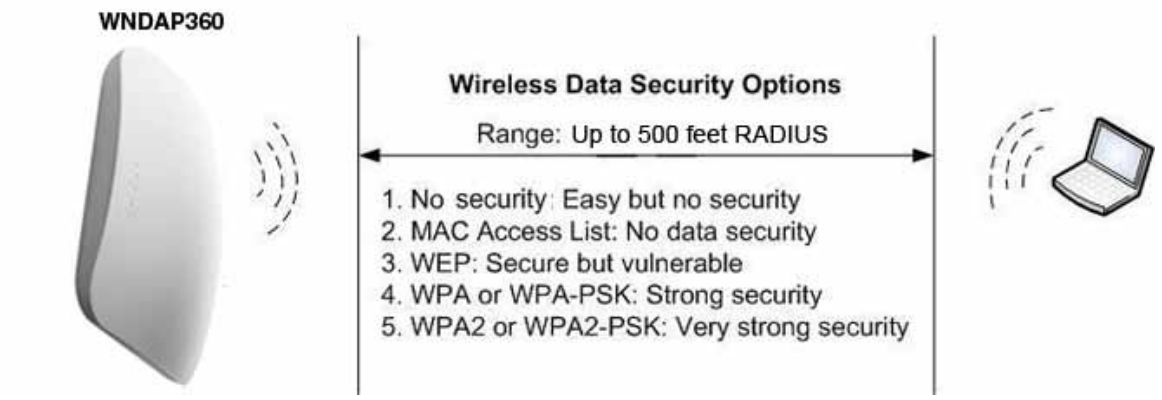


Figure 14.

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 42.
- **Restrict access based by MAC address**. You can allow only trusted PCs to connect so that unknown PCs 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 53.
- **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 of broadcast of the SSID, see *Configure and Enable Security Profiles* on page 42.
- **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 42 and *Configure an Open System with WEP or Shared Key with WEP* on page 47.
- **Legacy 802.1X**. Legacy 80.1X uses RADIUS-based 802.1x authentication but no data encryption.

- **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 make it virtually impossible to compromise.

  WPA uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 42 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 49.

  WPA-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 42 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 50.

- **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 make it virtually impossible to compromise.

  WPA2 uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 42 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 49.

  WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 42 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 50.

- **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 42 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 49.

  WPA-PSK & WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 42 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 50.

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 42).

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 on configuring WPA2 settings.

For information about the types of network authentication that the wireless access point supports, see *Configure and Enable Security Profiles* on page 42.

- **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 42.
- **Wireless client security separation**
  If enabled, the associated wireless clients (using the same SSID) will not be 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 42.
- **VLAN ID**
  If 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 will be 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 42.

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 the following form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step.

Form for 802.11b/bg/ng modes

Store this information in a safe place:

- **SSID**: The service set identification (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, Key Format Passphrase, and Authentication**
  Choose the key size by circling one: 64, 128, or 152 bits.
  Choose the key format by circling one: ASCII or HEX.
  Choose the authentication type by circling one: Open or Shared.

  Passphrase: _____

  Note: If you select shared key, the other devices in the network will not 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: _____

Form for 802.11a/an modes

Store this information in a safe place:

- **SSID**: The service set identification (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, Key Format Passphrase, and Authentication**
  Choose the key size by circling one: 64, 128, or 152 bits.
  Choose the key format by circling one: ASCII or HEX.
  Choose the authentication type by circling one: Open or Shared.

  Passphrase: _____

  Note: If you select shared key, the other devices in the network will not 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: _____

Configure and Enable Security Profiles

➢ **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:

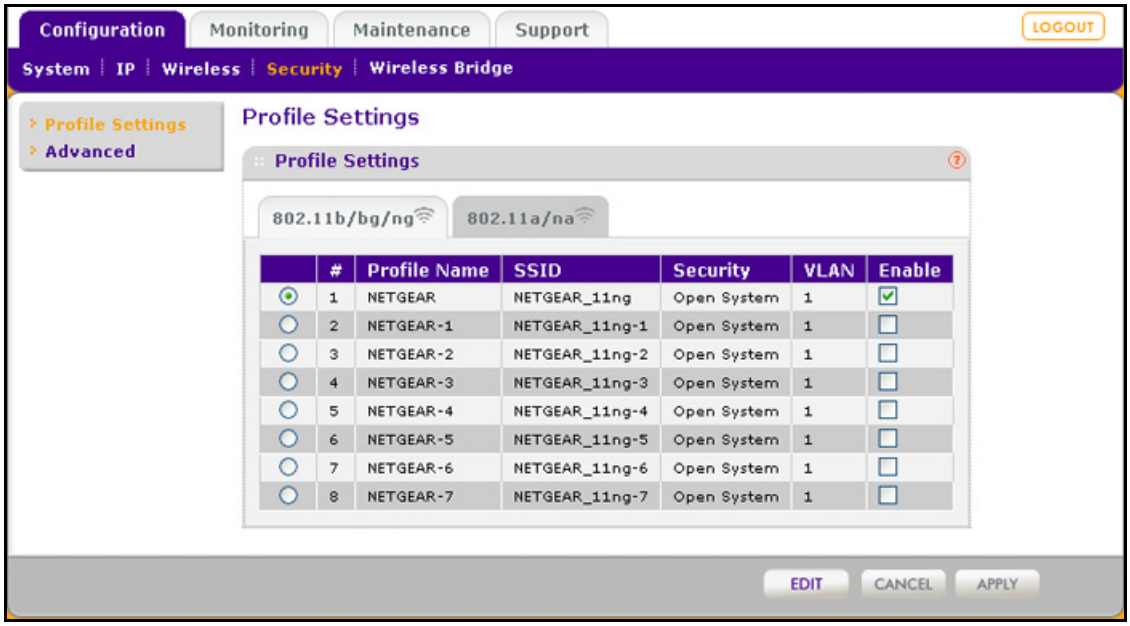


Figure 15.

2. Optionally: 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:

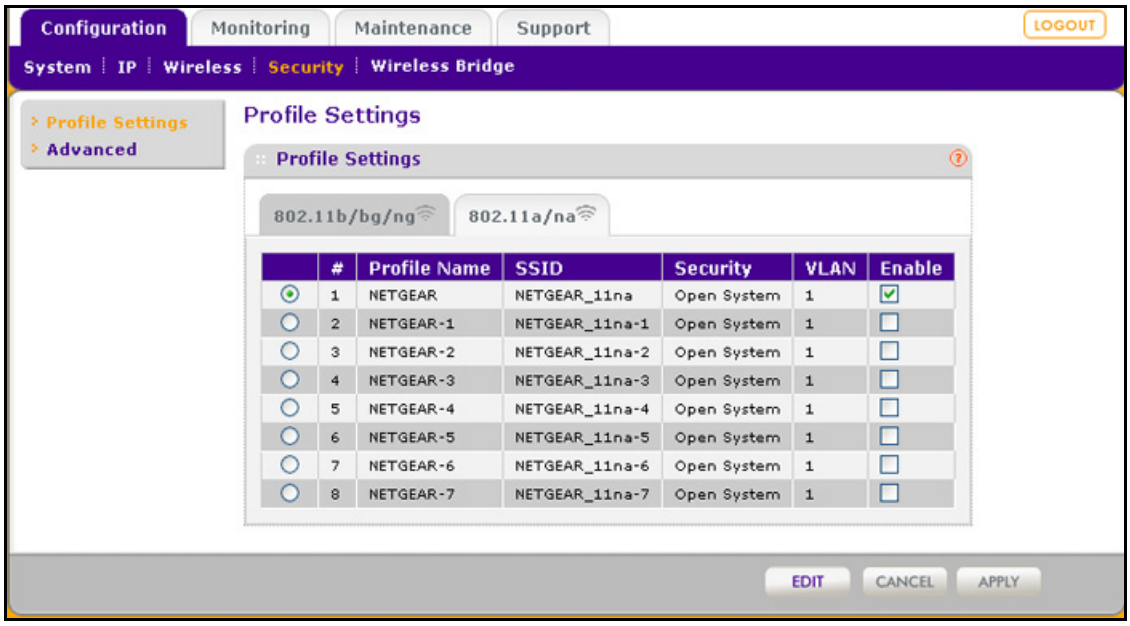


Figure 16.

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

Table 8. Profile Settings Screen

Field	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 first section on the screen is the Profile Definition section; the second section is the Authentication Settings section. These sections are explained separately.

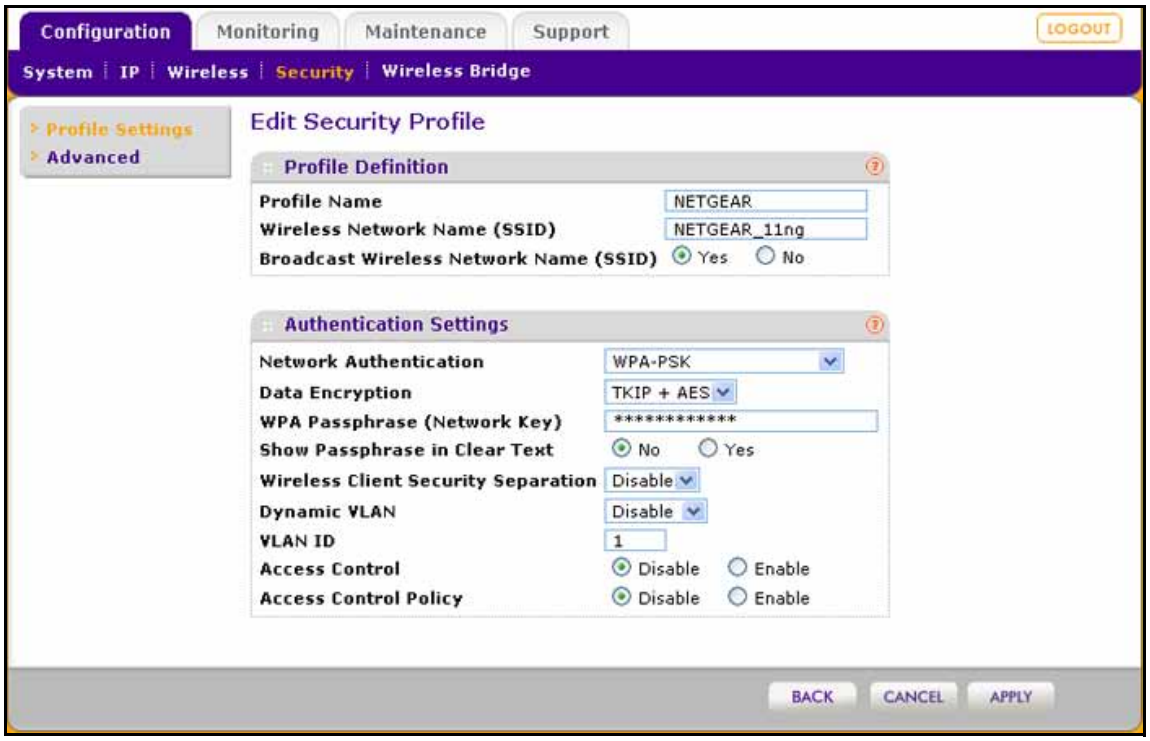


Figure 17.

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 of the Edit Security Profile Screen

Field	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.
Broadcast Wireless Network Name (SSID)	Select the **Yes** radio button to enable the wireless access point to broadcasts 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 on configuring WPA2 settings.

Table 10. Authentication Settings of the Edit Security Profile Screen

Field	Description	
Network Authentication and Data Encryption **Note:** The data encryption fields that are displayed on screen depend on you selection from the Network Authentication drop-down list.	Open System	This is the default setting. You can 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 47.
	Shared Key	You need to use WEP encryption and enter at least one shared key. See *Configure an Open System with WEP or Shared Key with WEP* on page 47.
	Legacy 802.1X	You need to configure the RADIUS server settings to use this option. See *Configure Legacy 802.1X* on page 48.
	WPA with Radius	You need to configure the RADIUS server settings to use this option. See *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 49.
	WPA2 with Radius	Select this setting only if all clients support WPA2. If selected, you need to use AES encryption and configure the RADIUS server settings. See *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 49.
	WPA & WPA2 with Radius	Select this setting to allow clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you need to use TKIP + AES encryption and configure the RADIUS server settings. See *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 49.
	WPA-PSK	You need to use TKIP or TKIP + AES encryption and enter a WPA passphrase (network key). See *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 50.
	WPA2-PSK	Select this only if all clients support WPA2. If selected, you need to use AES and TKIP + AES encryption and enter a WPA passphrase (network key). See *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 50.
	WPA-PSK & WPA2-PSK	Select this setting to allow clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you need to use TKIP + AES encryption and enter a WPA passphrase (network key). See *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 50.

Table 10. Authentication Settings of the Edit Security Profile Screen (Continued)

Field	Description
Wireless Client Security Separation	If you enable wireless client security separation by selecting **Enable** from the drop-down list, the associated wireless clients are not be able to 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.
Dynamic VLAN	From the drop-down list, select how VLANs operate by making one of the following selections: • **Disable**. Disables dynamic VLANs, and enables static VLANs. This is the default setting. • **Optional**. Enables dynamic VLANs but if a RADIUS server does not return a VLAN ID, the wireless station is still allowed to connect to the wireless access point. • **Required**. Enables dynamic VLANs. If a RADIUS server does not return a VLAN ID, the wireless station is not authenticated and cannot connect to the wireless access point. For dynamic VLANs to operate (that is, the selection is Optional or Required), the following is required: • The hubs and switches on your LAN need to support the VLAN (802.1Q) standard. • The authentication is set to any RADIUS type authentication: either the network authentication in the wireless security profile or the remote MAC address database authentication for the MAC Authentication feature can be used.
VLAN ID	Enter the default VLAN ID that needs 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.
Access Control	**Note:** Access control functions only when static VLANs are enabled, that is, you select **Disable** from the Dynamic VLAN drop-down list. The Access Control radio buttons let you enable or disable access control through a RADIUS server to ensure that clients are connected to the wireless access point through the correct VLAN. • **Disable**. Access control is disabled. This is the default setting. • **Enable**. Access control is enabled. Clients are authenticated through a RADIUS server.
Access Control Policy	When access control is enabled, the access control policy lets you specify whether or not a client can access the wireless access point when the client is not authenticated because the VLAN ID is incorrect. Select a radio button to enable or disable access: • **Disable**. If the RADIUS server does not authenticate the client, the client is still allowed to connect to the wireless access point through the default VLAN (which is specified in the VLAN ID field) instead of through the VLAN to which the client is assigned in the RADIUS server. • **Enable**. If the RADIUS server does not authenticate the client, the client is not allowed to connect to the wireless access point.

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

WARNING!

If you use a wireless computer to configure wireless security settings, you will be 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.

Configure an Open System with WEP or Shared Key with WEP

Wether you use an open system with WEP or shared key with WEP, specify the fields 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:

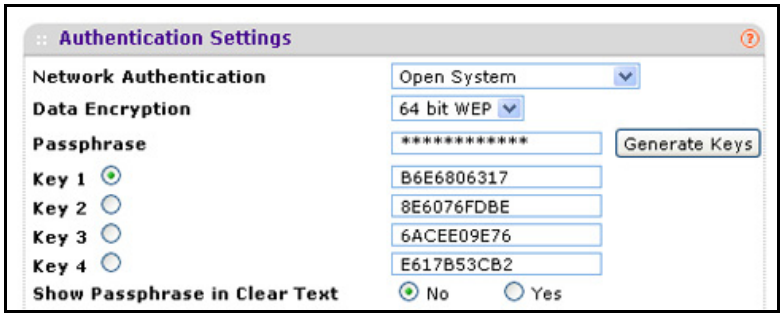


Figure 18.

- **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:

Figure 19.

Table 11. WEP Encryption Settings

Field	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 bits encryption. This mode functions only with other wireless station 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 automatically generate the keys by clicking **Generate Keys**. The default passphrase is sharedsecret. You can display the actual passphrase by selecting the **Show Passphrase in Clear Text** radio button.
Encryption Key (Key1–Key4)	Either manually enter a key or allow the key to be automatically generated by clicking **Generate Key**. • 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 (152-bit WEP) characters. • 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. **Note:** Not all wireless adapters support passphrase key generation.
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 51.

When you select **Legacy 802.1X** from the Network Authentication drop-down list, the Data Encryption drop-down list becomes nonoperational (it shows None only). You need to define the RADIUS servers only to use legacy 802.1X security.

Figure 20.

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 51.

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 following table.

- **WPA with RADIUS**

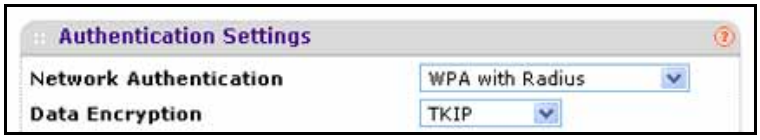


Figure 21.

- **WPA2 with RADIUS**

Figure 22.

- **WPA & WPA2 with RADIUS**

Figure 23.

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

Field	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 WNDAP360 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 following table.

- **WPA-PSK**

Figure 24.

- **WPA2-PSK**

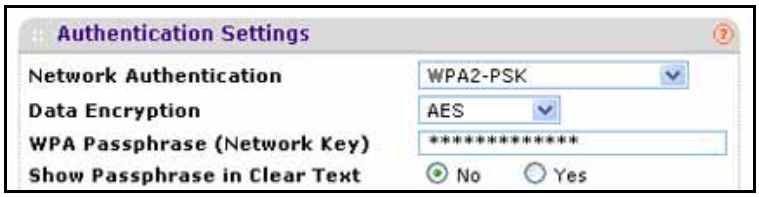


Figure 25.

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

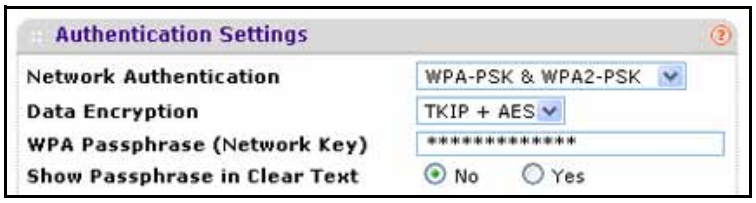


Figure 26.

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

Field	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 WNDAP360 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** 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.

➢ **To configure the RADIUS server settings:**

1. Select **Configuration > Security > Advanced > Radius Server Settings**. The Radius Server Settings screen displays. (The following figure shows some examples.)

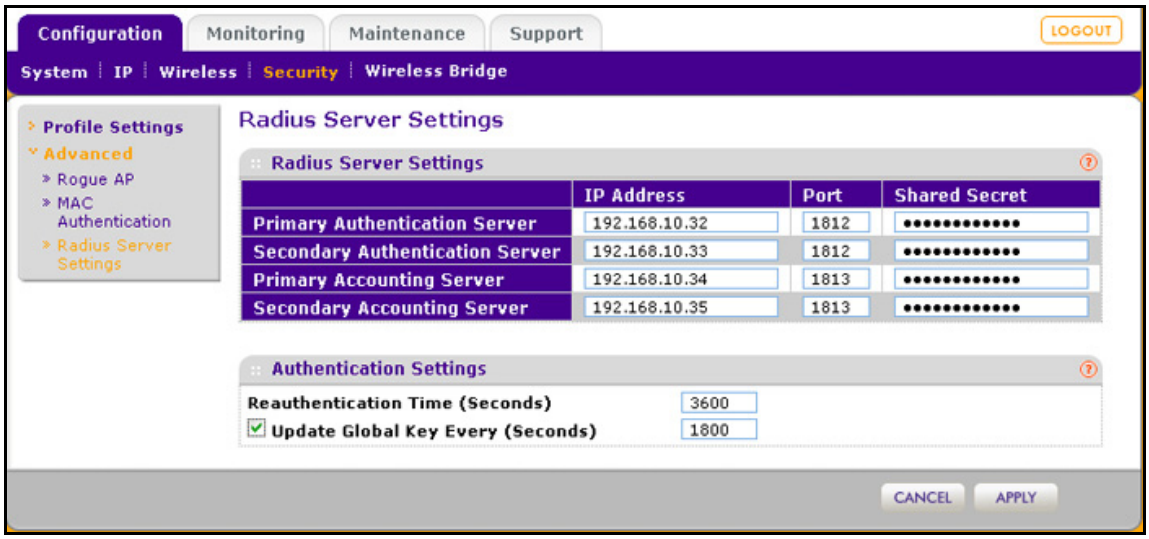


Figure 27.

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

Table 14. RADIUS Server Settings

Field	Descriptions	
RADIUS Server Settings		
Primary Authentication Server	IP Address	Enter the IP address of the primary RADIUS server for authentication.
	Authentication Port	Enter the UDP port number of the wireless access point that is used to access the primary RADIUS server for authentication. The default port number is 1812.
	Secret	Enter the shared key that is used between the wireless access point and the primary RADIUS server during authentication.
Secondary Authentication Server	IP 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.
	Authentication Port	Enter the UDP port number of the wireless access point that is used to access the secondary RADIUS server for authentication. The default port number is 1812.
	Secret	Enter the shared key that is used between the wireless access point and the secondary RADIUS server during authentication.
Primary Accounting Server	IP Address	Enter the IP address of the primary RADIUS server for accounting.
	Authentication Port	Enter the UDP port number of the wireless access point that is used to access the primary RADIUS server for accounting. The default port number is 1813.
	Secret	Enter the shared key that is used between the wireless access point and the primary RADIUS server during the accounting process.

Table 14. RADIUS Server Settings (Continued)

Field	Descriptions	
Secondary Accounting Server	IP 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.
	Authentication Port	Enter the UDP port number of the wireless access point that is used to access the secondary RADIUS server for accounting. The default port number is 1813.
	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 wirelessly connect 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 one example.)

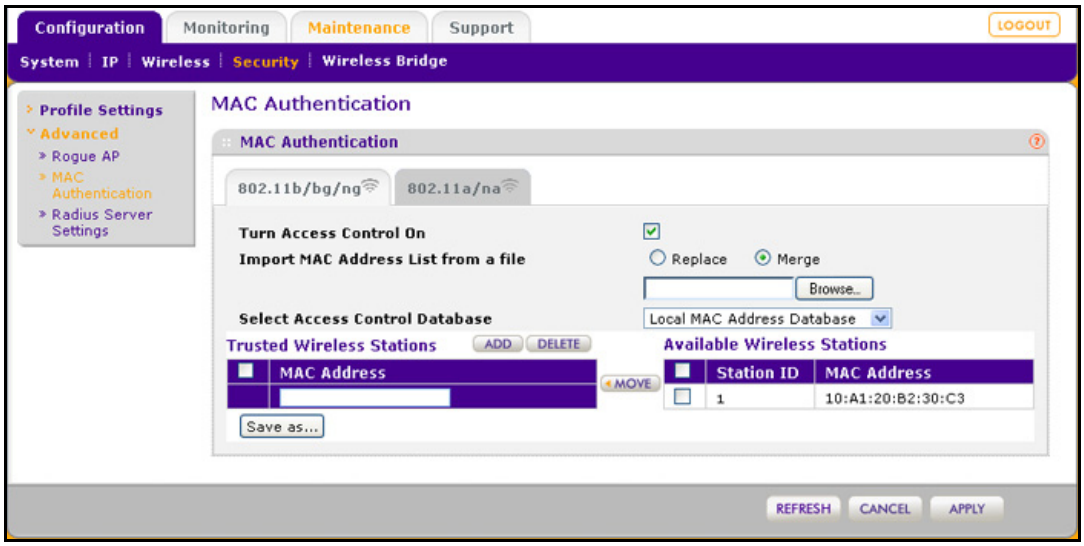


Figure 28.

2. Optionally: 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 51).
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 wirelessly connect to the wireless access point.

WARNING!

When configuring the wireless access point from a wireless computer whose MAC address is not in the access control list, you will 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 which is on the access control list to make any further changes.

Schedule the Wireless Radio to Be Turned Off

The capability to schedule 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:

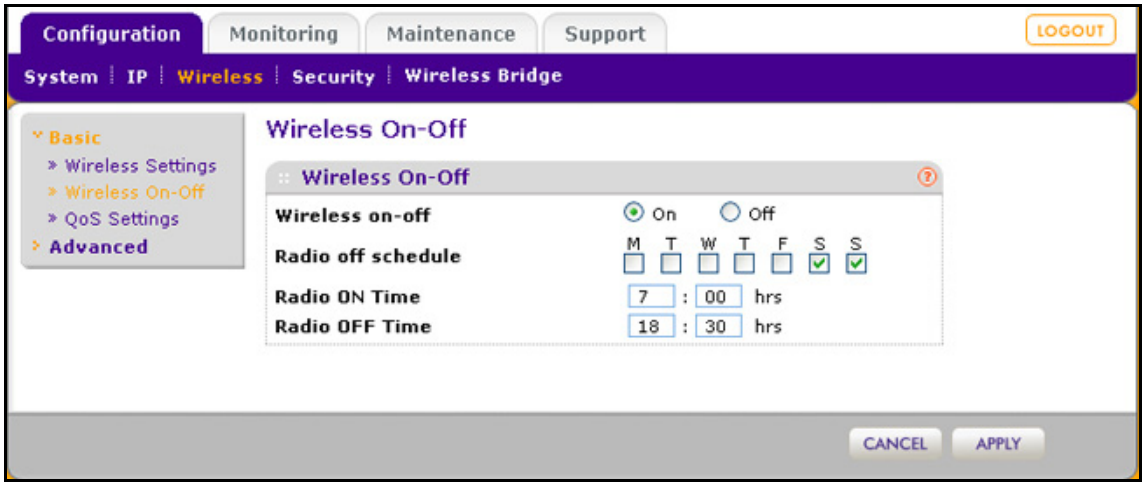


Figure 29.

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

Table 15. Wireless Radio On/Off Settings

Field	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.

Table 15. Wireless Radio On/Off Settings (Continued)

Field	Description
Radio ON Time	Fill in the time that you want the radio to be turned back on. Use 24-hour time format.
Radio OFF Time	Fill in 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 application 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 QoS Settings* on page 86.

➢ **To configure basic wireless QoS:**

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

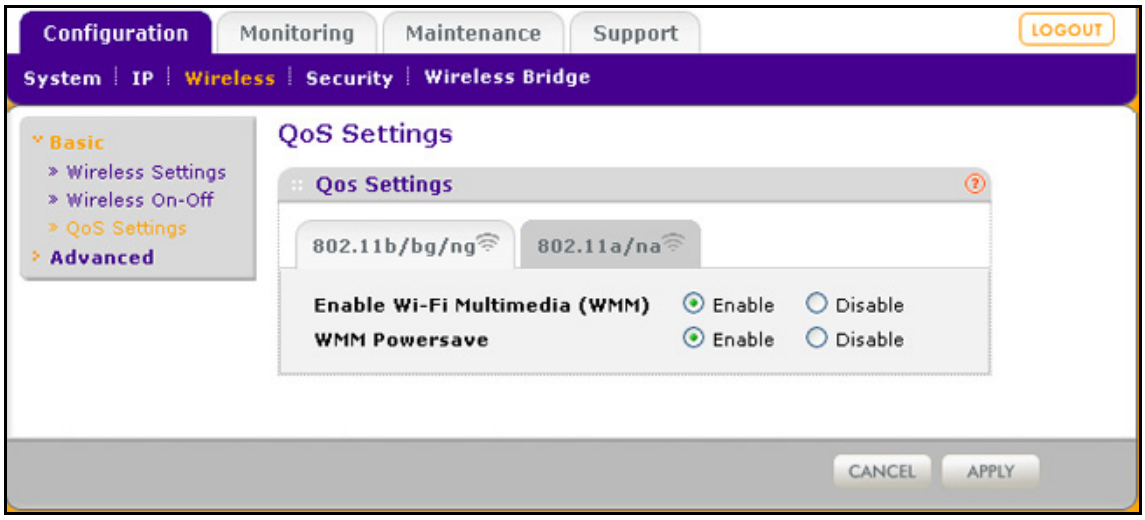


Figure 30.

2. Optionally: 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** button to disable the feature.
   - **WMM Powersave**. To enable this feature, select the **Enable** radio button, which is the default setting. Select the **Disable** button to disable the feature.
4. Click **Apply** to save your settings.

Management

4

This chapter describes how to use the management and monitoring features of your ProSafe Dual Band Wireless-N Access Point WNDAP360. This 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*
- *Enable the Syslog Server*
- *Monitor the Wireless Access Point*
- *Enable Rogue AP Detection and Monitor Access Points*

Enable Remote 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 a 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:

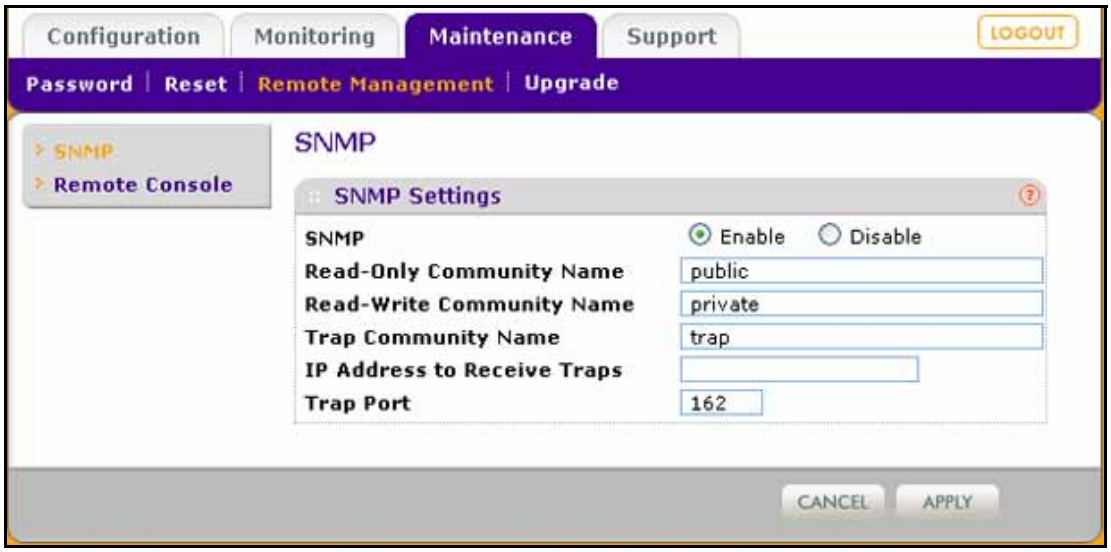


Figure 31.

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

Table 16. SNMP Settings

Field	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	The community string to allow the SNMP manager to send traps. The default is trap.
IP Address to Receive Traps	The IP address of the SNMP manager to receive traps sent from the wireless access point.
Trap Port	The port number of the SNMP manager 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:

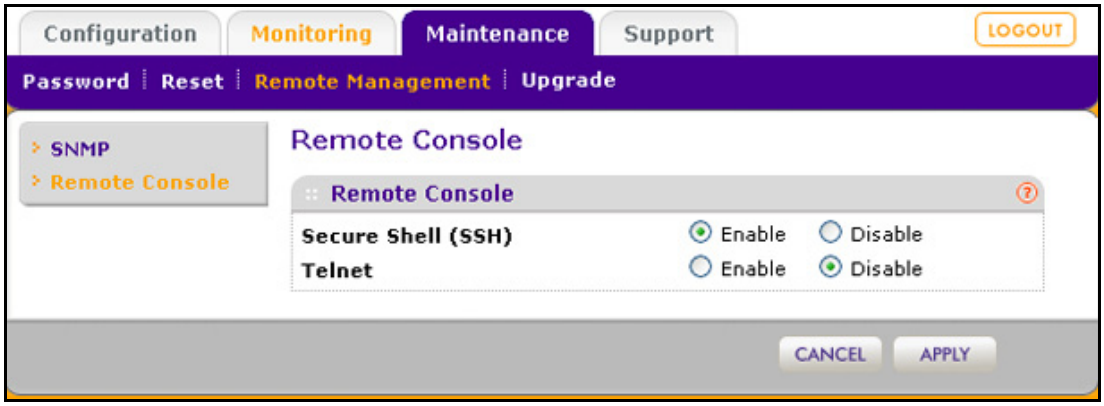


Figure 32.

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 should display:

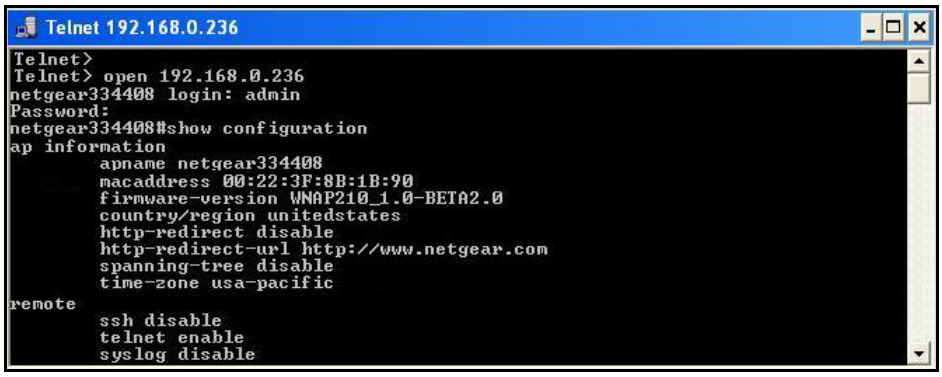


Figure 33.

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

   After successful login, the **>** prompt should appear 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 completely 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:

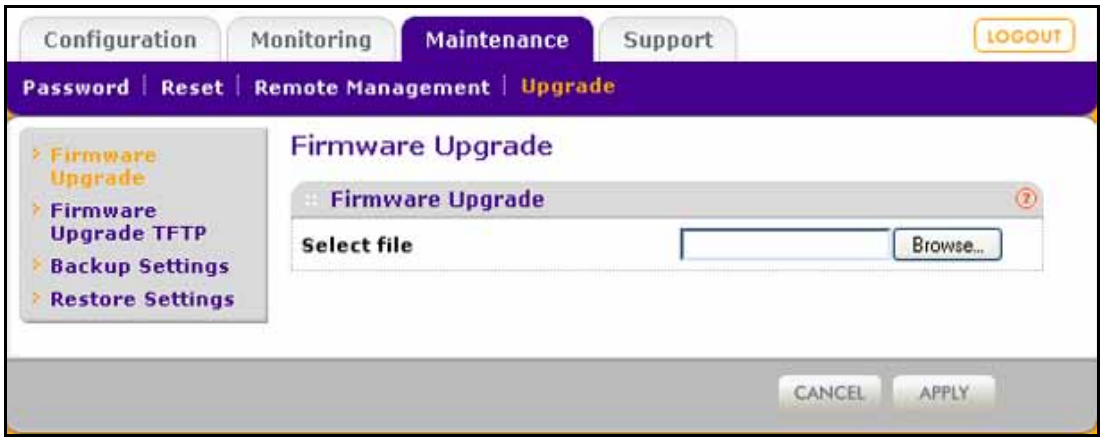


Figure 34.

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 42* on page 70). 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:

Figure 35.

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 42* on page 70). The firmware version is shown in the Access Point Information section of the screen.

Manage the Configuration File or Reset to Factory Defaults

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.

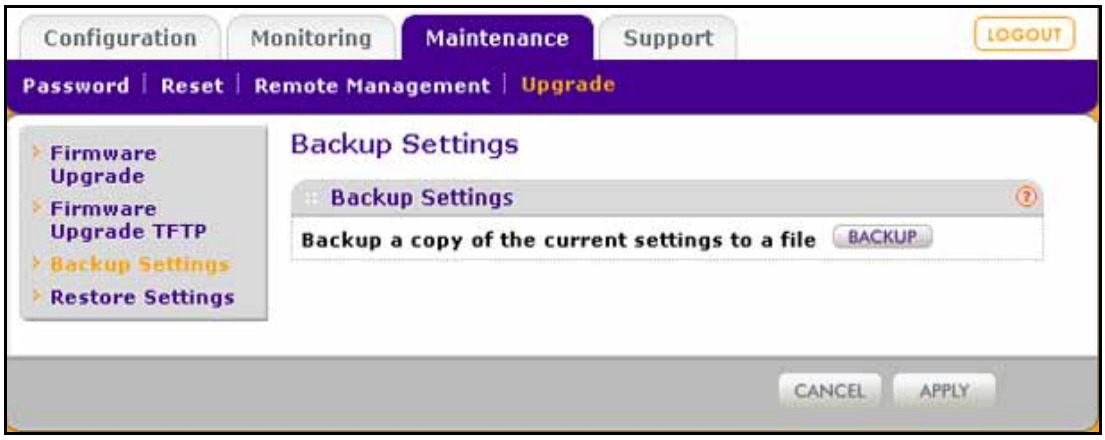


Figure 36.

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:

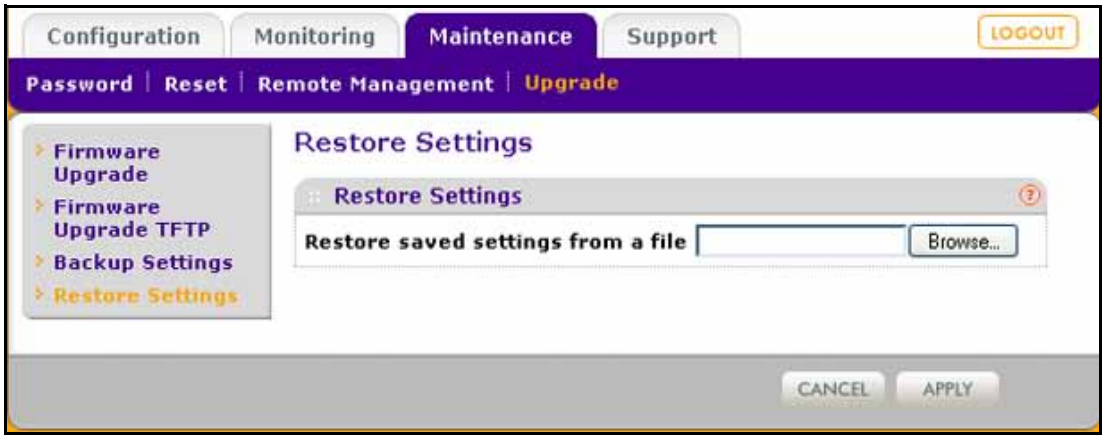


Figure 37.

2. Click **Browse** and locate the saved 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 will be lost.
* The login password will be **password.**
* The default LAN IP address will be **192.168.0.100**.
* The DHCP client will be disabled.
* The Access Point Name field will be 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:

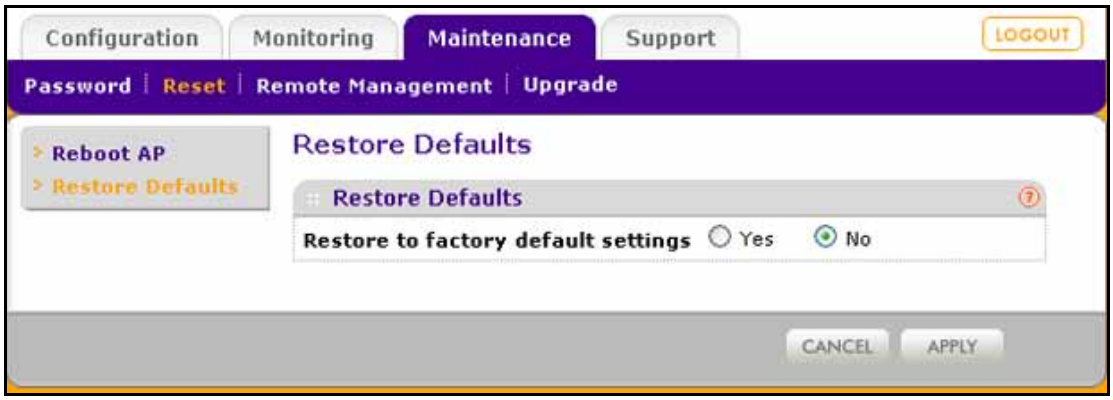


Figure 38.

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 12).

➢ **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 period of 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:

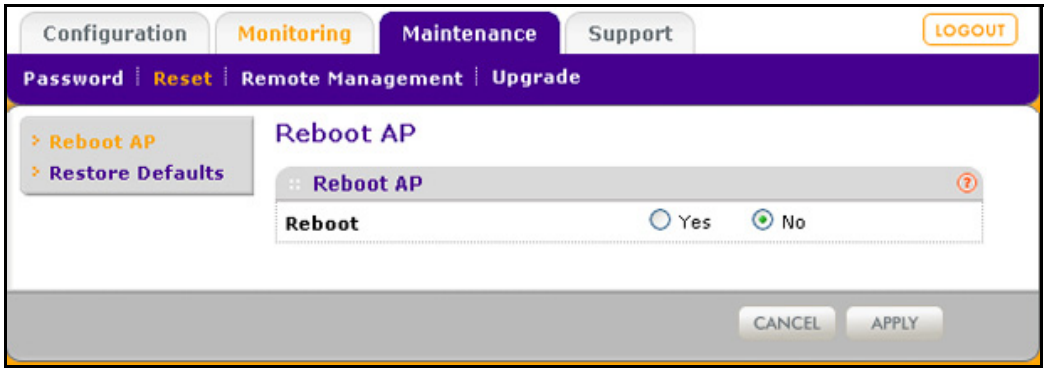


Figure 39.

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**. You should change this password to a more secure password. You cannot change the administrator login name (admin).

The ideal password should contain no dictionary words from any language, and should be 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:

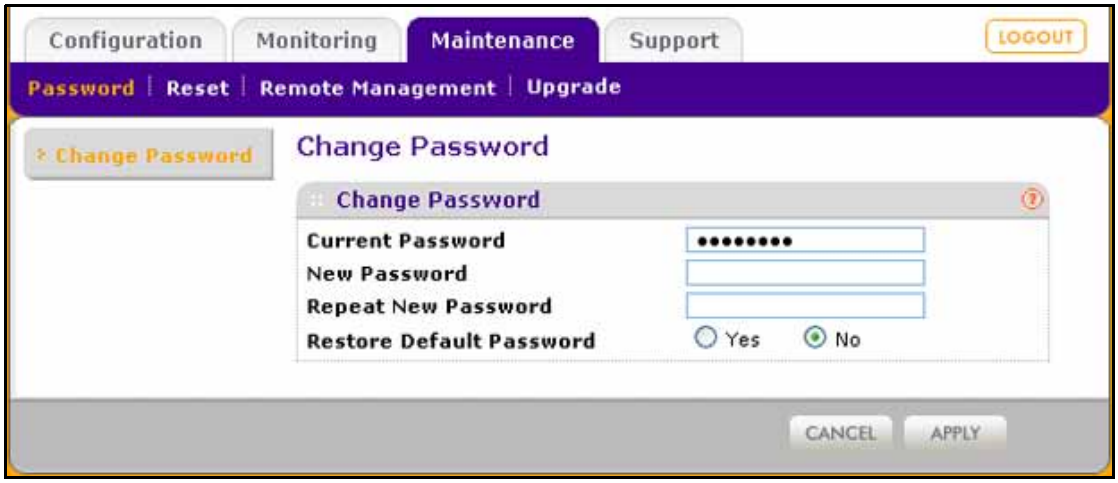


Figure 40.

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 will be **password**. If you have configured a new password, write it down in a secure place.

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:

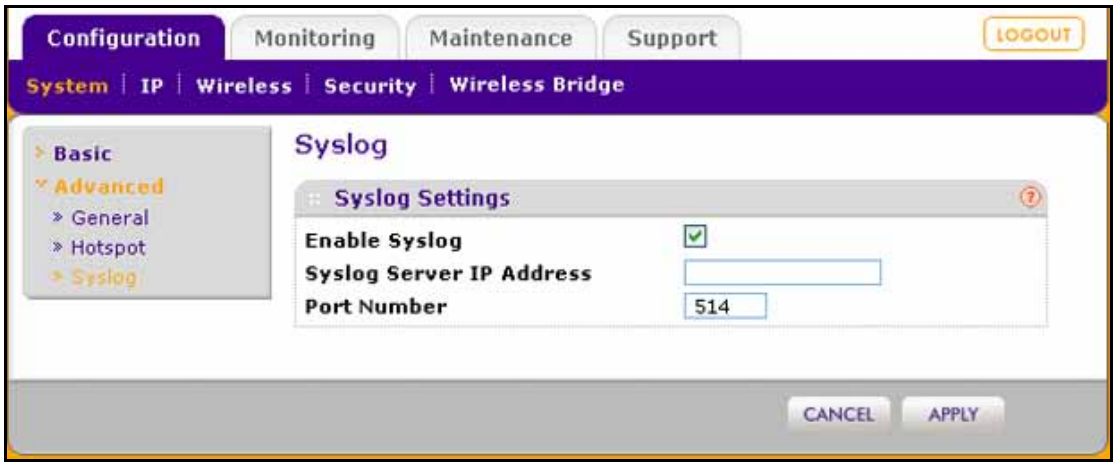


Figure 41.

Specify the settings as explained in the following table:

Table 17. Syslog Settings

Field	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

The wireless access point provides a variety of status and usage information that is discussed in the following sections:

- *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**.

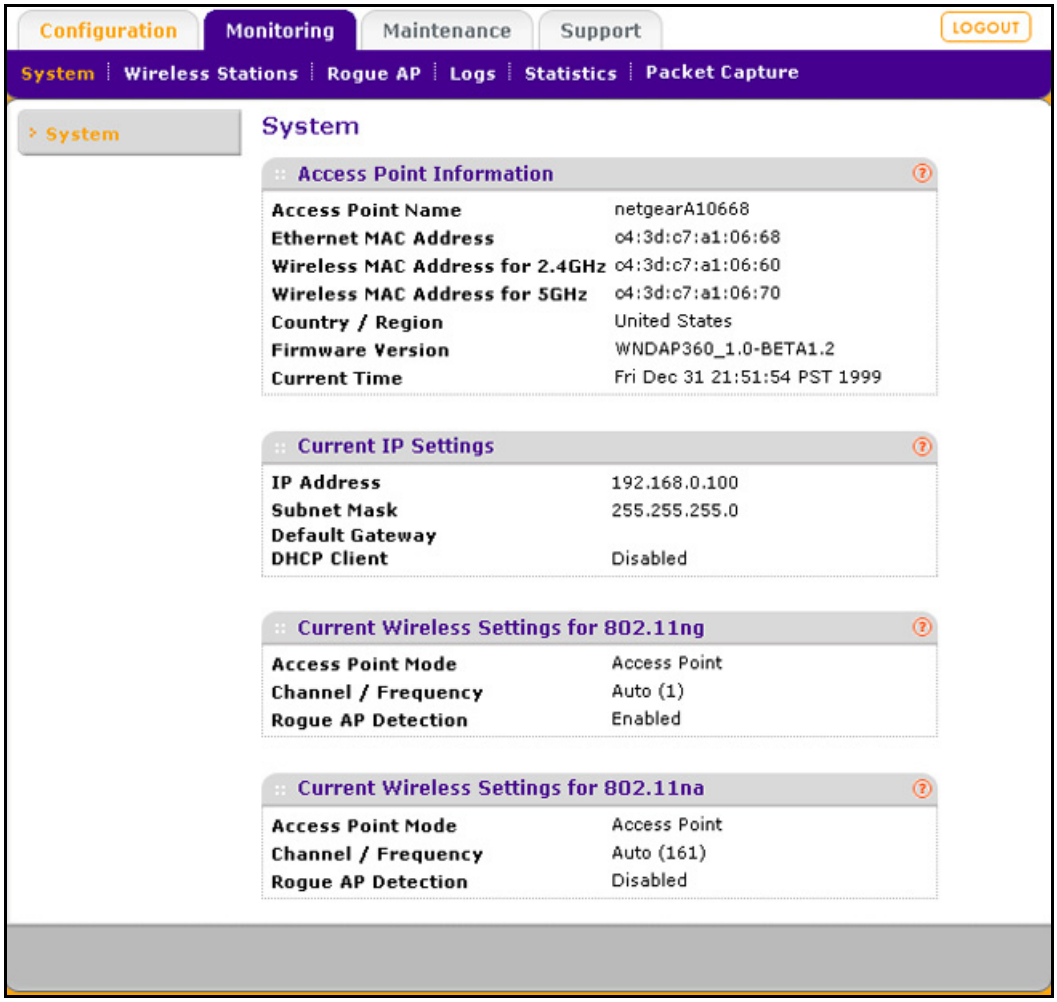


Figure 42.

The following table explains the fields of the System screen:

Table 18. System Screen Fields

Field	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 19.
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.
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 19. **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.
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 19.
Current IP Settings For information about how to change any of these IP settings, see *Configure IP Settings and Optional DHCP Server Settings* on page 21.	
IP Address	The IP address of the wireless access point.
Subnet Mask	The subnet mask for the wireless access point.
Default Gateway	The default gateway for the wireless access point communication.
DHCP Client	Enabled indicates that the current IP address was obtained from a DHCP server on your LAN network. Disabled indicates a static IP configuration.
Current Wireless Settings for 802.11n/g	
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 89.
Channel / Frequency	The channel 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 23.
Rogue AP Detection	Enabled indicates that rogue AP detection is enabled; Disabled indicates that it is not.

Table 18. System Screen Fields (Continued)

Field	Description
Current Wireless Settings for 802.11n/a	
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 89.
Channel / Frequency	The channel the wireless port is using. For information about how to change the channel and frequency, see *Configure 802.11a/na Wireless Settings* on page 27.
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 and 802.11a or 802.11na).

Note: A wireless network can include multiple wireless access points, all using the same network name (SSID). This 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:

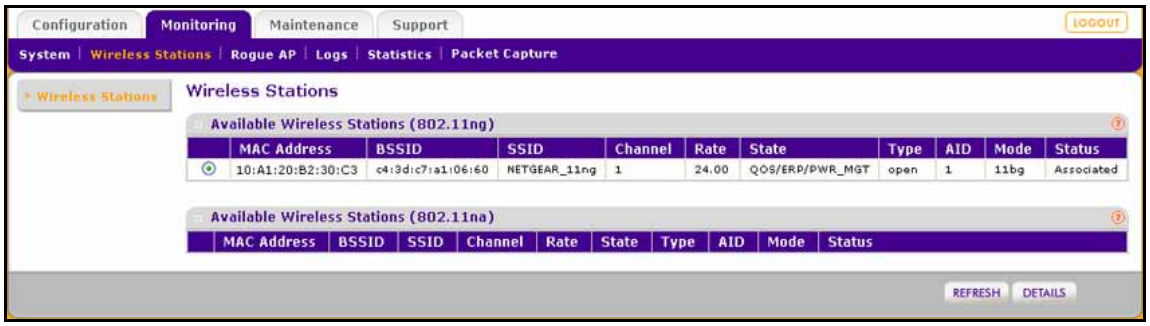


Figure 43.

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**.

There is an Available Wireless Stations table for each selected 2.4-GHz and 5-GHz radio mode. For each radio mode, the Available Wireless Stations table shows for each device the MAC address, BSSID, SSID, channel, rate, state, type, AID, mode, and status. For information about these and more fields, see the following table.

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

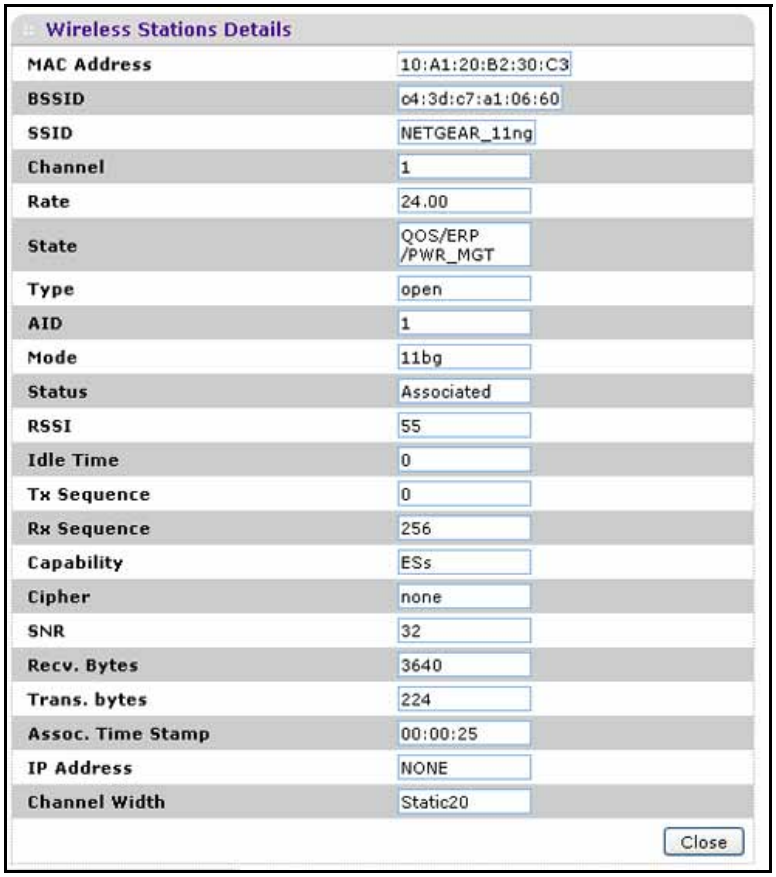


Figure 44.

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

Table 19. Wireless Stations Details Fields

Field	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 capability summary of the wireless station that was detected during association.
Cipher	The cipher that is used by the wireless station 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 log onscreen and save the logs.

➢ **To display the activity log and save it:**

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

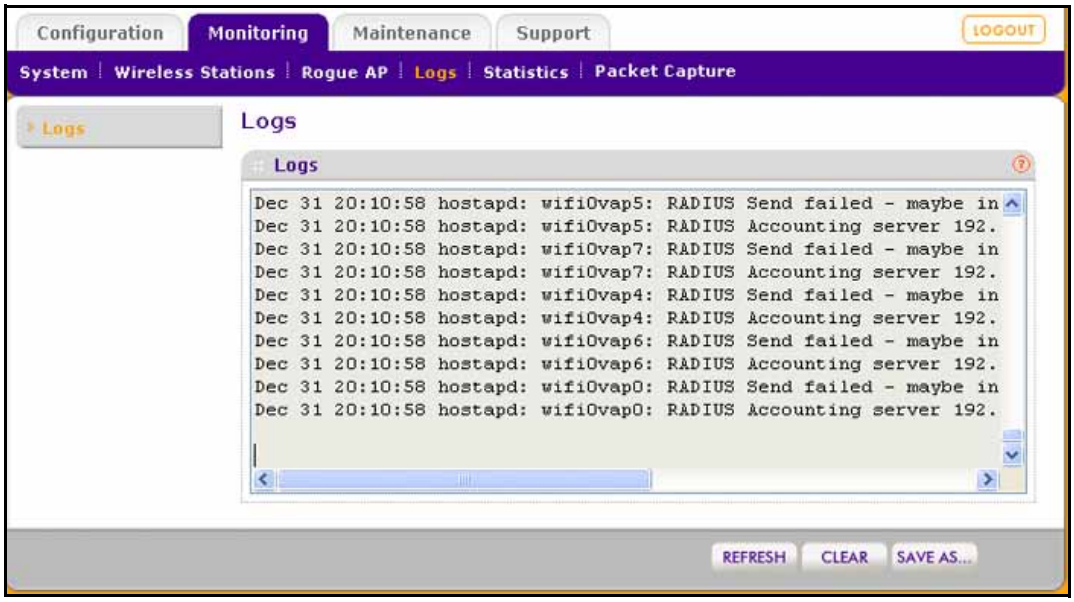


Figure 45.

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

   To update the display on screen, 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**.

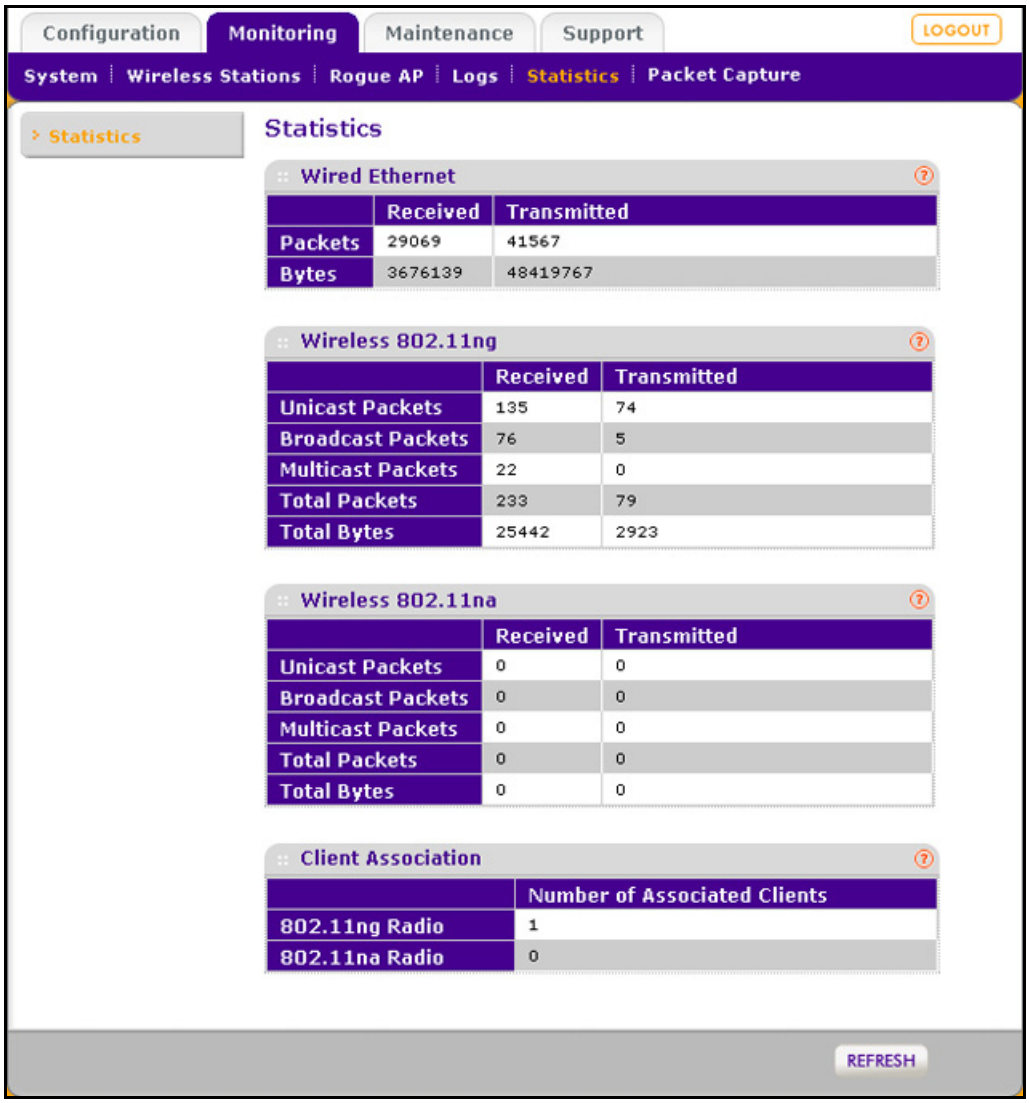


Figure 46.

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

The following table explains the fields of the Statistics screen:

Table 20. Statistics Fields

Field	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.

Table 20. Statistics Fields (Continued)

Field	Description
Wireless 802.11b, Wireless 802.11bg, or Wireless 801.11ng 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.
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.
Wireless 802.11a or Wireless 801.11na The section heading depends on the configured wireless mode. The fields that are displayed are the same as the ones for the 2.4 GHz modes (see the previous rows).	
Client Association	
802.11b Radio, 802.11bg Radio, or 802.11ng Radio	The number of associated clients connected to the radio in the configured wireless modes.
802.11na Radio or 802.11a Radio	

Enable Rogue AP Detection and Monitor Access Points

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 point 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.)

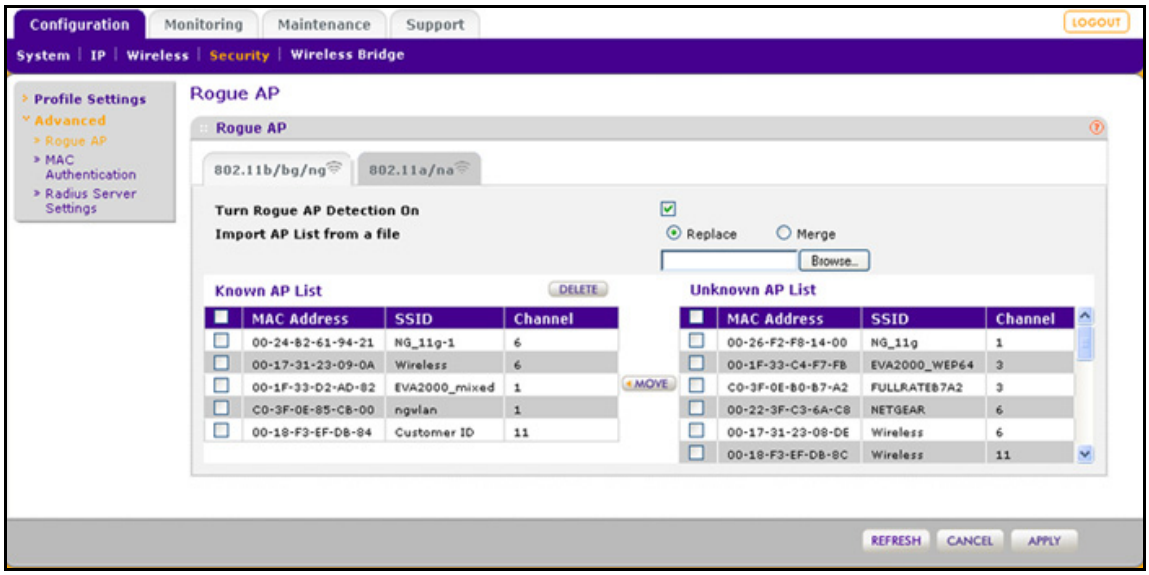


Figure 47.

2. Optionally: To enable and configure rogue AP detection for the 802.11a/na modes, click the **802.11a/na** tab.
3. Click **Refresh** to let the wireless access point discover the access points and populate the Unknown AP List.
4. 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.
5. Click **Move** to transfer the access points from the Unknown AP List to the Known AP List.
6. Select the **Turn Rogue AP Detection On** check box to enable rogue AP detection.
7. 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 with access points replace the existing Known AP List.
   - Select the **Merge** radio button to add the imported list with access points to the existing Known AP List.
2. Click **Browse** and locate the file that contains the list with 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 with 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:

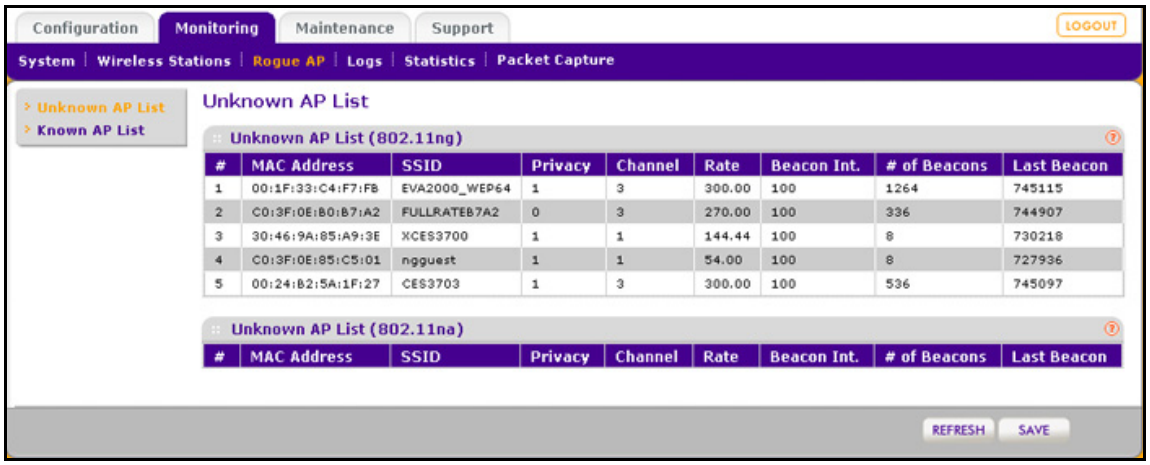


Figure 48.

2. Click **Refresh** to let the wireless access point discover the access points and populate the Unknown AP List for the selected 2.4-GHz and 5-GHz modes.

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

Table 21. Unknown AP List Fields

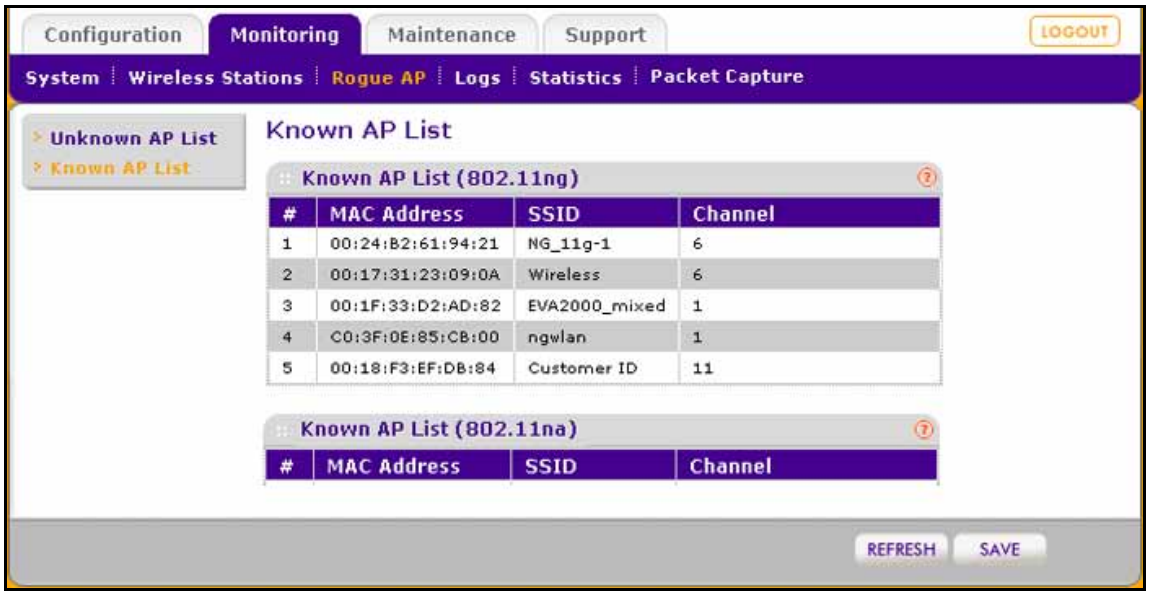
Field	Description
MAC Address	The MAC address of the unknown AP.
SSID	The SSID that the unknown AP is using.
Privacy	Indicates whether or not security is enabled (1 means enabled; 0 means disabled).
Channel	The channel that the unknown AP is using.
Rate	The transmit data rate in Mbps of the unknown the AP.
Beacon Int.	The interval for each beacon transmission in ms.
# of Beacons	The number of beacons transmitted by the unknown AP that the wireless access point has detected.
Last Beacon	The timestamp 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 77).

➢ **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:



2. Click **Refresh** to let the wireless access point discover the access points and populate the Known AP List for the selected 2.4-GHz and 5-GHz modes.

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

Table 22. Known AP List Fields

Field	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 77).

Advanced Configuration

5

This chapter describes how to configure the advanced features of your ProSafe Dual Band Wireless-N Access Point WNDAP360. This chapter includes the following sections:

- *Spanning Tree Protocol and 802.1Q VLAN*
- *Hotspot Settings*
- *Configure Advanced Wireless Settings*
- *Configure Advanced QoS Settings*
- *Configure Wireless Bridging*

Spanning Tree Protocol and 802.1Q VLAN

The advanced General system settings screen allows you to enable the Spanning Tree Protocol (STP) and configure the VLANs.

STP provides network traffic optimization in locations where multiple wireless access points are active.

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

- **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 89). 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:

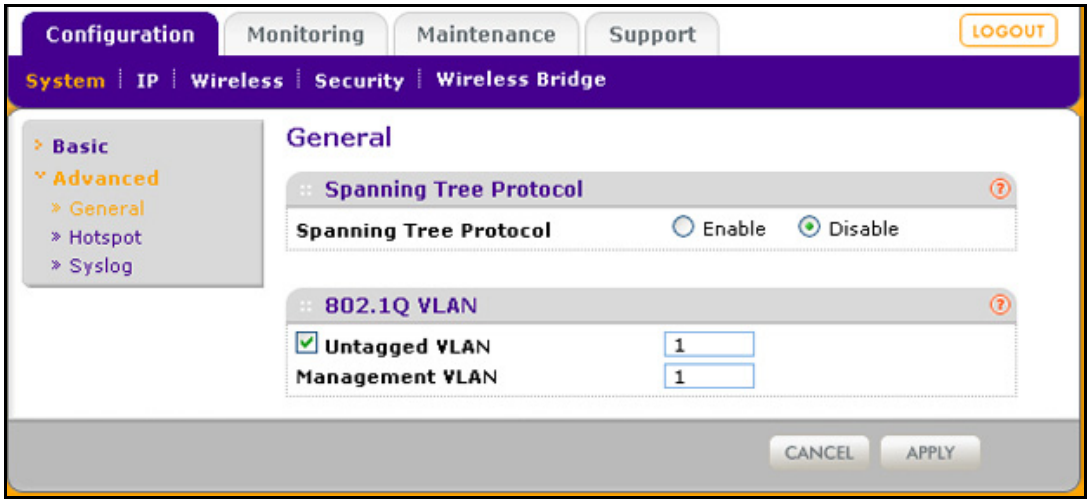


Figure 49.

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

Table 23. STP and VLAN Settings

Field	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.

Table 23. STP and VLAN Settings (Continued)

Field	Description
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 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.

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

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:

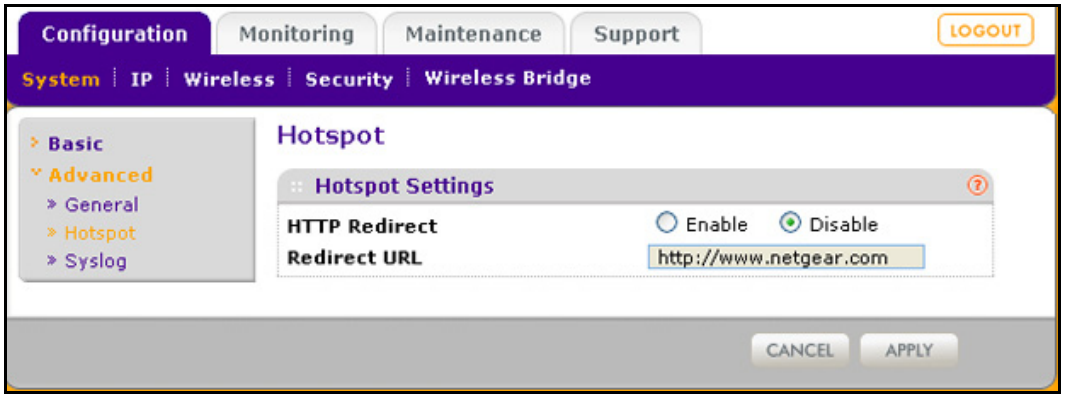


Figure 50.

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

You use the advanced Wireless Settings screen to configure and enable various WLAN settings for 802.11b, 802.11bg, or 802.11ng wireless mode. The active wireless mode is indicated on screen. (For information about how to change the wireless mode, see *Configure Basic Wireless Settings* on page 23.)

The default WLAN settings normally work well. However, you can use these settings to fine-tune the overall performance of your wireless access point for your 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—see the wireless icon that is displayed next to ng.)

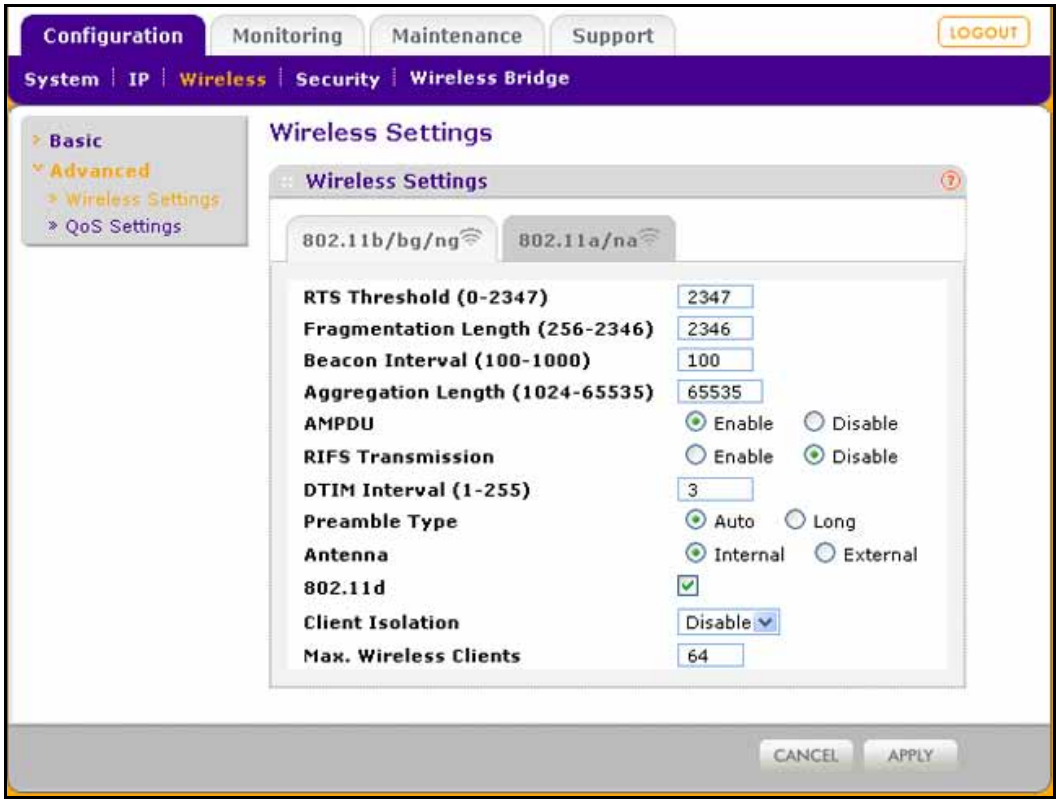


Figure 51.

2. Optionally: 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 24. Advanced Wireless Settings

Field	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.
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 (AMPDU) 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 Aggregated MAC Protocol Data Unit (AMPDU) 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.

Table 24. Advanced Wireless Settings (Continued)

Field	Description
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 settings automatically handles 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.
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 64 clients.

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

Configure Advanced QoS 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 56.

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 56.)

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:

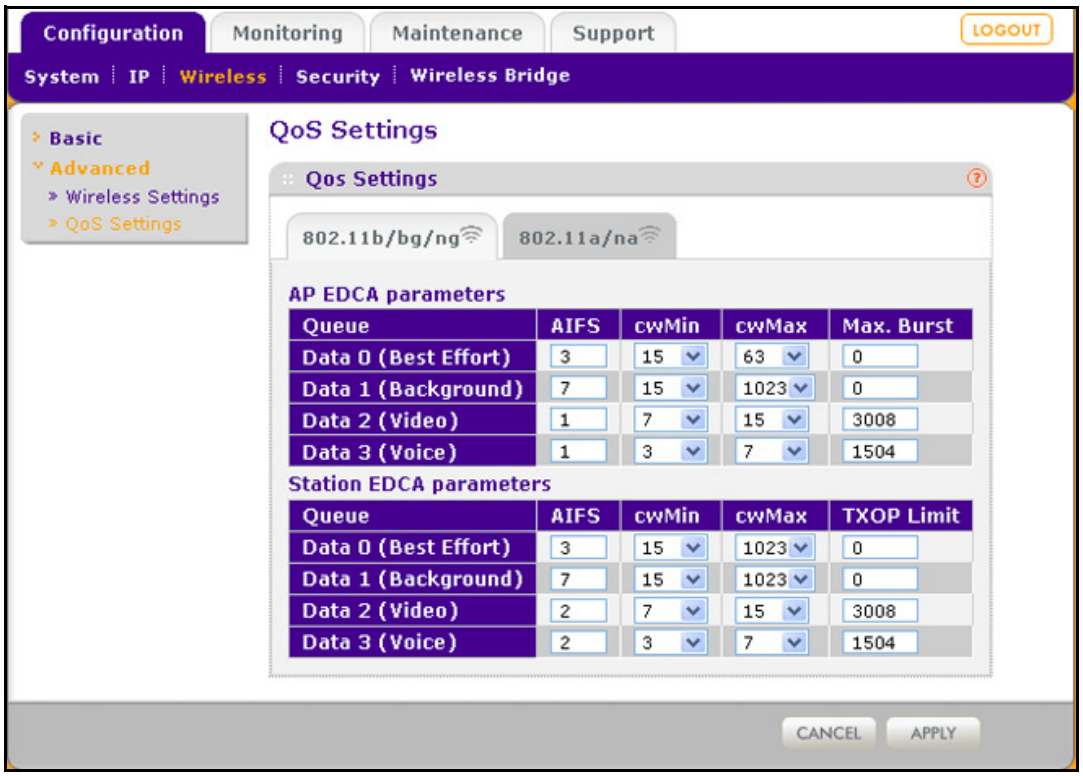


Figure 52.

2. Optionally: 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 25. EDCA Settings

Field	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, or 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, or 1023. The default values are: Data 0: 63; Data 1: 1023; Data 2: 15; Data 3: 7.
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, or 1023. The default values are: Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.

Table 25. EDCA Settings (Continued)

Field	Description
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, or 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 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 90.
- **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 93.
- **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 98.

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 Basic Wireless Settings* on page 23).

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:

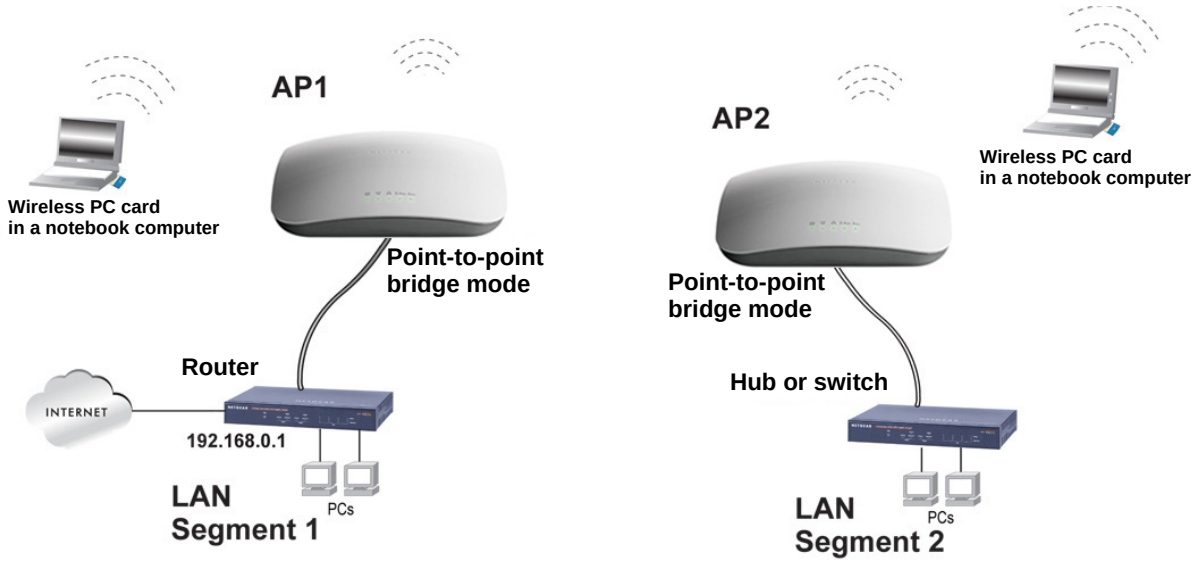


Figure 53.

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

1. Select the **802.11b/bg/ng** or **802.11a/na** tab.
2. 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. 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.
   c. Select the **Wireless Point-to-Point Bridge** radio button. The screen adjusts.

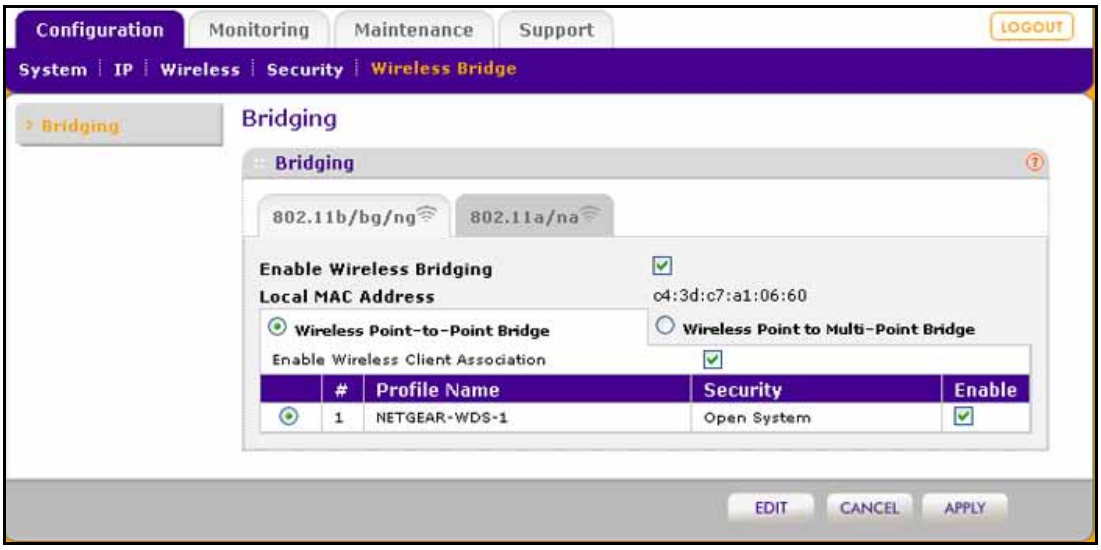


Figure 54.

d. 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.

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

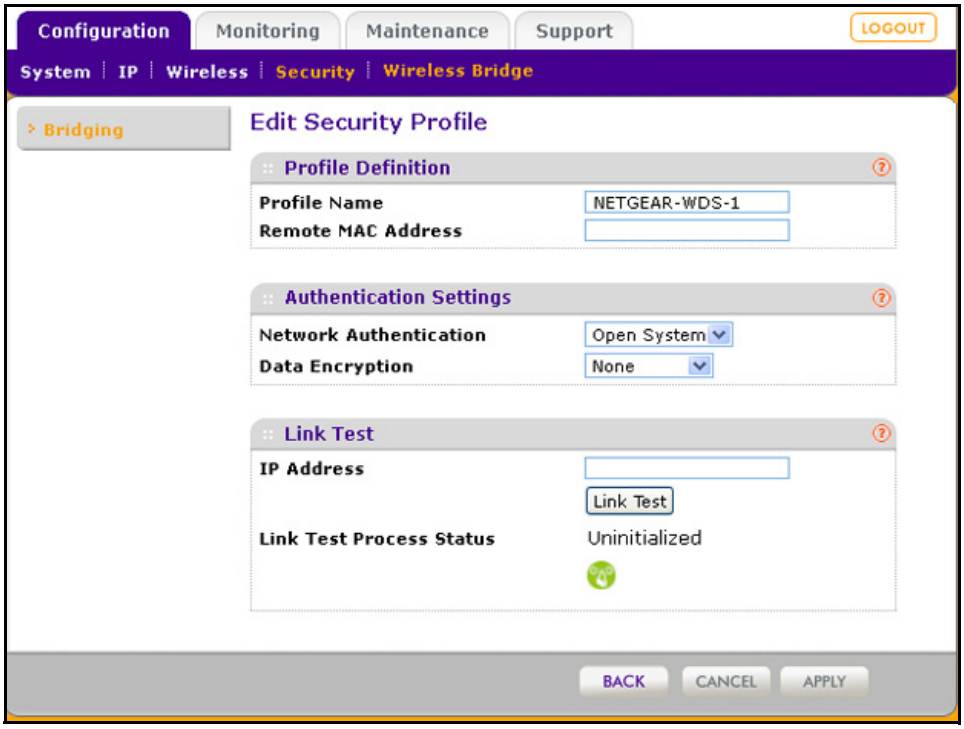


Figure 55.

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

Table 26. Point-to-Point Bridge Profile and Authentication Settings

Field	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 53* on page 90).	
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 or not 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 bits encryption. This mode functions only with other wireless station 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.

Table 26. Point-to-Point Bridge Profile and Authentication Settings (Continued)

Field	Description
Link Test	
IP Address	To verify the connection between the access point and the wireless station that you intend to build a bridge with, enter the IP address of the wireless station, and then click **Link Test**. The Link Test Process Status field displays the results of the test (Uninitialized, In Process, Success, Timed Out, or Failure). **Note:** You should be able to ping the IP address of both APs from a connected client. Failure to ping one of the APs means that the wireless signal is not traversing the bridge. Failure to ping both IP addresses means that the clients is not connected correctly.

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

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

i. Click **Apply** in the Bridging screen to save your point-to-point bridge settings.

3. Configure a second wireless access point (AP2) on LAN Segment 2 (see *Figure 53* on page 90) 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.

4. Configure and verify the following settings for both wireless access points:
   - Verify the LAN network configuration of the wireless access points. Both need to be configured to operate in the same LAN network address range as the LAN devices.
   - Both wireless access points need to use the same channel, authentication mode, and security settings.

5. 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-*multi*point 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-*multi*point bridge mode and AP2 and AP3 function in point-to-point bridge mode:

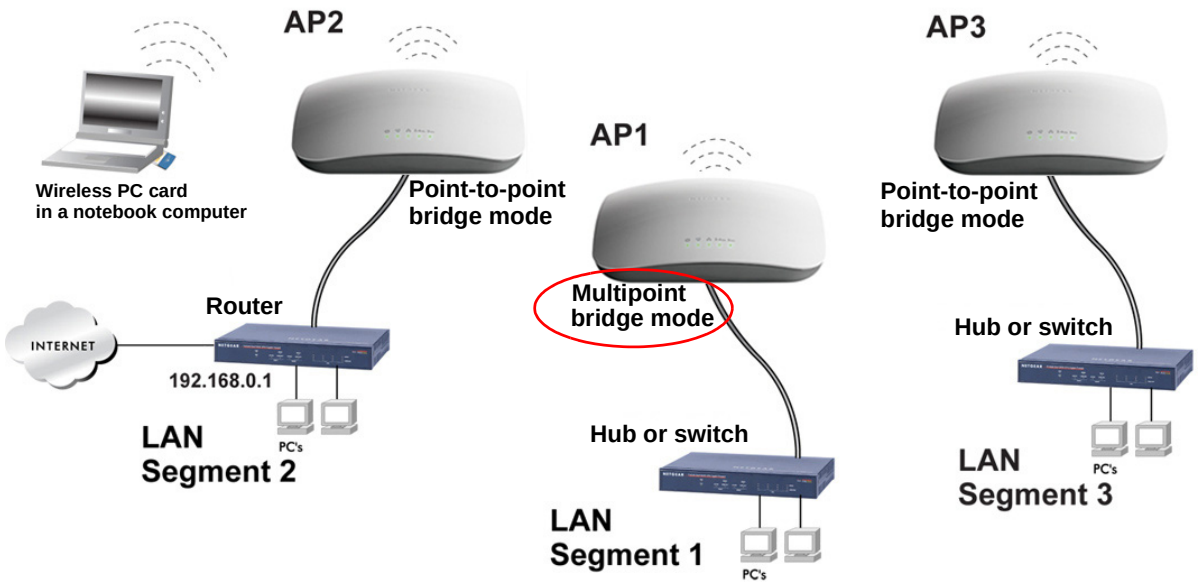


Figure 56.

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

1. Select the **802.11b/bg/ng** or **802.11a/na** tab.
2. 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 c*.)

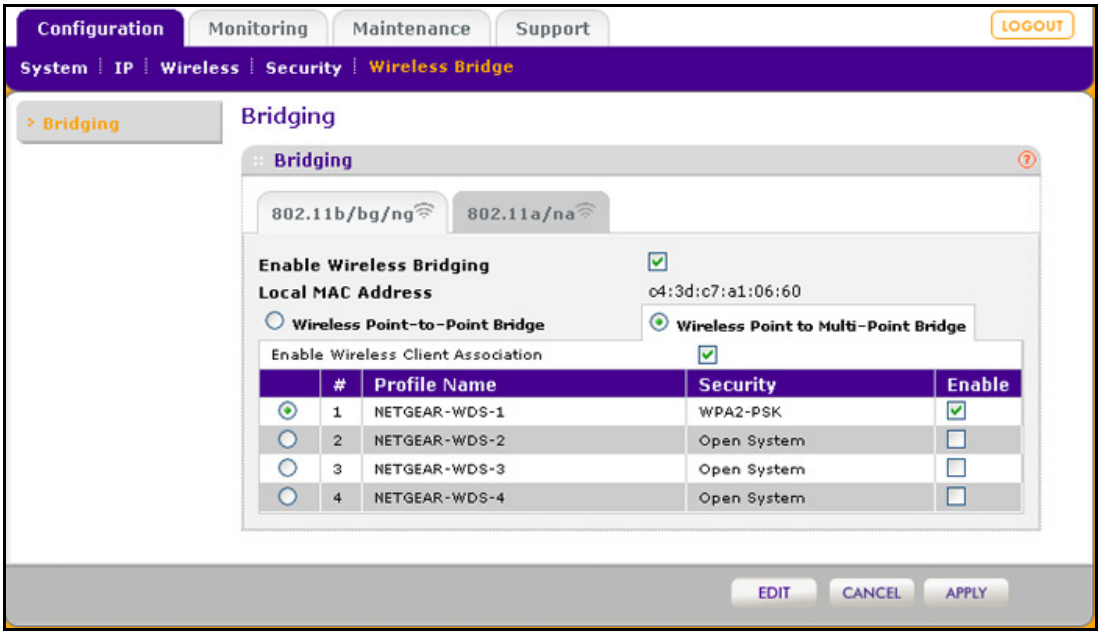


Figure 57.

b. 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.

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

d. 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.

e. Click **Edit** to configure the selected security profile settings. The Edit Security Profile screen displays for the selected security profile. (The following figure contains some examples.)

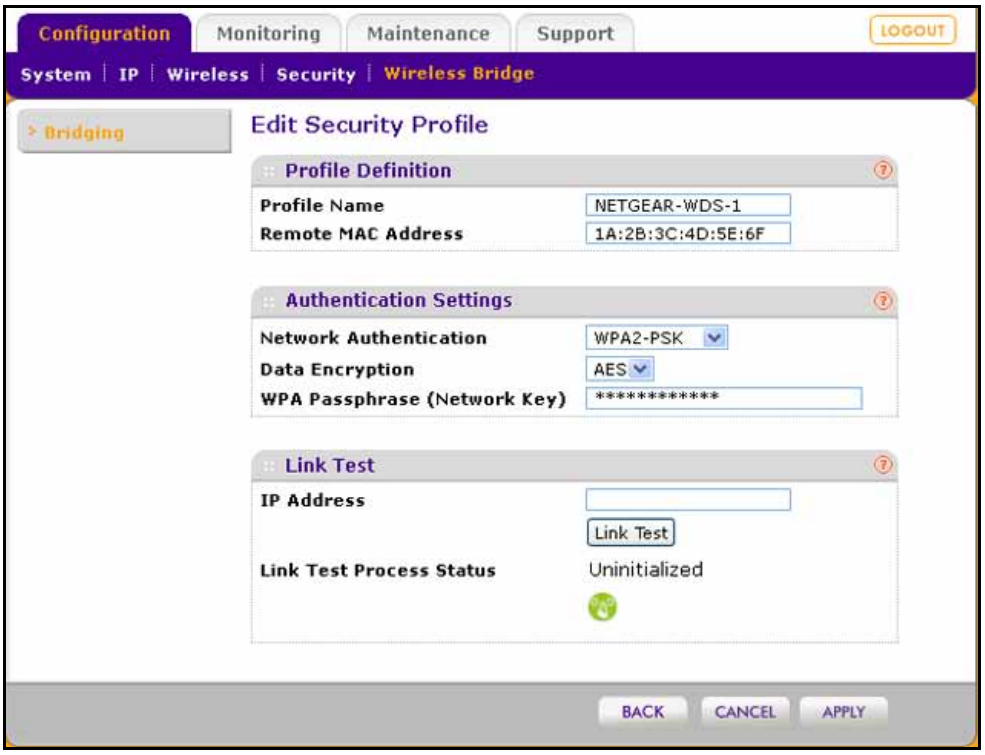


Figure 58.

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

Table 27. Point-to-Multipoint Bridge Profile and Authentication Settings

Field	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 56* on page 94).

Table 27. Point-to-Multipoint Bridge Profile and Authentication Settings (Continued)

Field	Description	
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 or not 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 bits encryption. This mode functions only with other wireless station 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.
Link Test		
IP Address	To verify the connection between the access point and the wireless station that you intend to build a bridge with, enter the IP address of the wireless station, and then click **Link Test**. The Link Test Process Status field displays the results of the test (Uninitialized, In Process, Success, Timed Out, or Failure). **Note:** You should be able to ping the IP address of both APs from a connected client. Failure to ping one of the APs means that the wireless signal is not traversing the bridge. Failure to ping both IP addresses means that the clients is not connected correctly.	

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

h. Repeat *step b* through *step g* 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 56* on page 94).

3. Activate the wireless access point (AP1 on LAN Segment 1 in *Figure 56* on page 94) 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 will 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** in the Bridging screen to activate your point-to-multipoint bridge settings.

4. Configure AP2 on LAN Segment 2 (see *Figure 56* on page 94) in point-to-point bridge mode with the remote MAC address of AP1.

5. Configure AP3 on LAN Segment 3 (see *Figure 56* on page 94) in point-to-point bridge mode with the remote MAC address of AP1.

6. 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) needs to have AP1's MAC address in their Remote MAC Address field.
- All APs need to be on the same LAN, that is, the LAN IP addresses of all APs need to be in the same network as the LAN devices.
- If you use DHCP, all wireless access points need to obtain an IP address automatically (as a DHCP client). For more information, see *Configure IP Settings and Optional DHCP Server Settings* on page 21.
- All wireless access points need to use the same channel, authentication mode, and security settings.

7. 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 PCs 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-*multi*point bridge mode. AP2 requires a security profile for AP1 and another one for AP3:

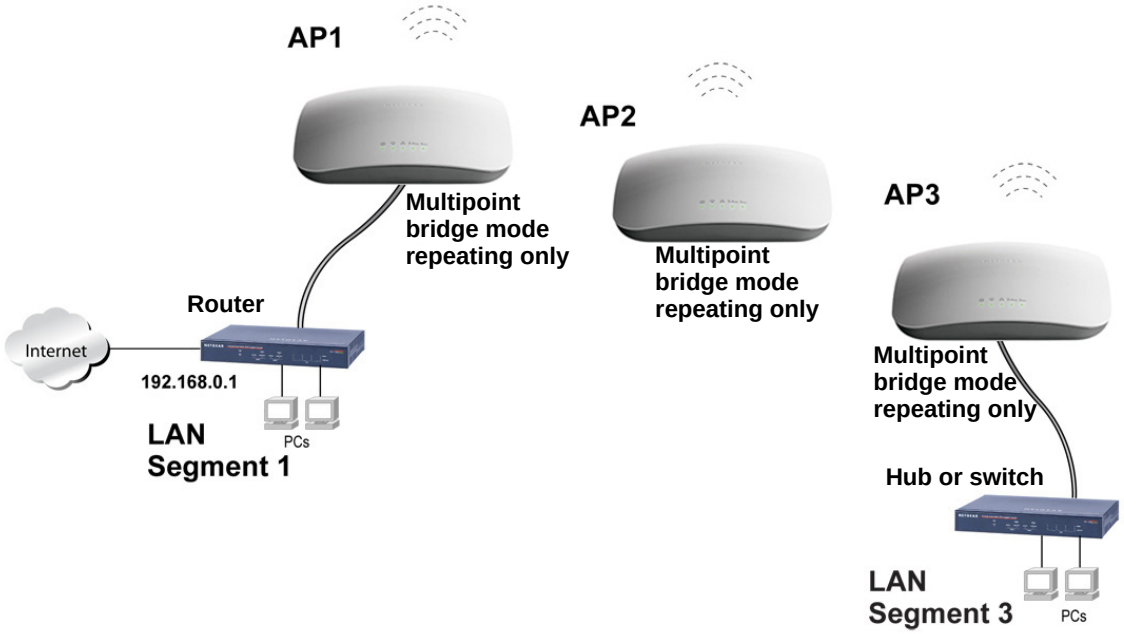


Figure 59.

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

1. Select the **802.11b/bg/ng** or **802.11a/na** tab.
2. 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. 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.
   c. Select the **Wireless Point-to-Multi-Point Bridge** radio button. The screen adjusts.

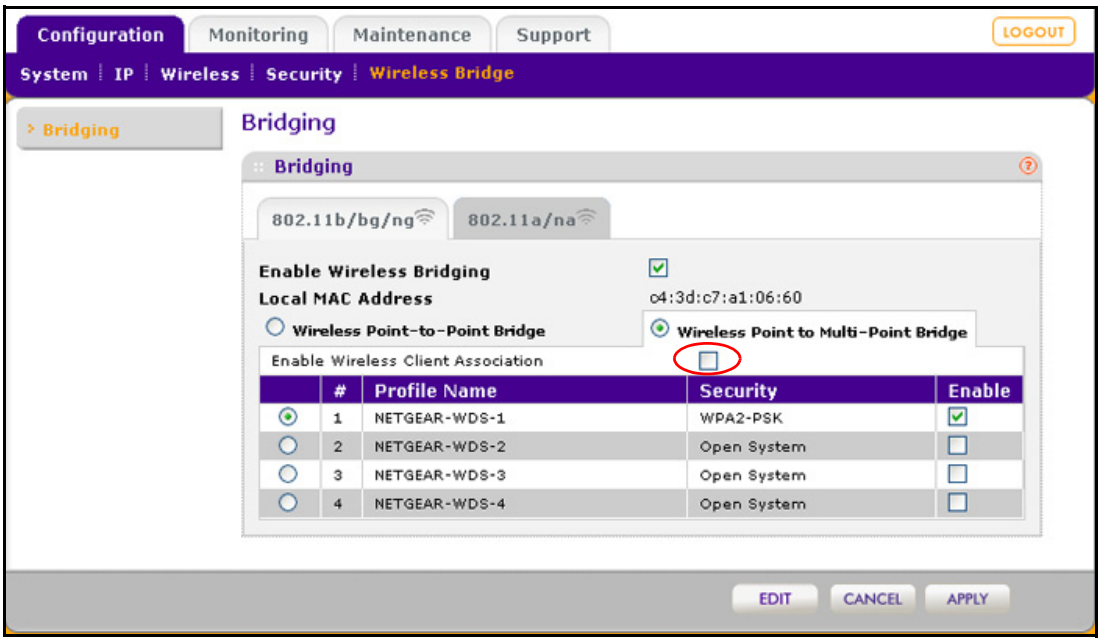


Figure 60.

   d. 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.
   e. Click **Edit** to configure the selected security profile settings. The Edit Security Profile screen displays for the selected security profile. (The following figure contains some examples.)

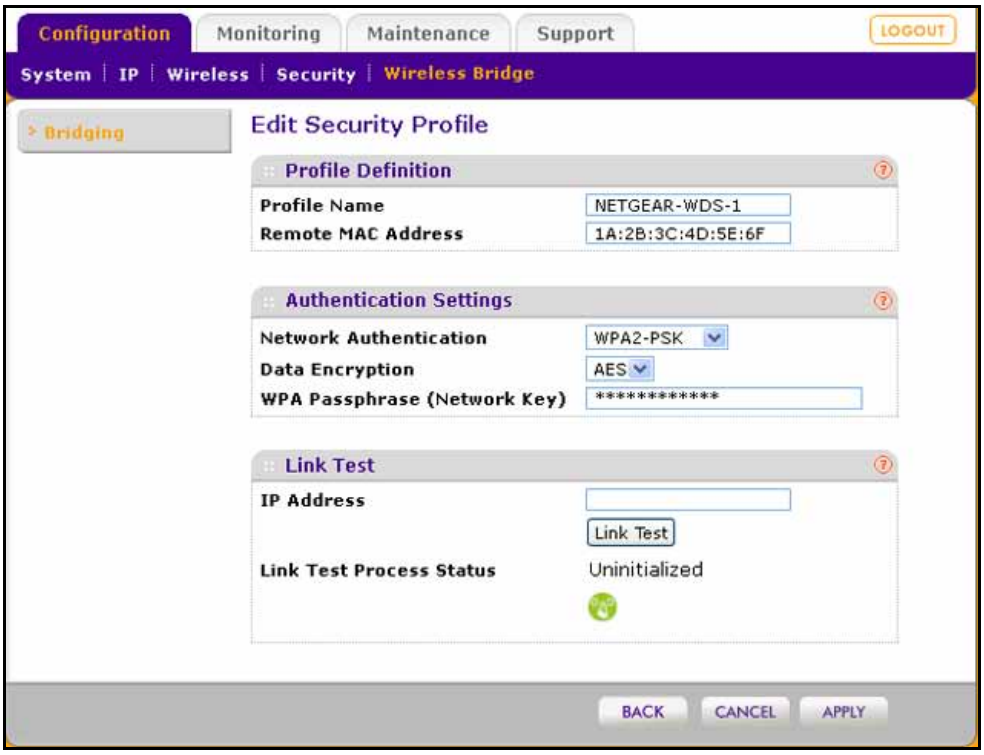


Figure 61.

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

Table 28. Wireless Signal Repeating Profile and Authentication Settings

Field	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 59* on page 98).
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 or not the WPA Passphrase (Network Key) field displays.

Table 28. Wireless Signal Repeating Profile and Authentication Settings (Continued)

Field	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 bits encryption. This mode functions only with other wireless station 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.
Link Test		
IP Address	To verify the connection between the access point and the wireless station that you intend to build a bridge with, enter the IP address of the wireless station, and then click **Link Test**. The Link Test Process Status field displays the results of the test (Uninitialized, In Process, Success, Timed Out, or Failure). **Note:** You should be able to ping the IP address of both APs from a connected client. Failure to ping one of the APs means that the wireless signal is not traversing the bridge. Failure to ping both IP addresses means that the clients is not connected correctly.	

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

h. Repeat *step d* through *step g* 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 59* on page 98).

3. Activate repeater mode on the wireless access point (AP2 in *Figure 59* on page 98):
   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 60* on page 99).

Note: If you do not clear the Enable Wireless Client Association check box, the wireless access point functions in regular point-to-*multi*point 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** in the Bridging screen to activate your repeater settings.
4. Configure AP1 on LAN Segment 1 (see *Figure 59* on page 98) in repeater mode with the remote MAC address of AP2.
5. Configure AP3 on LAN Segment 3 (see *Figure 59* on page 98) in repeater mode with the remote MAC address of AP2.
6. Verify the following for all wireless access points:
   - All APs need to be on the same LAN, that is, the LAN IP addresses of all APs need to be in the same network as the LAN devices.
   - If you use DHCP, all wireless access points need to obtain an IP address automatically (as a DHCP client). For more information, see *Configure IP Settings and Optional DHCP Server Settings* on page 21.
   - All wireless access points need to use the same channel, authentication mode, and security settings.
7. 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 PCs 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-*multi*point bridge mode without client association. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Troubleshooting

6

This chapter provides information about troubleshooting your ProSafe Dual Band Wireless-N Access Point WNDAP360. 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 104.

- Have I connected the wireless access point correctly?

  Go to *Basic Functioning* on page 104.

- 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 105.

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

  Go to *You Cannot Configure the Wireless Access Point from a Browser* on page 106.

- A time-out occurs.

  Go to *When You Enter a URL or IP Address a Time-Out Error Occurs* on page 107.

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

  Go to *Change the Administrator Password* on page 68.

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

  Go to *Restore the Wireless Access Point to the Factory Default Settings* on page 66.

- The date or time is not correct.

  Go to *Problems with Date and Time* on page 108.

The wireless access point provides a packet capture tool that enables you to perform problem diagnoses. For information about how to use this tool, go to *Use the Packet Capture Tool* on page 109.

Basic Functioning

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 IP Settings and Optional DHCP Server Settings* on page 21).
- 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 IP Settings and Optional DHCP Server Settings* on page 21).
- 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.

Troubleshooting a TCP/IP Network Using the Ping Utility

Most TCP/IP terminal devices and routers contain a ping utility that sends an echo request packet to the designated device. The device then responds with an echo reply. You can easily troubleshooting a TCP/IP network by using the ping utility in your computer.

Testing 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 192.168.0.229

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 105.
  - 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.

Testing 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
   ```

   in which **`IP address`** is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as in the previous section 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 19).

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 servers on

the Internet that you specify in the Time Settings screen (see *Configure Basic General System Settings and Time Settings* on page 19). Each entry on the Logs screen is stamped with the date and time of day. Problems with the date and time function can include:

- 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 19).

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:

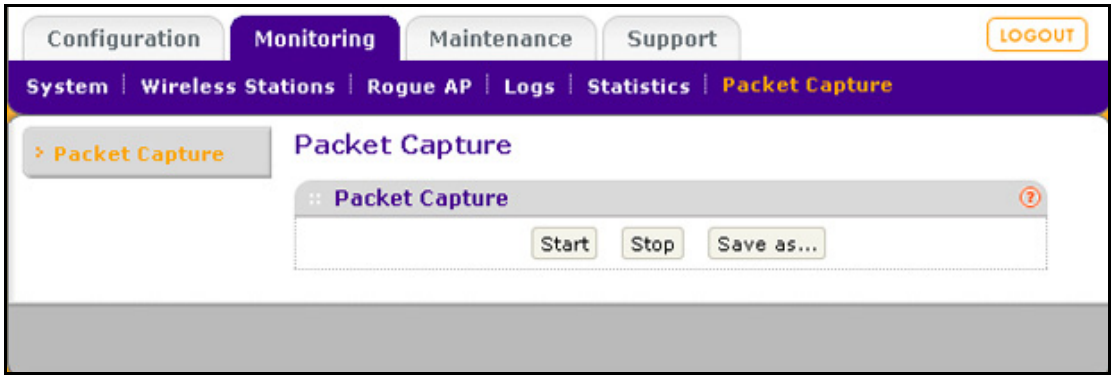


Figure 62.

2. Click **Start** to start capturing wireless packets leaving or entering the wireless access point on the active operating channel. Packets on the 2.4-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 related documentation, factory default settings, and technical specifications for the ProSafe Dual Band Wireless-N Access Point WNDAP360. This appendix includes the following sections:

- *Technical Specifications*
- *Factory Default Settings*

Technical Specifications

Table 29. Technical Specifications WNDAP360

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, 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, 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, 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, and auto-rate capable

Table 29. Technical Specifications WNDAP360 (Continued)

Feature	Description
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, 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, 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, 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, and auto-rate capable
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

Table 29. Technical Specifications WNDAP360 (Continued)

Feature	Description
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 64 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: 0.886 kg (1.95 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 Class B and Class E, CE, and 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 push 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 30. Default Configuration Settings WNDAP360

Feature		Description
Login		
	User login URL	192.168.0.100
	User name (case-sensitive)	admin
	Login password (case-sensitive)	password
Ethernet Connection		
	Static IP address	192.168.0.210
	Ethernet MAC address	See bottom label.
	Port speed	10/100/1000
Local Network (LAN)		
	LAN IP address	192.168.0.100
	Subnet mask	255.255.255.0
	Gateway address	0.0.0.0
	DHCP server	Disabled
	DHCP client	Disabled
	Time zone	USA-Pacific
	SNMP	Disabled
	Spanning Tree Protocol	Disabled
	Secure Shell (SSH)	Enabled
	Secure Telnet	Disabled

Table 30. Default Configuration Settings WNDAP360 (Continued)

Feature		Description
Wireless Local Network (WLAN)		
	Operating mode	Access point, infrastructure mode
	Wireless access point name	netgearxxxxxx where xxxxxx is the last 6 digits of the wireless access point MAC address.
	Wireless communication	Enabled
	11 b/g/n wireless network name (SSID)	NETGEAR_11ng
	Broadcast network name SSID	Enabled
	Security	Disabled (open system)
	Transmission speed	Best[a]
	Country and region	Varies by region
	802.11ng radio frequency channel	Auto
	Output power	Full
	Wireless card access list	All wireless stations allowed
	WMM support	Enabled

a. 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.

Command-Line Reference

B

The ProSafe Dual Band Wireless-N Access Point WNDAP360 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
| |-dhcp>                              --DHCP server
| | |-dns-server                       --DNS server
| | |-gateway                          --default gateway
| | |-ip-address                       --IP range
| | |-lease-time                       --lease time
| | |-status                           --status
| | |-subnet-mask                      --subnet mask
| | |-wins-server                      --WINS server
| |
| |-http-redirect                      --enable HTTP redirection
| |-http-redirect-url                  --HTTP redirection URL
| |-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
| | | | |-extension-protection-spacing --wireless extension protection spacing
| | | | |-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
| | | | |-security-profile>           --create security profile
| | | | | |-1>                        --1st security profile
| | | | | | |-authentication          --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
| | | | | | |
| | | | | |-2>                        --2nd security profile
| | | | | | |-authentication          --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
| | | | | |
| | | | | |-3>                         --3rd security profile
| | | | | | |-authentication            --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
| | | | | |
| | | | | |-4>                         --4th security profile
| | | | | | |-authentication            --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
| | | | | |
| | | | | |-5>                         --5th security profile
| | | | | | |-authentication            --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
| | | | | | |
| | | | | |-6>                        --6th security profile
| | | | | | |-authentication          --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
| | | | | | |
| | | | | |-7>                        --7th security profile
| | | | | | |-authentication          --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
| | | | | |
| | | | | |-8>                       --8th security profile
| | | | | | |-authentication           --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
| | | | | |
| | | | |
| | | | |-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
| | | | | |-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
| | | | |
| | | |
| | | |-5>                           --5 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
| | | | |-extension-protection-spacing --wireless extension protection spacing
| | | | |-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>                      --modify wireless access control (ACL)
| | | | | |-add                         --add wireless access control (ACL)
| | | | | |-del                         --delete wireless access control (ACL)
| | | | |
| | | | |-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
| | | | |-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
| | | | |-security-profile>            --create security profile
| | | | | |-1>                         --1st security profile
| | | | | | |-authentication           --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
| | | | | |
| | | | | |-2>                         --2nd security profile
| | | | | | |-authentication           --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
| | | | | | |
| | | | | |-3>                         --3rd security profile
| | | | | | |-authentication           --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
| | | | | | |
| | | | | |-4>                         --4th security profile
| | | | | | |-authentication           --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
| | | | | | |
| | | | | |-5>                         --5th security profile
| | | | | | |-authentication           --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
| | | | | | |
| | | | | |-6>                         --6th security profile
| | | | | | |-authentication           --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
| | | | | | |
| | | | | |-7>                         --7th security profile
| | | | | | |-authentication           --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
| | | | | |
| | | | | |-8>                       --8th security profile
| | | | | | |-authentication           --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
| | | | | |
| | | | |
| | | | |-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
| | | | | |-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                    --???
| | | | |
| | | |
| | |
| |-ip>                                --set host IP
| | |-address                          --host IP address
| | |-default-gateway                  --IP address of default gateway
| | |-dhcp-client                      --enable dhcp client
| | |-dns-server                       --IP address of DNS server
| |
| |-log>                               --syslog setting
| | |-syslog                           --enable syslog client
```

```
| | |-syslog-server-ip                 --syslog server IP address
| | |-syslog-server-port               --syslog server port number
| |
| |-radius>
| | |-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
| |
| |-remote>                          --enable remote access via SSH
| | |-ssh-port                       --SSH port
| | |-sshd                           --SSH daemon
| | |-telnet                         --enable remote access via Telnet
| |
| |-snmp>                            --SNMP setting
| | |-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
| | |-daylightsaving                 --daylight saving
| | |-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
|-password                            --system password
|-restore-configuration               --restore system configuration
|-restore-default-password            --restore default system password
|-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
| | | | |-knownaplist                 --known access point list
| | | | |-stationlist                 --station list
| | | | |-statistics                  --interface statistics
| | | | |-trusted-stationlist         --trusted station list
| | | | |-unknownaplist               --unknown access point list
| | | |
| | | |-5GHz>                         --5GHz wlan interface settings
| | | | |-configuration               --interface configuration
| | | | |-knownaplist                 --known access point list
| | | | |-stationlist                 --station list
| | | | |-statistics                  --interface statistics
| | | | |-trusted-stationlist         --trusted station list
| | | | |-unknownaplist               --unknown access point list
| | | |
| | |
| |
| |-log                               --system log
| |-system                            --system setting
```

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

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 22 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 Dual Band Wireless-N Access Point WNDAP360 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 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 device is for operation within the 5.150 ~ 5.250 GHz frequency range, and it is restricted to an indoor environment.

- 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.

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 20cm 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 20 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.

Index

Numerics

11a and 11na wireless modes 27
11b, 11bg, and 11ng wireless modes 24
2.4 GHz/5 GHz concurrent operation 9
2.4-GHz antenna, connector for 13
64-bit, 128-bit, and 152-bit WEP 48
802.11d support 86
802.1Q VLAN 8

A

access control, wireless stations 46
access point EDCA parameters 88
access, restricting by MAC address 53
accounting, RADIUS servers 51–52
Active LED
    behavior 17
    description 12
    troubleshooting 105
ActiveX 106
activity log 75
admin password
    changing or restoring 68
    default 113
AES (Advanced Encryption Standard) 38, 49–51
Aggregated MAC Protocol Data Unit (A-MPDU) frames 85
aggregation length 85
AID (associated identifier) 74
AIFS (Arbitration Inter-Frame Spacing) interval 88
antennas
    connecting external antennas 13
    enabling internal or external antennas 86
    external orientation 15
associations, clients 77
authentication
    network 38
    RADIUS servers 51–52
autosensing over Ethernet 10

B

background traffic
    advanced QoS 87
    WMM QoS 56
backing up 64
basic service set (BSS) 39
basic service set identifier (BSSID) 37–38
beacon interval 85
beacons, unknown access points 79
best effort traffic
    advanced QoS 87
    WMM QoS 56
bridging modes, wireless 89
broadcast packets, transmitted and received 77
broadcasting wireless network names (SSIDs)
    802.11a/na modes 28
    802.11b/bg/ng modes 25
    security 37
browsers, recommended 17
BSS (basic service set) 39
BSSID (basic service set identifier) 37–38
bytes, received and transmitted
    Ethernet connection 76
    wireless connection 74

C

capturing packets 109
Carrier Sense Multiple Access (CSMA) 85
Category 5 Ethernet cable 7
channel width (802.11na) 28
channel width and offset (802.11ng) 25–26
channels and frequencies
    defaults 111
    selecting for 802.11a/na modes 28
    selecting for 802.11b/bg/ng modes 25
channels, wireless spacing 15
Clear to Send (CTS) packets 85
CLI command sets 115
clients
    associated, number of 77
    DHCP, enabling 21
    isolation, enabling 86

maximum number 86
NTP, enabling 20
wireless separation, enabling 39, 46
collision detection and collision avoidance, CSMA 85
community names and traps, SNMP 59
compliance 128
electromagnetic 112
notification of 128
concurrent dual-band operation 9
configuration file, backing up or restoring 64
connectors and ports, rear panel 12
CSMA (Carrier Sense Multiple Access) 85
CTS (Clear to Send) packets 85
cwMin (Minimum Contention Window) and cwMax (Maximum Contention Window) values 88

D

data encryption
WEP 48
WPA and WPA2 51
data rates
802.11a mode 29
802.11b/bg modes 26
specifications for all modes 110
date and time, troubleshooting 108
defaults
channels and frequencies 111
DHCP gateway 22
factory settings 66, 112
IP address 17, 113
ISP gateway 21
login password 18, 113
SNMP 59
subnet mask 21, 113
user name 18, 113
DHCP (Dynamic Host Configuration Protocol) client and server 21–23
DNS (Domain Name System) servers 21–23
DTIM (Delivery Traffic Indication Message) interval 85
dual-band concurrent operation 9
dynamic and static VLANs 46
Dynamic Host Configuration Protocol (DHCP) client and server 21–23

E

EDCA (Enhanced Distributed Channel Access) parameters 86
electromagnetic compliance 112
encryption
WEP 48
WPA and WPA2 51
environmental specifications 112
ESS (extended service set) 39
Ethernet cabling requirements 15
external antennas
connecting 13
enabling 86

F

factory default settings 66, 112
firmware
backing up 64
factory defaults 66
restoring from saved file 65
upgrading 62
version, viewing 71
flash memory 61
fragmentation length 85
frequencies and channels
defaults 111
selecting for 802.11a/na modes 28
selecting for 802.11b/bg/ng modes 25
FTP traffic
advanced QoS 87
WMM QoS 56

G

gateways, ISP and DHCP 21–22
generating keys, WEP 48
Gigabit Ethernet (RJ-45) port 13
graphical user interface (GUI)
description 18
troubleshooting 106
guard interval
802.11na 28
802.11ng 26
guides, installation 7

H

hotspot server 83

I

idle time 74
importing known access points 78
infrastructure mode 29
installation guide 7
installation kits 30
installation order 16
interference 15
internal antenna, disabling 86

Internet browsing, troubleshooting 105
IP addresses
default 17, 21, 113
DHCP and DNS servers 21–23
DHCP WINS servers 23
NTP servers 20
RADIUS servers 52
SNMP manager 59
static 113
syslog server 69
TFTP server 64
isolating clients 86

J

Java and Javascript 106

K

key generation, WEP 48
key update, RADIUS servers 53

L

LAN
configuration requirements 15
IP address 113
troubleshooting 105
LAN LED
behavior 17
description 12
troubleshooting 105
LAN path, troubleshooting 107
lease, DHCP 23
LEDs
behavior 17
description 12
troubleshooting 104
legacy 802.1X (wireless security) 45, 48
link test, wireless bridge 93, 96, 101
local MAC addresses 54
location, country and region 19
logging activities 75
logging in 17
login URL, name, and password 113
losing wireless connection 55

M

MAC addresses
Ethernet port 71
known access points 80
restricting access by 37, 53
unknown access points 79
wireless access point 19
wireless card 71
management VLAN 82
management, remote options 58
maximum burst value 88
Maximum Contention Window (cwMax) value 88
maximum number of clients 86
MCS (Modulation and Coding Scheme)
index and data rate 80211na 28
index and data rate 80211ng 25
Minimum Contention Window (cwMin) value 88
Modulation and Coding Scheme (MCS) 25, 28
mounting plate
ceiling 31
wall 33
multicast packets, transmitted and received 77

N

name, wireless access point 19
names, profiles 44
NetBIOS name 19
network
authentication 38
configuration, troubleshooting 108
integrity check 21
Network Time Protocol (NTP), client and server 20

O

open system (no security) 45, 47
operating frequencies 111
order of installation and configuration 16
output power
2.4-GHz transmission 26
5.4-GHz transmission 29

P

package contents 7
packets
capturing 109
received and transmitted 76
passphrase
WEP 48
WPA, WPA2, and mixed mode 38, 51
password
changing or restoring 68
default 18
login 113
physical connections, troubleshooting 108

physical specifications 112
pinging wireless access point 106, 107
placement, wireless equipment 14
PoE (Power over Ethernet) 10, 17
point-to-multipoint bridge
    regular mode 93
    repeating wireless signal 98
point-to-point bridge 90
policy, access control 46
port and connectors, rear panel 12
ports
    RADIUS servers 52
    SNMP manager, traps 59
    syslog server 69
power adapter specifications 112
Power/Test LED
    behavior 17
    description 12
    troubleshooting 104
powersaving, WMM 57
preamble type 86
pre-shared key (PSK), WPA, WPA2, and mixed mode 38, 51
priority queues
    advanced QoS 87
    WMM QoS 56
profiles, security
    creating and configuring 42–46
    description 38
protection spacing (11ng only) 25
PSK (pre-shared key), WPA, WPA2, and mixed mode 38, 51

Q

QoS (Quality of Service)
    advanced 86
    WMM 56

R

radio
    scheduling to turn off 55
    turning off, 2.4 GHz 24
    turning off, 5 GHz 27
RADIUS servers, configuring 51
range guidelines, wireless equipment 14
read-only name, read-write name, SNMP 59
rear panel 12
reauthentication time, RADIUS servers 53
rebooting from web management interface 67
received signal strength indicator (RSSI) 74
redirecting HTTP requests 83
Reduced Interframe Space (RIFS) transmission 85
remote devices, troubleshooting 108
remote MAC addresses 54
remote management, options 58
Request to Send (RTS) threshold 85
Reset button 13, 67, 112
restoring
    factory defaults 66
    password 68
    settings, from saved file 65
restricting access by MAC address 37
RIFS (Reduced Interframe Space) transmission 85
roaming 39
rogue access points, detection of 77
RSSI (received signal strength indicator) 74
RTS (Request to Send) threshold 85
Rx sequence 74

S

Secure Shell (SSH), enabling 60
security lock 13
security profiles
    creating and configuring 42–46
    description 38
security, wireless options 36
separating wireless clients 39, 46
servers, configuring
    DHCP 22
    DNS 21–23
    hotspot 83
    NTP 20
    RADIUS 51
    syslog 69
service set identifiers. *See* SSIDs.
shared key, WEP 45, 47
shared secrets, RADIUS servers 52
show configuration CLI command 61
signal-to-noise ratio (SNR) 74
SMA connectors, external antennas 13
SNMP (Simple Network Management Protocol), configuring 59
software
    backing up 64
    factory defaults 66
    restoring from saved file 65
    upgrading 62
    version, viewing 71
Spanning Tree Protocol (STP), enabling 82
specifications, technical 110

SSH (Secure Shell), enabling 60
SSIDs (service set identifiers)
broadcasting 44
broadcasting and security 37
broadcasting for 802.11a/na modes 28
broadcasting for 802.11b/bg/ng modes 25
matching 29
static and dynamic VLANs 46
station EDCA parameters 88
statistics, traffic 75
STP (Spanning Tree Protocol), enabling 82
streaming media
advanced QoS 87
WMM QoS 56
subnet mask
default 113
DHCP clients 22
wireless access point 21
supported standards 8
syslog 69
system requirements 7

T

tagged VLAN 82
TCP/IP network, troubleshooting 107
technical specifications 110
technical support 2
Telnet, enabling 60
Temporal Key Integrity Protocol (TKIP) 38, 49–51
testing wireless bridge connection 93, 96, 101
TFTP server, upgrade procedure 63
time and time zone
configuring 20
troubleshooting 108
time-out error 107
TKIP (Temporal Key Integrity Protocol) 38, 49–51
TKIP + AES (WPA & WPA2 mixed mode) 49–51
top panel 11
trademarks 2
traffic
advanced QoS 87
patterns, analyzing 109
statistics 75
WMM QoS 56
Transmission Opportunity (TXOP) limit 89
transmission output power
2.4-GHz radio 26
5.4-GHz radio 29
traps and community names, SNMP 59
troubleshooting
basic functioning 104
browser configuration 106
capturing packets 109
date 108
Internet and LAN connection 105
LAN path 107
LEDs 104
network configuration 108
path to remote device 108
physical connections 108
pinging 106, 107
PoE connection 104
power cord 104
TCP/IP settings 105
time and time zone 108
time-out error 107
trusted wireless stations 54
turning off
2.4 GHz radio 24
5 GHz radio 27
scheduling wireless radio 55
Tx sequence 74
TXOP (Transmission Opportunity) limit 89

U

unicast packets
encryption methods 49
transmitted and received 77
untagged VLAN 81
upgrading, software 62
URLs, redirecting 83
user name, default 18, 113

V

VAPs (virtual access points) 86
version, software 71
video traffic
advanced QoS 87
WMM QoS 56
virtual access points (VAPs) 86
VLANs
DHCP server VLAN ID 22
dynamic and static 46
identifiers (IDs) 39, 46
tagged, untagged, and management, enabling 81
VoIP (voice over IP) traffic
advanced QoS 87
WMM QoS 56

W

web browsers, recommended 17
web management interface

description 18
troubleshooting 106

WEP (wired equivalent privacy)
configuring 45, 47
types of encryption 37

WEP legacy 802.1X, configuring 45, 48

Wi-Fi Multimedia (WMM) 10, 56, 57

Wi-Fi protected access (WPA), WPA2, and mixed mode
adapter restrictions 44
PSK (pre-shared key), configuring with 45, 50
RADIUS, configuring with 45, 49
types of encryption 38

WINS servers 23

wired equivalent privacy (WEP)
configuring 45, 47
types of encryption 37

wireless adapters, 802.11b/g and 802.11n 15

wireless bridging modes 89

wireless clients, separating 39, 46

wireless connection, losing 55

wireless equipment, placement and range 14

wireless modes
2.4-GHz band 24
5-GHz band 27

wireless network name (SSID)
broadcasting 44
broadcasting and security 37
broadcasting for 802.11a/na modes 28
broadcasting for 802.11b/bg/ng modes 25
matching 29

wireless radio, turning off
2.4 GHz radio 24
5 GHz radio 27
scheduling 55

wireless security
options 36
settings 45

wireless specifications 110

wireless stations
access control 46
trusted 54

WLAN LED
behavior 17
description 12
troubleshooting 105

WMM (Wi-Fi Multimedia) 10, 56, 57

WPA (Wi-Fi protected access), WPA2, and mixed mode
adapter restrictions 44
PSK (pre-shared key), configuring with 45, 50
RADIUS, configuring with 45, 49
types of encryption 38