



ProSAFE Wireless-N Access Point WNAP210

User Manual



350 East Plumeria Drive
San Jose, CA 95134
USA

November, 2015
202-10474-04

Support

Thank you for purchasing this NETGEAR product. You can visit www.netgear.com/support to register your product, get help, access the latest downloads and user manuals, and join our community. We recommend that you use only official NETGEAR support resources.

Conformity

For the current EU Declaration of Conformity, visit http://kb.netgear.com/app/answers/detail/a_id/11621.

Compliance

For regulatory compliance information, visit <http://www.netgear.com/about/regulatory>.

For the Notification of Compliance statement, visit http://www.netgear.com/images/pdf/Notification_of_Compliance.pdf.

See the regulatory compliance document before connecting the power supply.

Trademarks

© NETGEAR, Inc., NETGEAR and the NETGEAR Logo are trademarks of NETGEAR, Inc. Any non-NETGEAR trademarks are used for reference purposes only.

Revision History

Publication Part Number	Publish Date	Comments
202-10474-04	November 2015	Revised the Support section on this page.
202-10474-03	October 2015	Removed the Notification of Compliance appendix and provided a Notification of Compliance link on this page.
202-10474-02	December 2011	Revised the manual.

Contents

Chapter 1 Getting Started

System Requirements	6
What Is In the Box	6
Hardware Description	7
Front Panel	7
Rear Panel	8

Chapter 2 Installation and Configuration

Wireless Equipment Placement and Range Guidelines	10
Prepare to Install the Access Point	10
Connect to the Access Point	11
Log In to the Access Point	11
Configure LAN Settings	12
Set Basic IP Options	13
IP Settings Fields	14
Set Up and Test Basic Wireless Connectivity	15
Basic Wireless Setting Fields	16
QoS Settings	18
Deploy the Access Point	18
Wall Mount Kit (Optional)	19
Wireless Security Options	20
Security Profiles	21
Profile Definition	21
Network Authentication Settings	22
RADIUS Server Settings	24
Change or Edit a Security Profile	25
Restrict Wireless Access by MAC Address	29

Chapter 3 Management

Change the Password	32
Remote Management	32
Remote Console	34
Management Using Telnet	34
Upgrade the Access Point Firmware	35
Save or Restore the Configuration File	36
Enable the Syslog Server	37
Restore Defaults	37

Chapter 4 Monitoring

System Information	40
Wireless Stations	41
Enable Rogue AP Detection	41
Import a Rogue AP List from a File	42
View and Save AP Lists	43
Create AP Lists Manually	43
Activity Log	44
Network Traffic Statistics	44

Chapter 5 Advanced Configuration

802.1Q VLAN	47
Untagged VLANs	47
Management VLANs	47
Hotspot Settings	48
Advanced Wireless Settings	48
Advanced Wireless Settings Fields	49
Advanced QoS Settings	50
Wireless Bridging and Repeating	51
Point-to-Point Bridge	53
Point-to-Multi-Point Wireless Bridge	54
Wireless Repeater	56
Client Mode	57

Chapter 6 Troubleshooting and Debugging

Troubleshooting with the LEDs	59
All LEDs Are Off	59
LAN LED Is Off	59
WLAN LED Is Off	59
Cannot Connect to the Access Point to Configure It	60
Wireless Access to the Network	60
Time-Out Error for URL or IP Address	60

Appendix A Supplemental Information

Factory Default Settings	63
Technical Specifications	65

Appendix B Command Line Reference

Command Sets	66
--------------------	----

Index

Getting Started

1

The NETGEAR ProSAFE Wireless-N Access Point WNAP210 is the basic building block of a wireless LAN infrastructure. It provides connectivity between Ethernet wired networks and radio-equipped wireless computers, wireless devices, print servers, and other devices.

This chapter covers the following topics:

- *System Requirements*
- *What Is In the Box*
- *Hardware Description*

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

System Requirements

Before installing the access point, make sure that your system has the following:

- 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 100–120 V, 50–60 Hz AC power source
- A web browser for configuration such as Microsoft Internet Explorer 5.0 or later, or Mozilla 3.0 or later
- At least one computer with the TCP/IP protocol installed
- 802.11b/g- or 802.11b/g-compliant devices

What Is In the Box

The product package should contain the following items:

- ProSAFE Wireless-N Access Point WNAP210
- Power adapter and cord (12V DC, 1.0A)
- Straight-through Category 5 Ethernet cable
- *Product Installation Guide*
- *Resource CD*, which includes this manual
- Vertical stand feet (2)
- Wall-mount kit made up of brackets (2) 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 *Product Installation Guide* along with the original packing materials, and use the packing materials to repack the 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>.

Hardware Description

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

Front Panel

The front hardware functions are described in the following figure and table.

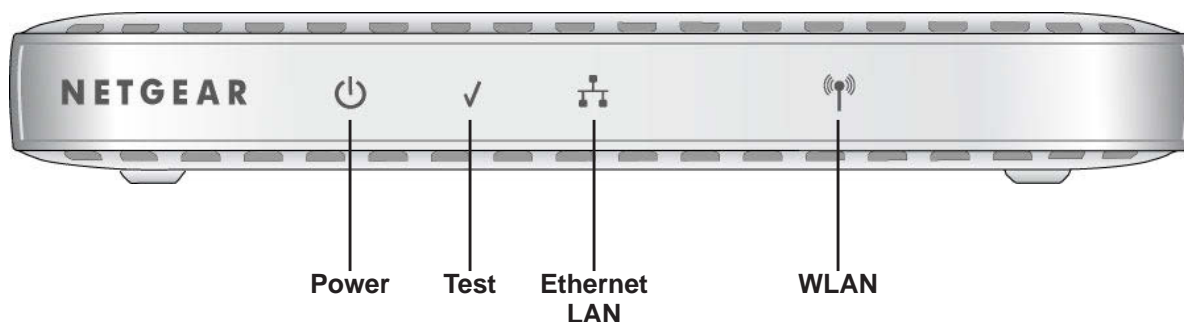






Figure 1. Front view

The following table explains the LEDs:

Table 1. Front panel LEDs

LED	Description
Power 	<ul style="list-style-type: none"> • Off. Power is off. • On. Power is on.
Test 	<p>Blinking. The device is running a self-test or is loading software. This LED might blink for a minute before going off. If it continues to blink, it indicates a system fault.</p>
Ethernet LAN 	<ul style="list-style-type: none"> • Off. A 10 Mbps link or no link is detected. • Amber. A 10/100 Mbps link is detected. • Green. A 1000 Mbps link is detected.
WLAN 	<p>Blinking (blue). Wireless activity has been detected.</p>

Rear Panel

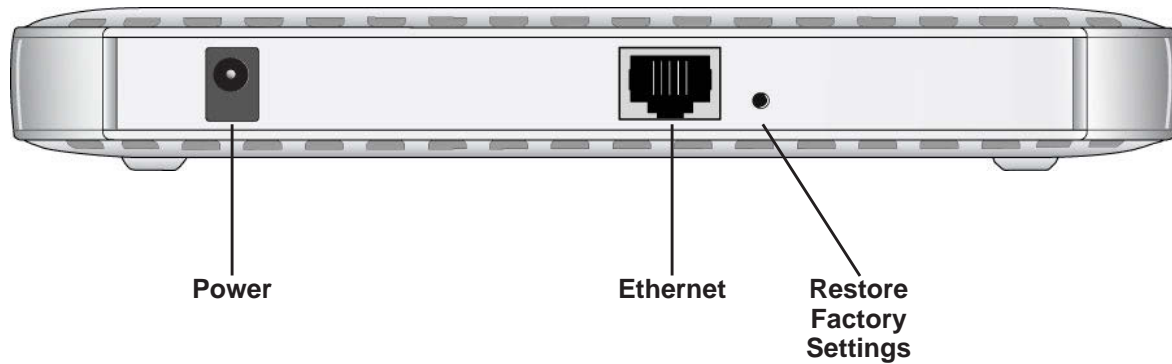


Figure 2. Rear panel

The access point rear panel functions are described in the following list:

- Power socket. This socket connects to the 12V 1.0A power adapter.
- RJ-45 Ethernet port. Use the Ethernet RJ-45 port to connect to an Ethernet LAN through a device such as a hub, switch, router, or PoE switch.
- Restore Factory Settings button. This button restores the access point to the factory default settings.

This chapter describes how to set up your access point for wireless connectivity to your LAN. This basic configuration will enable computers with 802.11b/g/n wireless adapters to connect to the Internet, or access printers and files on your LAN. This chapter covers the following topics:

- *Wireless Equipment Placement and Range Guidelines*
- *Prepare to Install the Access Point*
- *Connect to the Access Point*
- *Log In to the Access Point*
- *Configure LAN Settings*
- *Set Basic IP Options*
- *Set Up and Test Basic Wireless Connectivity*
- *QoS Settings*
- *Deploy the Access Point*
- *Wireless Security Options*
- *Security Profiles*
- *Restrict Wireless Access by MAC Address*

You need to prepare these three things before you can establish a connection through your wireless access point:

- A location for the access point that conforms to the guidelines in the following section, *Wireless Equipment Placement and Range Guidelines* on page 10.
- The wireless access point connected to your LAN through a device such as a hub, switch, router, or cable or DSL gateway.
- One or more computers with correctly configured 802.11b/g/n wireless adapters.

Wireless Equipment Placement and Range Guidelines

The operating distance or range of your wireless connection can vary significantly based on the physical placement of the 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 access point. For complete performance specifications, see [Appendix A, Supplemental Information](#).

For best results, place your access point:

- Near the center of the area in which your computers and wireless devices 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 computers, microwaves, and 2.4 GHz cordless phones.
- Away from large metal surfaces.

A wall-mount kit is provided with your access point. For installation instructions, see [Wall Mount Kit \(Optional\)](#) on page 19.

If using multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is five channels (for example, use Channels 1 and 6, or 6 and 11).

The time it takes to establish a wireless connection can vary depending on both your security settings and placement. Some types of security connections can take slightly longer to establish and can consume more battery power on a notebook computer.

Prepare to Install the Access Point

Before installing the access point, you should make sure that your Ethernet network is up and working. You will be connecting the access point to the Ethernet network so that computers with 802.11b/g/n wireless adapters will be able to communicate with computers on the Ethernet network. For this to work correctly, you should verify that you have met all of the system requirements, shown in [System Requirements](#) on page 6.

Connect to the Access Point

Tip: Before mounting the access point in a high location, set up and test the access point to verify wireless network connectivity.

➤ To connect the access point:

1. Prepare a computer with an Ethernet adapter. If this computer is already part of your network, record its TCP/IP settings.
2. Turn on your computer and configure it with a static IP address of 192.168.0.210 and a subnet mask of 255.255.255.0.
3. Connect an Ethernet cable from the access point to the computer.
4. Connect the power adapter to the access point, and verify the following:
 - The Power LED goes on.
 - The Ethernet LAN LED is lit when the access point is connected to a powered-on computer.
 - The WLAN LED is blinking.

Log In to the Access Point

The access point is set by default with the IP address of 192.168.0.236 with DHCP disabled.

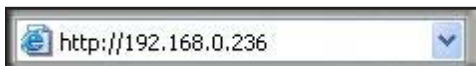
If you log in using the default IP address, the computer you use to connect to the access point has to be set up with an IP address in the range 192.168.0.0 to 192.168.0.255 and a subnet mask of 255.255.255.0.

If DHCP is enabled, there are two methods you can use to connect to the access point after the DHCP server on your network assigns it a new IP address.

- If your access point is to be deployed on a local network, you can enter the NetBIOS name in your web browser. The default wireless access point name is **netgearxxxxxx**, where xxxxxx represents the last 6 bytes of the MAC address. The MAC address is printed on the product label. (Using the NetBIOS naming convention to access your router across several network segments is known to be unreliable.)
- Reserve an IP address (based on the access point's MAC address) on the DHCP server. That way, if your router is deployed across several segments, you can configure the access point with a static IP address, which you can always use to log in to make future configuration changes.

➤ To log in using the default IP address:

1. Open a web browser such as Mozilla Firefox or Internet Explorer.
2. Connect to the access point by entering the default address of **http://192.168.0.236** into your browser.



3. The login screen displays. Enter **admin** for the user name and **password** for the password, both in lower case letters.
4. Click **Login**.

Your web browser should automatically find the access point and display the General screen.

Configure LAN Settings

When you log in, the General screen displays:



➤ To configure the LAN settings:

1. Enter the access point name.

This unique name is the access point NetBIOS name. The access point name is printed on the rear label of the access point. The default is **netgearxxxxxx**, where xxxxxxx represents the last 6 digits of the access point MAC address. You can replace the default name with a unique name up to 15 characters long.

2. From the Country/Region drop-down list, select the region where the access point will be used (the country/region is not configurable in the United States but is configurable in the rest of the world). Click **Apply**.

Note: If your country or region is not listed, check with NETGEAR support.

3. Select **Configuration > System > Basic > Time**.

The screenshot shows the web interface of the ProSAFE Wireless-N Access Point WNAP210. The 'Configuration' tab is active, and the 'Time' settings page is displayed. The 'Time Settings' section includes the following fields:

- Time Zone:** A drop-down menu set to 'USA-Pacific'.
- Current Time:** Displays 'Fri Dec 31 16:31:38 PST 1999'.
- NTP Client:** Radio buttons for 'Enable' (selected) and 'Disable'.
- Use Custom NTP Server:** An unchecked checkbox.
- Hostname / IP Address:** A text field containing 'time-b.netgear.com'.

4. Adjust the following fields:

- **Time Zone.** From the drop-down list, select the local time zone for your access point from a list of all available time zones. The default is USA-Pacific. The access point will get the current time from the connecting computer.
- **NTP Client.** Enable the NTP client to synchronize the time of the access point with an NTP server. The default is Enable.

Note: You need an Internet connection to get the current time using an NTP client.

- **Use Custom NTP Server.** Select this check box if you have a custom NTP server. The default is not selected.
- **Hostname / IP Address.** Enter the host name or the IP address of the custom NTP server. The default is time-b.netgear.com.

5. Click **Apply**.

6. Specify the IP settings as described in the following section.

Set Basic IP Options

Enter the basic IP settings for your access point on this screen. The default settings work in most cases. However, if your access point is part of a more complex LAN network, then modify these settings to meet the requirements of your network.

➤ To configure the basic IP settings of your access point:

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

The screenshot shows the web interface of the ProSAFE Wireless-N Access Point WNAP210. At the top, there are tabs for Configuration, Monitoring, Maintenance, and Support, with a LOGOUT button. Below these is a navigation bar with System, IP, Wireless, Security, and Wireless Bridge. The IP Settings page is displayed, featuring a sidebar with a link to IP Settings. The main content area has a title 'IP Settings' and a sub-header 'IP Settings'. It includes a DHCP Client toggle set to 'Disable' (with 'Enable' as an option). Below this are input fields for IP Address (192.168.0.236), IP Subnet Mask (255.255.255.0), Default Gateway, Primary DNS Server, and Secondary DNS Server.

2. If necessary, edit the IP address fields described in *IP Settings Fields* on page 14.
3. Click **Apply** to save your basic IP settings.

If you change the default subnet of the LAN IP address, you will be disconnected from the access point user interface. To reconnect, reconfigure your computer with a static IP address within the new LAN IP subnet.

By default, the access point is set with the DHCP client disabled. If your network uses dynamic IP addresses, you need to change this setting.

IP Settings Fields

The following fields are available on the IP Settings screen.

- **DHCP Client.** By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you enable DHCP, the wireless access point gets its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the access point to your LAN.
- **IP Address.** Enter the IP address of your access point. The default IP address is 192.168.0.236. To change it, enter an unused IP address from the address range used on your LAN; or enable DHCP.
- **IP Subnet Mask.** The access point automatically calculates the subnet mask based on the IP address that you assign. Otherwise, you can use 255.255.255.0 (the default) as the subnet mask.
- **Default Gateway.** Enter the IP address of the gateway for your LAN. For more complex networks, enter the address of the router for the network segment to which the access point is connected. The default is 0.0.0.0.
- **Primary DNS Servers.** This is the IP address for the primary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.
- **Secondary DNS Servers.** This is the IP address for the secondary Domain Name Server used by stations on your LAN. The default is 0.0.0.0.

Set Up and Test Basic Wireless Connectivity

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

Note: If you connect wirelessly to the access point and you change the SSID, channel, or security profile settings, you will lose your wireless connection when you click Apply. To avoid this situation, you can use a LAN connection to set up the access point.

➤ **To set up and test basic wireless connectivity:**

1. Select **Configuration > System**. Verify that the correct country/region in which the wireless interface will operate has been selected.
2. Click **Apply** to save any changes.
3. Select **Configuration > Wireless**, and the following screen displays:

The screenshot shows the 'Wireless Settings' page in the Netgear configuration utility. The left sidebar has a tree view with 'Basic' expanded, showing 'Wireless Settings', 'QoS Settings', and 'Advanced'. The main content area is titled 'Wireless Settings' and shows the '802.11b/bg/ng' tab selected. The settings are as follows:

Setting	Value
Wireless Mode	2.4GHz Band
Turn Radio On	<input checked="" type="checkbox"/>
Wireless Network Name (SSID)	NETGEAR_11ng
Broadcast Wireless Network Name (SSID)	<input checked="" type="radio"/> Yes <input type="radio"/> No
Channel / Frequency	Auto
MCS Index / Data Rate	Best
Channel Width	40 MHz
Guard Interval	Auto
Output Power	Full

4. Ensure that the auto channel (default) feature is selected for your network. This feature selects a channel that has the least interference.

You don not need to change the wireless channel unless you notice interference or are near another wireless access point. Select a channel that is not being used by any other wireless networks within several hundred feet of your access point.

Note: If you select a wireless mode option and other settings on this screen are disabled, then you have to select the **Turn Radio On** check box to enable options on this screen.

5. Click **Apply** to save any changes.
6. Select **Security**. For initial configuration and testing, the Security field for Profile 1 (the default profile) is set to Open System and the SSID is set to NETGEAR_11ng (for information about how to configure a profile, see [Security Profiles](#) on page 21).

Note: *The SSID of any wireless client has to match the SSID you configured in the access point. If they do not match, you cannot get a wireless connection.*

7. Click **Apply** to save any changes.
8. Configure and test your remaining wireless clients for wireless connectivity.
Check that they have a wireless link and can obtain an IP address by DHCP from the access point. Then you can configure the wireless security.

Basic Wireless Setting Fields

The following fields are available in the Wireless Settings screen:

Wireless Mode

The default is 11ng. The options are:

- **11b.** All 802.11b wireless stations can be used. (The 802.11g wireless stations can still be used if they can operate in 802.11b mode.)
- **11bg.** Both 802.11b and 802.11g wireless stations can be used.
- **11ng.** All 11b, 11g, and 11ng wireless stations can be used. This is the default. If you select this option, then two additional options, Channel Width and Guard Interval, display.

Turn Radio On

On by default. You can also turn off the radio to disable access through this device. This can be helpful for configuration, network tuning, or troubleshooting activities.

Wireless Network Name (SSID)

This is the name of your wireless network. It is set to the default name of NETGEAR_11a for 802.11a/n devices and NETGEAR_11ng for 802.11b/g/n devices.

Broadcast Wireless Network Name (SSID)

If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. The default is Yes.

Channel/Frequency

The wireless channel in use can be from 1 to 11 for the United States and Canada, or 1 to 13 for Europe and Australia. The default is Auto.

Do not change the wireless channel unless you experience interference (shown by lost connections or slow data transfers). Should this happen, you might need to experiment with different channels to see which is the best. You can select the Auto channel option to have the access point intelligently pick the channel with the least interference. When selecting or changing channels, bear these points in mind:

- Access points use a fixed channel. You can select the channel used. This allows you to 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 access points, it is better if adjacent access points use different channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).
- Wireless stations usually scan all channels, looking for an access point. If more than one access point can be used, the one with the strongest signal is used. This can happen only when the access points use the same SSID.

MCS Index/Data Rate

You can select the transmit data rate of the wireless network. Depending on the band selected, the set of rates varies. (When auto channel is enabled in the 802.11n mode, then the default channel width mode is 20 MHz. In this case, you cannot modify this parameter unless you change to a static channel.) The possible supported data rates are:

- **Channel Width=20 MHz and Guard Interval=short (400 ms).** Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps.
- **Channel Width=40 MHz and Guard Interval=short.** Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps.
- **Channel Width.** The following options are available:
 - **20 MHz.** This is the static, legacy mode. It gives the least throughput.
 - **40 MHz.** This is the static, high-throughput mode. Legacy clients cannot connect in this mode.
 - **20/40 MHz.** This is the dynamic, compatibility mode. Legacy clients can connect to 20 MHz and 11n clients can connect to 40 MHz.

Guard Interval

The guard interval protects from interference from other transmissions. The default is Auto.

Output Power

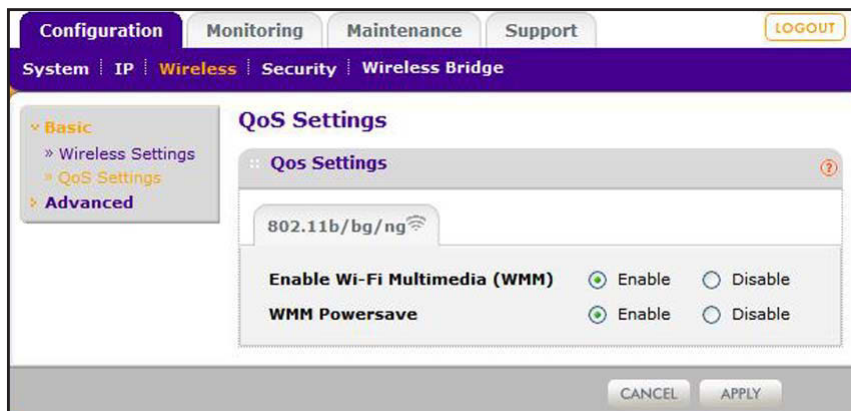
This is the transmit power of the access point. The options are Full, Half, Quarter, Eighth, and Minimum. Decrease the transmit power if two or more access points are close together and use the same channel frequency. The default is Full. (The transmit power might vary depending on the local regulatory regulations.)

QoS Settings

Wireless 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 must support WMM. Wi-Fi Multimedia (WMM) is enabled by default in the access point.

➤ To change the QoS settings:

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



2. Select the **Enable** radio buttons for the options settings that you want to use.
3. Click **Apply** to save your settings.

Deploy the Access Point

Before mounting the access point in a high location, first set up and test the access point to verify wireless network connectivity.

By default, the access point has the DHCP client disabled. If your network uses dynamic IP addresses, you need to change this setting. To connect to the access point after the DHCP server on your network assigns it a new IP address, enter the access point name in your web browser. The default name is netgearxxxxxx, where xxxxxx represents the last 6 bytes of the MAC address. The default name is printed on the bottom label of the access point.

➤ **To deploy the access point:**

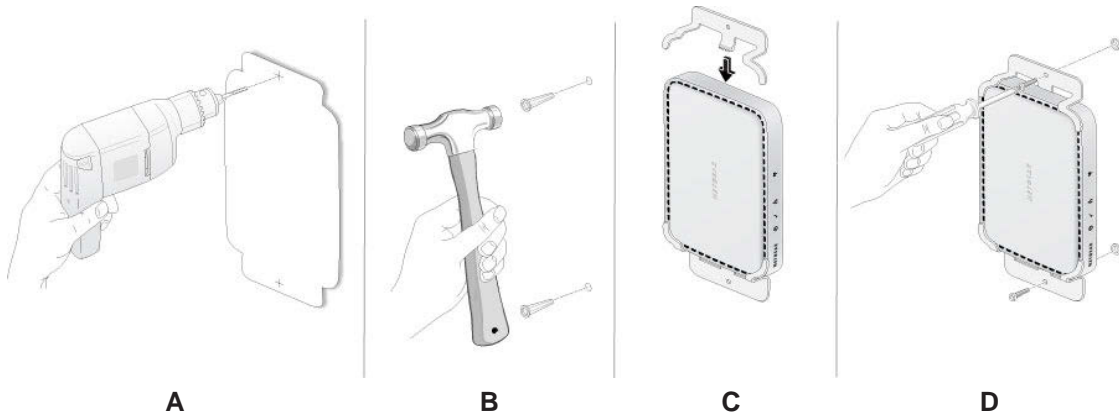
1. Disconnect the access point from the computer you used to configure it, and put the access point where it will be deployed.
The best location is elevated, such as on a wall or ceiling or on the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.
2. Connect an Ethernet cable from your access point to a LAN port on your router, switch, or hub.
3. If you are not using PoE, connect the power adapter to the wireless access point, and plug the power adapter into a power outlet. The Power and LAN LEDs should be on, and the WLAN LED should blink.

Wall Mount Kit (Optional)

Before mounting the access point in a high location, first set up and test the access point to verify wireless network connectivity. See [Set Up and Test Basic Wireless Connectivity](#) on page 15.

➤ **To install the access point mounting brackets:**

1. Disconnect the access point and position it where it will be deployed. The best location is elevated, such as on a wall or ceiling or the top of a cubicle, at the center of your wireless coverage area, and within line of sight of all the mobile devices.
2. Use the paper template provided to determine the location for the mounting holes. Drill holes 3/8 inches (~ 9 mm) and 13/16 in. (~20 mm) deep. The holes should be 10 1/4 in. (26 cm) apart, as shown in (A). Then tap in the anchors as shown in (B).



3. The tabs at the center of each bracket hook into the center vent slots on the bottom of the access point. The tabs on the ends of the brackets hook into the corner vent slots on the top of the access point. Hook the center tabs of one bracket in first. Then gently snap the tabs at the ends of the bracket into the top vents as shown in (C). Repeat for the second bracket.
4. Attach the brackets to the anchors using the screws from the mounting kit as shown in (D).
5. Connect an Ethernet cable from your access point to a LAN port on your router, switch, or hub. If power is not provided by PoE, connect the power adapter to the wireless access point and plug the power adapter into a power outlet. The Power, LAN, and WLAN LEDs should light up.

Wireless Security Options

Anyone with a compatible wireless adapter can receive your wireless data transmissions well beyond your walls. For this reason, use the security features of your wireless equipment. The access point provides highly effective security features, which are covered in detail in this chapter. Deploy the security features appropriate for your needs.

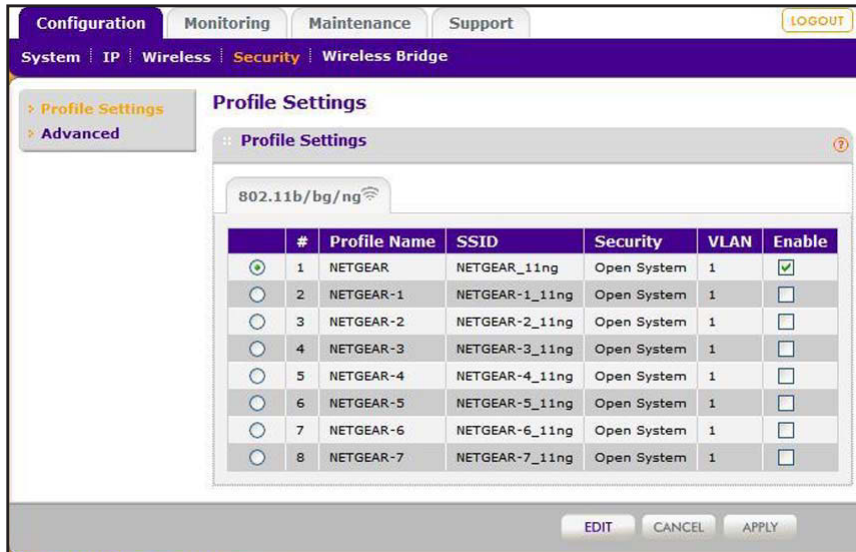
There are several ways you can enhance the security of your wireless network:

- **Restrict access based on MAC address.** You can restrict access to only trusted computers so that unknown computers cannot wirelessly connect to the 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. See [Restrict Wireless Access by MAC Address](#) on page 29.
- **Turn off the broadcast of the wireless network name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network “discovery” feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. See [Security Profiles](#) on page 21.
- **Use WPA2 or WPA Security Option.** A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are several types of encryption: Wi-Fi Protected Access II (WPA2), WPA, and Wired Equivalent Privacy (WEP). WPA2 is the latest and most secure, and is recommended if your equipment supports it. See [Security Profiles](#) on page 21.

Note: WEP and TKIP provide only legacy (slower) rates of operation. NETGEAR recommends AES encryption so that you can use the 11n rates and speed. See [Table 2](#) on page 22.

Security Profiles

Security profiles let you set up unique security settings for each SSID. You can configure up to eight unique 802.11b/g/n wireless security profiles on the access point. Select **Configuration > Security > Profile Settings** to display the Profile Settings screen:



If you are using a RADIUS server, configure the RADIUS settings first, as described in the [RADIUS Server Settings](#) on page 24.

An overview of the information that is required to set up a security profile follows—including a description of the network authentication choices that are available.

Profile Definition

Only the first profile is enabled by default. The rest of the profiles are disabled and need to be enabled if configured.

Specify the following settings:

- **Profile Name.** Use a name that makes it easy to recognize the profile and to tell profiles apart. (The default names are NETGEAR_11ng, NETGEAR-1_11ng, NETGEAR-2_11ng, and so on.) You can enter a value of up to 32 alphanumeric characters.
- **SSID.** This is the name of your wireless network. It is set to the default name of NETGEAR_11ng for 802.11b/g/n.
- **Security.** The wireless security used for this SSID.
- **VLAN.** You can use the default VLAN 1, or you can set up VLANs for your profiles. See [802.1Q VLAN](#) on page 47.
- **Enable.** Select the Enable check box to enable the profile.

Network Authentication Settings

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

- If you are using access point mode, then all options are available. In other modes such as repeater or bridge, some options might be unavailable.
- Not all legacy wireless adapters support WPA or WPA2. Windows XP and Windows 2000 with Service Pack 3 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.

You can configure the access point to use the types of network authentication shown in the table.

Table 2. Network authentication types

Type	Description
Open System	Can be used with WEP encryption or no encryption.
Shared Key	Compatible with WEP encryption. You enter at least one shared key.
Legacy 802.1x	You have to set up the RADIUS server settings to use this option.
WPA with RADIUS	You have to set up the RADIUS server settings to use this option.
WPA2 with RADIUS (WPA2 is a later version of WPA.)	Select this only if all clients support WPA2. If selected, you have to use AES encryption and configure the RADIUS server settings.
WPA and WPA2 with RADIUS	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you have to use TKIP + AES encryption and configure the RADIUS server settings.
WPA-PSK	You have to use TKIP or TKIP + AES encryption and enter the WPA passphrase (network key).
WPA2-PSK (WPA2 is a later version of WPA.)	Select this only if all clients support WPA2. If selected, you have to use AES and TKIP + AES encryption and enter the WPA passphrase (network key).
WPA-PSK and WPA2-PSK	This selection allows clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you have to use TKIP + AES encryption and enter the WPA passphrase (network key).

Data Encryption

The available options depend on the network authentication setting selected (see [Table 2](#)); otherwise, the default is None. The Data Encryption settings are explained in the following table:

Table 3. Data Encryption settings

Data Encryption Type	Description
None	No encryption is used.
64 bits WEP	Standard WEP encryption, using 40/64 bit encryption.
128 bits WEP	Standard WEP encryption, using 104/128 bit encryption.
152 bits WEP	Proprietary mode that works only with other wireless devices that support this mode.
TKIP	This is the standard encryption method used with WPA and WPA2.
AES	This is the standard encryption method for WPA2.
TKIP + AES	This setting supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES.

Passphrases and keys are used in the following ways:

- **Passphrase.** To use the passphrase to generate the WEP keys, enter a passphrase and click the **Generate Keys** button. You can also enter the keys directly. These keys have to match keys used by the other wireless stations.
- **Key 1, Key 2, Key 3, Key 4.** If you are using WEP, select the key to be used as the default key. Data transmissions are always encrypted using the default key. The other keys are used only to decrypt received data.
- **WPA Preshared Key Passphrase.** If you are using WPA-PSK, enter the passphrase here. All wireless stations have to use the same passphrase (network key). The network key has to be from 8 to 64 characters in length.

Wireless Client Security Separation

If this feature is enabled, the associated wireless clients will not be able to communicate with each other. (This feature is intended for hotspots and other public access situations.) The default is No.

VLAN ID

If the hubs or switches on your LAN support the VLAN (802.1Q) standard and this feature has been enabled, the default VLAN ID for WNAP210 is associated with each profile. The default profile VLAN ID has to match the IDs used by other network devices.

RADIUS Server Settings

You can set up or modify the RADIUS server settings to compliment network authentication security options. The RADIUS server needs to be used with Legacy 802.1x, and can be used with WPA and WPA2 network authentication. When using a RADIUS server, specify the RADIUS server settings before completing the network authentication security profile.

The RADIUS server settings apply to all profiles. They o need to be configured only once per access point.

➤ **To set up or modify the RADIUS server settings:**

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

	IP Address	Port	Shared Secret
Primary Authentication Server		1812
Secondary Authentication Server		1812
Primary Accounting Server		1813
Secondary Accounting Server		1813

2. Enter the following RADIUS server settings:
 - **Authentication Server.** This configuration is required for authentication using a RADIUS server. The IP address, port number, and shared secret are required for communication with the primary RADIUS server. You can also configure a secondary RADIUS server to use, if the primary RADIUS server fails.
 - **IP Address.** The IP address of the RADIUS server. The default is 0.0.0.0.
 - **Port.** The port number of the RADIUS server. The default is 1812.
 - **Shared Secret.** This is shared between the wireless access point and the RADIUS server when the supplicant (wireless client) is authenticated.
 - **Primary Accounting Server.** This configuration is required for accounting using a RADIUS server. The IP address, port number, and shared secret are required for communication with the primary RADIUS server. You can also configure a secondary RADIUS server to use if the primary RADIUS server fails.
 - **IP Address.** The IP address of the RADIUS server. The default is 0.0.0.0.
 - **Port.** Port number of the RADIUS server. The default: 1813.
 - **Shared Secret.** This is shared between the wireless access point and the RADIUS server when the supplicant (wireless client) is authenticated.
3. Click **Apply** to save your settings.

Change or Edit a Security Profile

The access point allows you to set up eight different security profiles. You can configure each profile with a different security option for network authentication.

➤ **To set up a security profile:**

If you are using a RADIUS server, configure the RADIUS settings first, as described in the [RADIUS Server Settings](#) on page 24.

1. Select **Configuration > Security > Profile Settings**. The profile settings you selected display.

#	Profile Name	SSID	Security	VLAN	Enable
1	NETGEAR	NETGEAR_11ng	Open System	1	<input checked="" type="checkbox"/>
2	NETGEAR-1	NETGEAR-1_11ng	Open System	1	<input type="checkbox"/>
3	NETGEAR-2	NETGEAR-2_11ng	Open System	1	<input type="checkbox"/>
4	NETGEAR-3	NETGEAR-3_11ng	Open System	1	<input type="checkbox"/>
5	NETGEAR-4	NETGEAR-4_11ng	Open System	1	<input type="checkbox"/>
6	NETGEAR-5	NETGEAR-5_11ng	Open System	1	<input type="checkbox"/>
7	NETGEAR-6	NETGEAR-6_11ng	Open System	1	<input type="checkbox"/>
8	NETGEAR-7	NETGEAR-7_11ng	Open System	1	<input type="checkbox"/>

2. Select the radio button of the profile you want to modify and click **Edit**. The Edit Security Profile screen for the selected profile displays.

Edit Security Profile

Profile Definition

Profile Name: NETGEAR

Wireless Network Name (SSID): NETGEAR_11ng

Broadcast Wireless Network Name (SSID): ☒ Yes ☐ No

Authentication Settings

Network Authentication: Open System

Data Encryption: None

Wireless Client Security Separation: ☐ Yes ☒ No

VLAN ID: 1

3. Give your profile a meaningful name so that you can remember it later.
4. The wireless network name (SSID) is set by default to identify it as NETGEAR_11ng.
5. Enable or disable the broadcast wireless network name (SSID). It is enabled by default. (If it is broadcast, it can be easily detected by other clients.)
6. Select the network authentication type you want to use for this profile.

7. Leave Wireless Client Security Separation set to **No** (it is disabled by default). If this feature is enabled, the associated wireless clients will not be able to communicate with each other.
8. If the hubs and switches on your LAN support the VLAN (802.1Q) standard and this feature has been enabled, the default VLAN ID for WNAP210 is associated with each profile. The default profile VLAN ID has to match the IDs used by other network devices.
9. Click **Apply** to save your security profile settings.
10. Click **Back**. Your new settings display in the Security Profiles table identified by the name of the profile. A VLAN ID is also assigned to your profile.

Note: Security profiles that share the same type of network authentication need not share the same passphrase or keys. Security profiles that use WEP have to share the same four keys, but they do not need to use the same default key.

➤ **To enable your security profile:**

1. Select the **Enable** check box in the column next to your profile.
2. Click **Apply**. Your security profile is enabled. If you enabled VLAN 802.1Q, your VLAN profile is enabled. (See [Set Basic IP Options](#) on page 13 for information about how to enable VLAN 802.1Q.)

WPA2, WPA2 & WPA, or WPA with RADIUS

Make sure that your wireless clients support WPA 2 or WPA with RADIUS. Note that you can set up the access point to work with a combination of clients, some of which use WPA2 and some of which use WPA.

➤ **To configure WPA2 or WPA with RADIUS:**

1. Select **Configuration > Security > Advanced > RADIUS Server Settings**. The RADIUS Server Settings screen displays.
2. Enter the RADIUS server settings as shown in [RADIUS Server Settings](#) on page 24, and click **Apply**.
3. Select **Configuration > Security > Profile Settings**. The profile settings you selected display.

4. Select the radio button of the security profile you want to modify, and click **Edit**.

Edit Security Profile

:: Profile Definition

Profile Name: NETGEAR

Wireless Network Name (SSID): NETGEAR_11g

Broadcast Wireless Network Name (SSID): ☒ Yes ☐ No

:: Authentication Settings

Network Authentication: WPA with Radius

Data Encryption: TKIP

Wireless Client Security Separation: ☐ Yes ☒ No

VLAN ID: 1

5. In the Network Authentication field, select one of the following:

- WPA2 with Radius
- WPA with Radius
- WPA2 & WPA with Radius

The encryption type displayed in the Data Encryption field is automatically updated based on your selection in the Network Authentication list.

6. Leave the Wireless Client Security Separation radio button set to **No** (it is selected by default). If this feature is enabled, associated wireless clients will not be able to communicate with each other. This feature is intended for hotspots and other public access situations.
7. Click **Apply** to save your settings.

WPA2-PSK, WPA-PSK, or WPA2-PSK & WPA-PSK

Make sure that your wireless clients support the option that you plan to use (WPA2-PSK or WPA-PSK).

➤ To configure WPA2-PSK, WPA-PSK, or WPA2-PSK & WPA-PSK:

1. Select **Configuration > Security > Profile Settings**. The profile settings you selected display.
2. Select the radio button of the security profile you want to modify, and click **Edit**.

Edit Security Profile

:: Profile Definition

Profile Name: NETGEAR

Wireless Network Name (SSID): NETGEAR_11g

Broadcast Wireless Network Name (SSID): ☒ Yes ☐ No

:: Authentication Settings

Network Authentication: WPA2-PSK & WPA-PSK

Data Encryption: TKIP + AES

WPA Passphrase (Network Key): [password field]

Wireless Client Security Separation: ☐ Yes ☒ No

VLAN ID: 1

3. In the Network Authentication field, select one of the following:

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

The Data Encryption field automatically updates based on your selection:

- WPA2-PSK is set to AES.
- WPA-PSK is set to TKIP.
- WPA2-PSK & WPA-PSK is set to TKIP+AES.

4. Enter the preshared key passphrase (network key).

5. Leave the Wireless Client Security Separation radio button set to **No** (it is selected by default). If this feature is enabled, associated wireless clients will not be able to communicate with each other. This feature is intended for hotspots and other public access situations.

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

WEP Security

WEP is a legacy security option. NETGEAR recommends that you use a newer security option such as WPA2 or WPA to protect your network.

➤ To configure WEP data encryption:

1. Select **Configuration > Security > Profile Settings**. The profile settings you selected display.
2. Select the radio button of the security profile you want to modify, and click **Edit**.

3. From the Network Authentication drop-down list, select either **Open System** or **Shared Key**.
4. From the Data Encryption drop-down list, select the encryption strength (64 bits, 128 bits, or 152 bits).

5. You manually or automatically program the four data encryption keys. These values have to be identical on all wireless clients and access points in your network. Select either:
 - **Automatic.** Enter a word or group of printable characters in the Passphrase box and click the **Generate Keys** button. The four fields are automatically populated with key values.
 - **Manual.** Enter the number of hexadecimal digits appropriate for the encryption strength: 10 characters for 64-bit, 26 digits for 128-bit, or 32 characters for 152-bit WEP encryption (any combination of **0–9**, **a–f**, or **A–F**).
Select which of the four keys will be the default.
6. Select the key to be used as the default key by selecting the radio button. (Data transmissions are always encrypted using the default key.)
7. Leave the Wireless Client Security Separation radio button set to **No** (it is selected by default). If this feature is enabled, associated wireless clients will not be able to communicate with each other. This feature is intended for hotspots and other public access situations.
8. Click **Apply** to save your settings.

Restrict Wireless Access by MAC Address

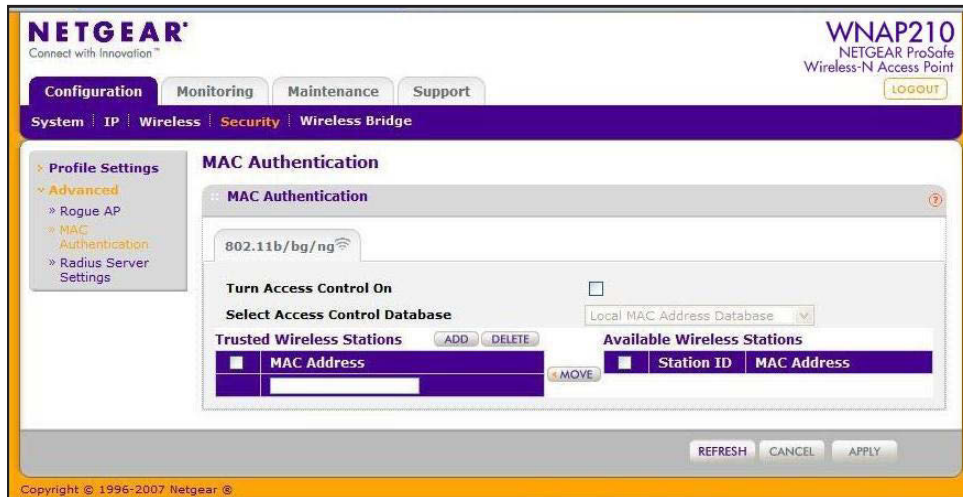
The access control list lets you block the network access privilege of any specified stations through the access point. When you enable access control, the access point accepts connections only from clients on the selected access control list. This provides an additional layer of security.

Note: If configuring the access point from a wireless computer whose MAC address is not in the access control list, if you select Turn Access Control On, you will lose your wireless connection when you click Apply. To make further changes, you have to connect to the access point from computer that is on the access control list.

➤ To restrict access based on MAC addresses:

1. Log in to the WNAP210 using the default address of **http://192.168.0.236**, user name of **admin**, and default password of **password**, or whatever LAN address and password you have set up.

2. Select **Configuration > Security > Advanced > MAC Authentication**. The MAC Authentication screen displays.



3. Select the **Turn Access Control On** check box to enable the access control feature.
4. Select the access control database options. The options are:
 - **Local MAC Address Database.** The access point will use the local MAC address table for access control. This is the default.
 - **RADIUS MAC Address Database.** The access point will use the MAC address table located on the external RADIUS server on the LAN for access control. If you select this database, you have to configure the RADIUS server settings first (see [RADIUS Server Settings](#) on page 24).
5. The Trusted Wireless Stations list shows any wireless stations you have entered. If you have not entered any wireless stations, this list is empty. To delete an existing entry, select it and click **Delete**.
6. Click **Refresh** to refresh the list of available wireless stations list found in your area.
7. Select the stations from the list of available wireless stations, or enter station MAC addresses manually. (The MAC address is usually on the bottom of the wireless adapter.)
8. Click **Add** to add the wireless device to the Trusted Wireless Stations list. Repeat these steps for each additional device you want to add to the list.
9. Click **Apply** to save your wireless access control list settings.

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

This chapter covers the following topics:

- *Change the Password*
- *Remote Management*
- *Remote Console*
- *Upgrade the Access Point Firmware*
- *Save or Restore the Configuration File*
- *Enable the Syslog Server*
- *Restore Defaults*

Change the Password

The default password for the user name admin is **password**. You should change this to a more secure password. You cannot change the admin user name.

➤ **To change the administrator password:**

1. Select **Maintenance > Password > Change Password** to display the Change Password screen:

The screenshot shows the web interface of the WNAP210. At the top, there are tabs for Configuration, Monitoring, Maintenance (selected), and Support. A LOGOUT button is in the top right. Below the tabs is a navigation bar with links: Password (selected), Reset, Remote Management, and Upgrade. On the left, there is a sidebar with a link to Change Password. The main content area is titled 'Change Password' and contains a form with the following fields: Current Password, New Password, Repeat New Password, and Restore Default Password. The Restore Default Password field has two radio buttons: Yes and No. At the bottom of the form are CANCEL and APPLY buttons.

2. Enter the password in the Current Password field.
3. Then enter the new password twice, once in the New Password field and again in the Repeat New Password field.
4. Click **Apply** to save your change.

Remote Management

Both the SNMP and Remote Console are enabled by default, which allows for remote management of the WNAP210 from a client running SNMP management software, as well as from a secure Telnet console.

➤ To set up an SNMP management interface:

1. Select **Maintenance > Remote Management > SNMP**. The SNMP screen displays, as shown in the following figure:

The screenshot shows the Netgear WNAP210 web interface. The top navigation bar includes tabs for Configuration, Monitoring, Maintenance, and Support. Under the Maintenance tab, there are links for Password, Reset, Remote Management, and Upgrade. The main content area displays the SNMP Settings form. The form includes a section for enabling or disabling SNMP, with 'Enable' selected. Below this are four text input fields: Read-Only Community Name (containing 'public'), Read-Write Community Name (containing 'private'), Trap Community Name (containing 'trap'), and IP Address to Receive Traps (empty). At the bottom of the form are 'CANCEL' and 'APPLY' buttons. The footer of the page shows the copyright notice: Copyright © 1996-2007 Netgear ©.

2. Enter the following information in the SNMP fields:
 - **SNMP.** Enable SNMP to allow the SNMP network management software, such as HP OpenView, to manage the wireless access point through SNMPv1/v2 protocol.
 - **Read-Only Community Name.** The community string to allow the SNMP manager to read the wireless access point's MIB objects. The default is Public.
 - **Read-Write Community Name.** 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. The default is 0.0.0.0.
3. Click **Apply**.

Remote Console

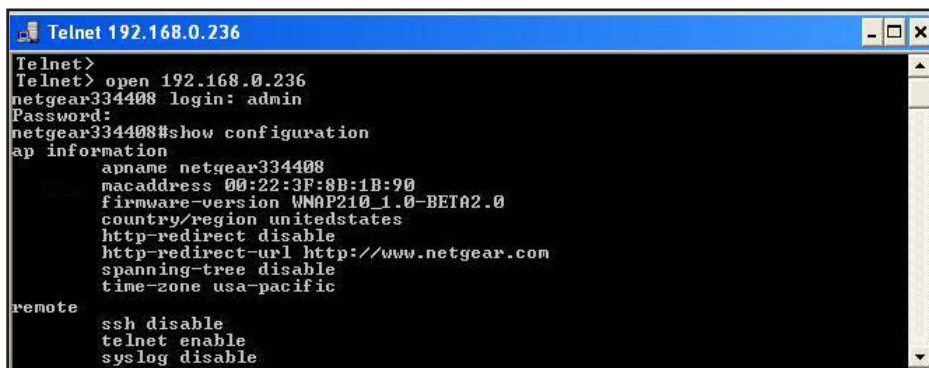
1. Select **Maintenance > Remote Management > Remote Console**.



2. Enter the following information in the Remote Console screen.
 - **Secure Shell (SSH)**. If set to Enable, the wireless access point allows remote access only through Secure Shell and Secure Telnet. The default is Enable.
 - **Telnet**. If set to Enable, the wireless access point allows remote access through Telnet. The default is Disable. If Telnet is enabled and the access point is accessed using a browser, the Telnet access is disconnected.
3. Click **Apply**.

Management Using Telnet

1. Open a secure Telnet session from your computer to the access point. The screen shown in the following figure should display.



2. Enter the login name and password (**admin** and **password** are the defaults).
After successful login, the <Access Point Name> prompt should display. In this example, the prompt is `netgear334408`.
3. Enter the desired CLI commands. You can enter `help` to display the CLI command help. The CLI commands are listed in [Appendix B, Command Line Reference](#).

Upgrade the Access Point Firmware

The firmware is stored in flash memory, and can be upgraded as NETGEAR releases new firmware. You can download upgrade files from the NETGEAR website. If the upgrade file is compressed (.zip file), you need to first extract the image (.rmt) file before sending it to the access point. You can send the upgrade file using your browser.

Note: Use a web browser such as Mozilla Firefox or Internet Explorer. The browser must support HTTP uploads.

You cannot perform the software upgrade from a computer that is connected to the access point wirelessly. You have to use a computer that is connected with an Ethernet cable.

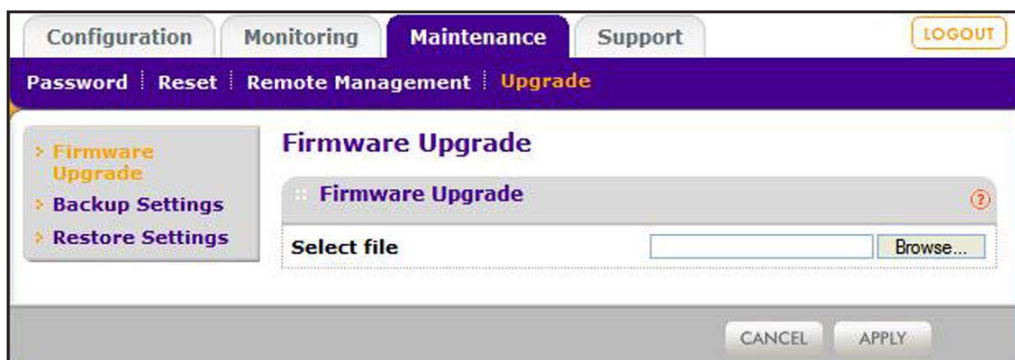


WARNING!

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

➤ To upgrade the firmware:

1. Download the new software file from the NETGEAR website, save it to your hard disk, and unzip it.
2. Select **Maintenance > Upgrade > Firmware Upgrade**. The Firmware Upgrade screen displays:



3. Click **Browse** and browse to the location of the image (.rmt) upgrade file.
4. Click **Apply**.

When the upload is completed, your access point automatically restarts. The upgrade process typically takes at least 3 minutes.

Save or Restore the Configuration File

The access point settings are stored in the access point in a configuration file. This file can be saved (backed up) or restored. You can also restore the factory settings as described in [Enable the Syslog Server](#) on page 37.

➤ **To save your settings in a configuration file:**

1. Select **Maintenance > Upgrade > Backup Settings** to back up your current settings. The Backup Settings screen displays.



2. Click **Backup**. Your browser extracts the configuration file from the access point and prompts you for a location on your computer to store the file.
3. Give the file a meaningful name, such as WNAP210.cfg, and click **Save**.

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

1. Select **Maintenance > Reset > Restore Defaults**. The Restore Defaults screen displays.
2. Select **No** for Restore to factory default settings and then click **Apply**. This displays a dialog box allowing you to select a file where you have previously saved configuration settings.
3. Enter the full path to the file on your computer, or click the **Browse** button to locate the file.
4. When you have located the file, click **Restore** to upload the file. After completing the upload, the access point reboots automatically.



Enable the Syslog Server

The Syslog screen allows you to enable the syslog option if you have a syslog server on your LAN.

➤ **To enable a syslog server:**

1. Select **Configuration > System > Advanced > SysLog** to display the Syslog screen.

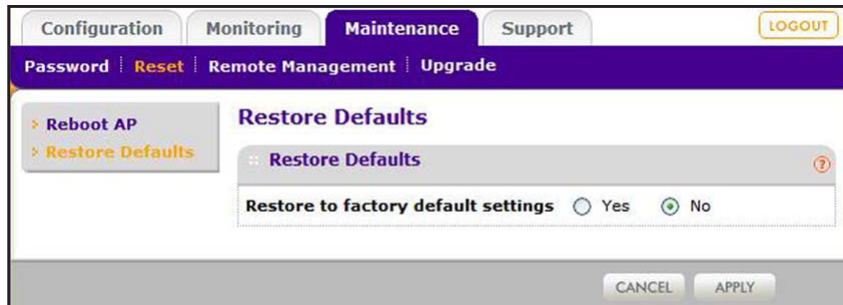
2. Specify the following settings:
 - **Enable Syslog.** Enable this option if you have a syslog server on your LAN. If this feature is enabled, you have to enter the IP address of your syslog server and the port number your syslog server is configured to use. The default is disabled.
 - **Syslog Server IP Address.** The access point sends all the syslog files to the specified IP address if the syslog option is enabled. The default is 0.0.0.0.
 - **Port Number.** The port number configured in the syslog server on your LAN. The default is 514.
3. Click **Apply** to save your syslog settings.

Restore Defaults

You can restore the access point to the factory default settings using the Restore Defaults menu selection, or by using the Restore Factory Settings button (see [Factory Default Settings](#) on page 63).

➤ **To restore the factory settings:**

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



2. Select the **Yes** radio button.
3. Click **Apply**.

The access point password is password, the access point DHCP client is disabled, the default LAN IP address is 192.168.0.236, and the access point name is reset to the name printed on the label on the bottom of the unit.

4. Monitoring

4

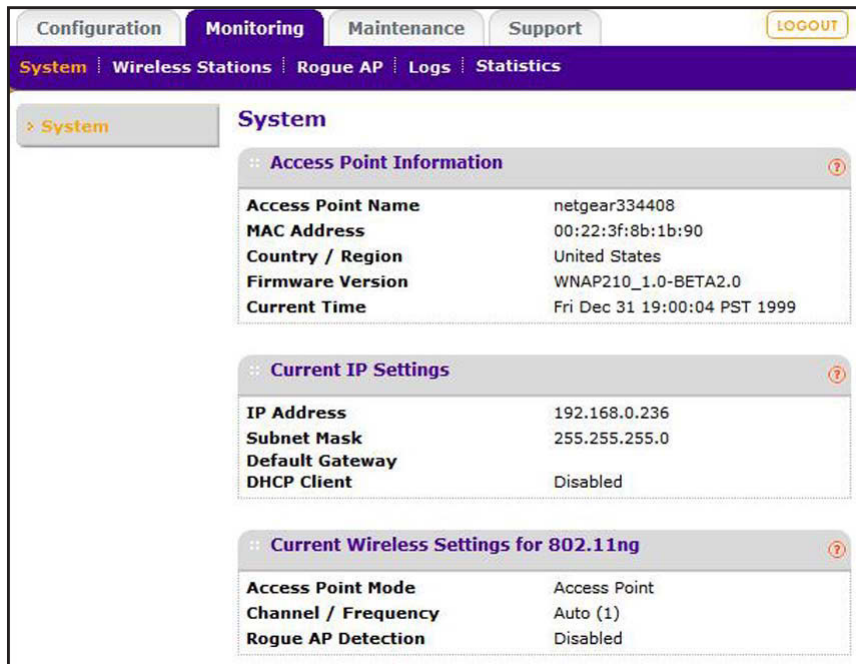
This chapter covers the following topics:

- *System Information*
- *Wireless Stations*
- *Enable Rogue AP Detection*
- *View and Save AP Lists*
- *Activity Log*
- *Network Traffic Statistics*

System Information

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

To access the System screen, select **Monitoring > System**.



This screen shows the following information:

- **Access Point Name.** The NetBIOS name. The default name can be changed.
- **MAC Address.** The MAC address of the access point's Ethernet port.
- **Country/Region.** The domain or region for which the access point is licensed for use. It might not be legal to operate this access point in a region other than one of those identified in this field.
- **Firmware Version.** The version of the firmware currently installed.
- **Current Time.** The time setting for the access point.
- **IP Address.** The IP address of the access point.
- **Subnet Mask.** The subnet mask for the access point.
- **Default Gateway.** The default gateway for the access point communication.
- **DHCP Client.** Enabled indicates that the current IP address was obtained from a DHCP server on your network. Disabled indicated a static IP configuration.
- **Access Point Mode.** The operating mode of the access point: Access Point or Point-to-point • **Channel/Frequency.** The channel the wireless port is using.
- **Rogue AP Detection.** Shows whether the rogue AP detection feature is enabled.

Wireless Stations

This screen shows all IP devices associated with this access point in the wireless network defined by the wireless network name (SSID). For each device, the screen shows the station ID, MAC address, IP address, BSSID, SSID, AID, channel rate, status (whether or not the station is allowed to communicate with the access point), type, mode, and state.

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 access point to another, providing seamless network connectivity. Under these circumstances, be aware that the Wireless Stations screen includes only the stations associated with this access point.

➤ **To view the Available Wireless Stations list:**

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



2. Click **Refresh** to update the list.

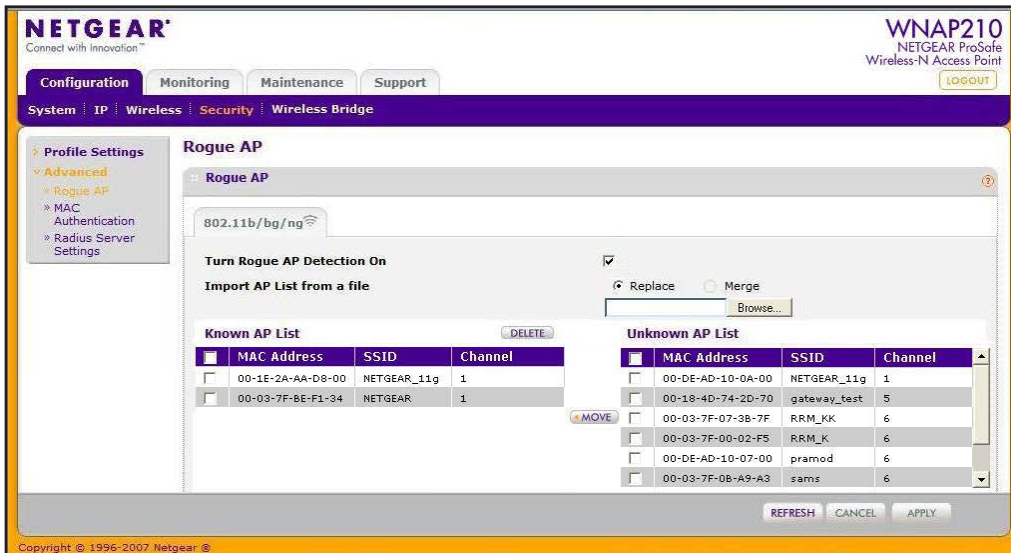
If the access point is rebooted, the data on this screen is lost until the access point rediscovers the devices. To force the access point to look for associated devices, click the **Refresh** button.

Enable Rogue AP Detection

The access point can detect rogue APs and wireless stations and can prevent them from connecting. The access point maintains a list of access points and wireless stations that 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 rogue AP detection. Monitoring 42 ProSafe Wireless-N Access Point WNAP210.

➤ To enable rogue AP detection:

1. Select **Configuration > Security > Advanced > Rogue AP**. The Rogue AP screen displays:



2. Click **Refresh** to discover the APs. See the following section for more information.
3. Click **Move** to add APs in the Unknown AP List to the Known AP List.
4. Click **Delete** to remove APs from the Known AP List back to the Unknown AP List.
5. Select the Turn Rogue AP Detection On check box, and click **Apply**.

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

Import a Rogue AP List from a File

You can import the Known AP List from a file.

➤ To replace an existing AP list:

1. Select the **Replace** radio button to replace the existing list of known APs.
2. Click **Browse**, and navigate to the location of the file containing the device list.
3. Select the file, and click **Open**.
4. Click **Import** to upload the list to the AP.

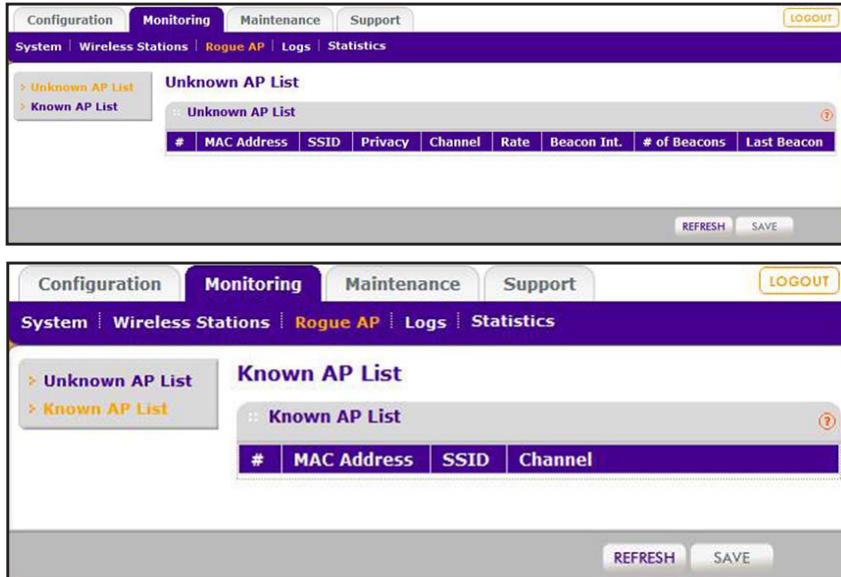
➤ To merge a file with an existing AP list:

1. Select the Merge radio button to add the new MAC addresses to the existing list.
2. Click **Browse**, and navigate to the location of the file containing the device list.
3. Select the file, and click Open.
4. Click Import to upload the list to the AP.

View and Save AP Lists

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

1. Select **Monitoring > Rogue AP**. Select **Unknown AP List** or **Known AP List** as required. The respective screens display:



2. In the Unknown AP List or the Known AP List screen, click **Refresh** to update the corresponding list.
3. Click **Save** to export the list of unknown or known APs to a file. A dialog box opens so you can browse to the location where you want to save the file. The default file name is WNAP210Rogue.cfg.

You can now import the saved lists into the Rogue AP screen.

Create AP Lists Manually

You can create and save lists of devices manually:

1. Create a text file that contains the MAC address of each known AP, separated by a space. The following example shows a list of six known APs that an administrator might upload to the AP:

00:0c:41:d7:ee:a5 00:0f:b5:92:cd:49 00:12:17:70:85:3d

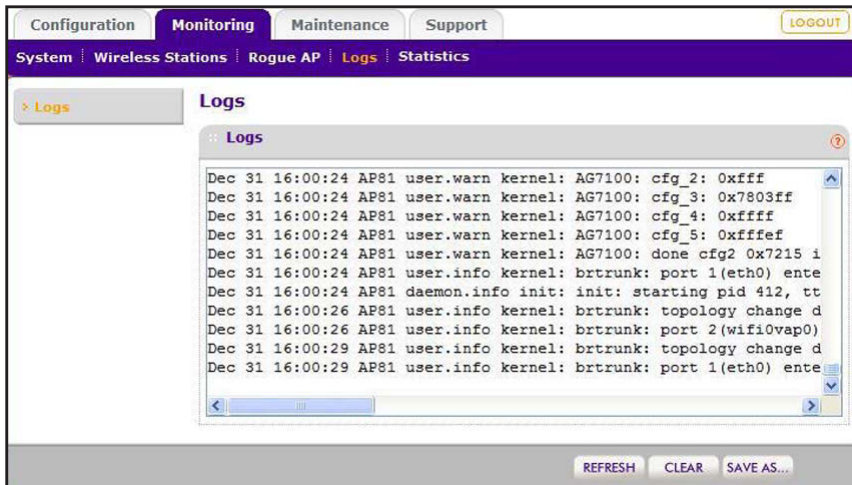
00:14:bf:ae:b1:e4 00:40:f4:f8:47:03 00:0c:41:d7:ee:b4

2. Select **Configure > Security > Advanced > Rogue AP**, and import the file.

Activity Log

The Activity Log screen displays the access point system activity.

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



2. Click **Refresh** to update the display, click **Clear** to clear the log content, or click **Save As** to save the log contents into a file on your computer or to save the file to a disk drive.

Network Traffic Statistics

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

To view statistics, select **Monitoring > Statistics**. The Statistics screen displays:

The screenshot shows the 'Statistics' screen in the web interface. It displays two tables of network traffic statistics:

Wired Ethernet		
	Received	Transmitted
Packets	13622	19679
Bytes	2181298	25195358

Wireless 11ng		
	Received	Transmitted
Unicast Packets	0	0
Broadcast Packets	0	252
Multicast Packets	0	0
Total Packets	0	252
Total Bytes	0	34257

You can click **Refresh** to update the statistics information for each interface.

The following information fields are displayed on the Statistics screen.

- **Packets.** The number of packets sent and received since the access point was restarted.
- **Bytes.** The number of bytes sent and received since the access point was restarted.
- **Unicast Packets.** The unicast packets sent and received since the access point was restarted.
- **Multicast Packets.** The broadcast packets sent and received since the access point was restarted.
- **Total Packets.** The wireless packets sent and received since the access point was restarted.
- **Total Bytes.** The wireless bytes sent and received since the access point was restarted.

5. Advanced Configuration

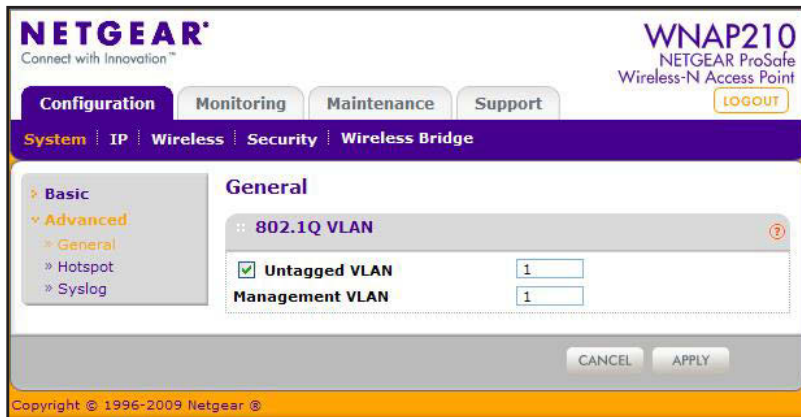
5

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

- *802.1Q VLAN*
- *Hotspot Settings*
- *Advanced Wireless Settings*
- *Advanced QoS Settings*
- *Wireless Bridging and Repeating*

802.1Q VLAN

The 802.1Q VLAN protocol on the access point logically separates traffic on the same physical network. Select **Configuration > System > General** to display the following screen:



Untagged VLANs

When the Untagged VLAN check box is selected, one VLAN can be configured as an untagged VLAN. When the access point sends frames associated with the untagged VLAN out the LAN (Ethernet) interface, those frames are untagged. When the access point receives untagged traffic from the LAN (Ethernet) interface, those frames are assigned to the untagged VLAN.

If this check box is not selected, the access point tags all outgoing LAN (Ethernet) frames. Only incoming frames tagged with known VLAN IDs are accepted.

You only need to clear the Untagged VLAN check box if the hubs or switches on your LAN support the VLAN (802.1Q) standard. Likewise, the Untagged VLAN value should be changed only if the hubs and switches on your LAN support the VLAN (802.1Q) standard. Changing either of these values results in a loss of IP connectivity if the hubs and switches on your network have not yet been configured with the corresponding VLANs.

Management VLANs

Management VLANs are used for managing traffic (Telnet, SNMP, and HTTP) to and from the access point. Frames belonging to the management VLAN are not given any 802.1Q header when sent over the trunk. If a port is in a single VLAN, it can be untagged. But if the port needs to be a member of multiple VLANs, it has to be tagged.

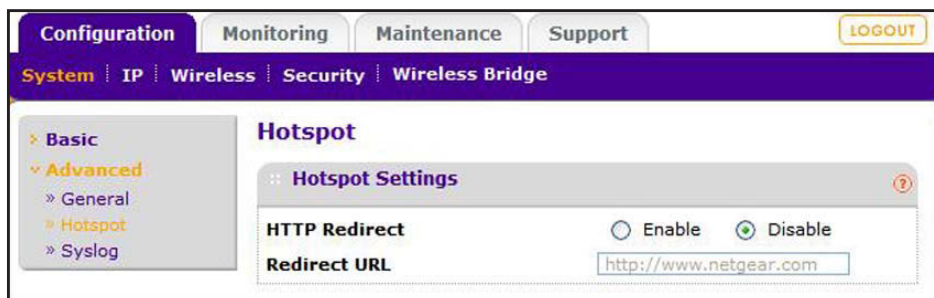
Hotspot Settings

If you want the access point to capture and redirect all HTTP (TCP, port 80) requests, use this feature to redirect the requests to the specified URL. For example, 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 a wireless client opens a web browser.

➤ **To set up a hotspot server:**

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



2. For HTTP Redirect, enter the URL of the web server to which you want to redirect HTTP (port 80) requests.
3. Click **Apply**. All port 80 requests are redirected to the specified URL.

Advanced Wireless Settings

The Wireless Settings screen is used to configure and enable various wireless LAN parameters for 11b/g/n mode. The default wireless LAN parameters usually work well. However, you can use these settings to fine-tune the overall performance of your access point for your environment.

➤ To configure advanced wireless settings:

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

The screenshot shows the 'Wireless Settings' page in the ProSAFE WNAP210 web interface. The page has a purple header with tabs for 'Configuration', 'Monitoring', 'Maintenance', and 'Support'. Below the header is a navigation bar with 'System', 'IP', 'Wireless', 'Security', and 'Wireless Bridge'. The 'Wireless' tab is selected. On the left, there is a sidebar with a tree view showing 'Basic', 'Advanced', 'Wireless Settings', and 'QoS Settings'. The 'Wireless Settings' tab is selected. The main content area is titled 'Wireless Settings' and contains a form for configuring 802.11b/bg/ng wireless settings. The form includes the following fields:

- RTS Threshold (0-2347)**: A text input field with the value 2347.
- Fragmentation Length (256-2346)**: A text input field with the value 2346.
- Beacon Interval (100-1000)**: A text input field with the value 100.
- Aggregation Length (1024-65535)**: A text input field with the value 65535.
- AMPDU**: A radio button group with 'Enable' selected and 'Disable' unselected.
- RIFS Transmission**: A radio button group with 'Enable' unselected and 'Disable' selected.
- DTIM Interval (1-255)**: A text input field with the value 3.
- Preamble Type**: A radio button group with 'Auto' selected and 'Long' unselected.

2. Enter the appropriate information in the following fields:
3. Click **Apply** to enable the wireless settings.

Advanced Wireless Settings Fields

The following fields are available in the advanced Wireless Settings screen:

- **RTS Threshold (0–2347)**. Request to Send Threshold. The packet size that is used to determine if it should use the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) mechanism or the CSMA/CA mechanism for packet transmission. With the CSMA/CD transmission mechanism, the transmitting station sends out the actual packet until the silence period ends. With the CSMA/CA transmission mechanism, the transmitting station sends out an RTS packet to the receiving station, and waits for the receiving station to send back a CTS (Clear to Send) packet before sending the actual packet data. The default is 2347.
- **Fragmentation Length (256–2346)**. This is the maximum packet size. Packets larger than the size specified in this field is fragmented. The Fragmentation Length value has to be larger than the RTS Threshold value. The default is 2346.
- **Beacon Interval (100–1000)**. The time interval between 100 ms and 1000 ms for each beacon transmission, which allows the access point to synchronize the wireless network. The default is 100.
- **Aggregation Length (1024 – 65535)**. The aggregation length defines the size of aggregated packets. Larger aggregation lengths can sometimes lead to better network performance. The default is 65535.
- **AMPDU**. Aggregated MAC Protocol data unit. Aggregates several MAC frames into a single large frame to achieve higher throughput. The default is enabled.

- **RIFS Transmission.** Reduced interframe space. RIFS transmissions are shorter than other interframe spaces, and if this feature is enabled, the access point allows transmission of successive frames at different transmit powers. The default is disabled.
- **DTIM Interval.** The delivery traffic indication message. Specifies the data beacon rate between 1 and 255. The default is 3.
- **Preamble Type.** A long transmit preamble can provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance. The Auto setting automatically handles both long and short preambles. The default is Auto.

Advanced QoS Settings

Wireless 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 have to support WMM.

For most networks, the default QoS (Quality of Service) queue settings work well. You can specify parameters on multiple queues for increased throughput and better performance of differentiated wireless traffic, like VoIP, and other types of audio, video, and streaming media, as well as traditional IP data.

The screenshot shows the 'QoS Settings' page in the web interface. The left sidebar has a menu with 'Basic' and 'Advanced' (expanded) options. Under 'Advanced', there are 'Wireless Settings' and 'QoS Settings'. The main content area is titled 'QoS Settings' and includes a tab for '802.11b/bg/ng'. It contains two tables: 'AP EDCA parameters' and 'Station EDCA parameters'.

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

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

The QoS options are as follows:

- **AP EDCA parameters.** Specify the AP EDCA parameters for different types of data transmitted from the access point to the wireless client.
- **Station EDCA parameters.** Specify the Station EDCA parameters for different types of data transmitted from the wireless client to the access point. If WMM is disabled, you cannot configure Station EDCA parameters.

The following table describes the settings for QoS queues.

Table 4. QoS queues and parameters

QoS queue	Description
Data 0 (Voice)	High-priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.
Data 1 (Video)	High-priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.
Data 2 (Best Effort)	Medium-priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.
Data 3 (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).
AIFS (Arbitration Inter-Frame Space)	Specifies a wait time (in milliseconds) for data frames. Valid values for AIFS are 1 through 255.
cwMin (Minimum Contention Window)	Upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Valid values for the cwMin are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024. The value for cwMin has to be lower than the value for cwMax.
cwMax (Maximum Contention Window)	Upper limit (in milliseconds) for the doubling of the random back-off value. Valid values for the cwMax are 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1024. The value for cwMax has to be higher than the value for cwMin.
Max. Burst Length	Specifies (in milliseconds) the maximum burst length allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Valid values for maximum burst length are 0.0 through 999.9.

Wireless Bridging and Repeating

The access point lets you build large bridged wireless networks. Select **Configuration > Wireless Bridge**.

Configuration | Monitoring | Maintenance | Support | LOGOUT

System | IP | Wireless | Security | **Wireless Bridge**

Bridging and Repeating

802.11b/bg/ng

Enable Wireless Bridging and Repeating ☐

Local MAC Address 00:22:3f:8b:1b:90

☒ Wireless Point-to-Point Bridge
 ☐ Wireless Point to Multi-Point Bridge
 ☐ Repeater
 ☐ Client

Enable Wireless Client Association ☒

#	Profile Name	Security	Enable
1	NETGEAR-WDS-1	Open System	<input checked="" type="checkbox"/>

EDIT CANCEL APPLY

Select the access point mode you want to use for your environment:

- **Wireless Point-to-Point Bridge.** In this mode, the access point can communicate with another bridge-mode wireless station and with wireless clients if you select the **Enable Wireless Client Association** check box. To associate wireless clients with this access point, select clients from the list in the Enable Wireless Clients Association table, and select the corresponding check box in the Enable column.
- **Wireless Point-to-Multi-Point Bridge.** Select this only if this WNAP210 access point is the master for a group of bridge-mode wireless stations. This mode supports default association with wireless clients. To associate wireless clients with this access point, select clients from the list in the Enable Wireless Clients Association table, and select the corresponding check box in the Enable column.

The other bridge-mode wireless stations have to be set to point-to-point bridge mode, using the MAC address of this access point access point. They then send all traffic to this master, rather than communicate directly with each other.

- **Repeater.** If this option is selected, this access point operates as a repeater only, and sends all traffic to the remote access point.

Note: This option does not support communication with wireless clients, that is, the client cannot associate with the access point when it is operating as a repeater.

- **Client Mode.** If selected, this access point operates as a client bridge only and sends all traffic to the remote access point or peer device. MAC cloning can also be enabled in client mode.

➤ **To edit a wireless bridge profile:**

1. Select a radio button for any option, an Edit button displays.
2. Click **Edit** to display a screen similar to the following:

3. Enter the profile name and the MAC address (physical address) of the other bridge-mode wireless station in the fields provided. WEP, WPA-PSK, or WPA2-PSK are supported. WPA2-PSK can (and should) be used to protect this communication

Point-to-Point Bridge

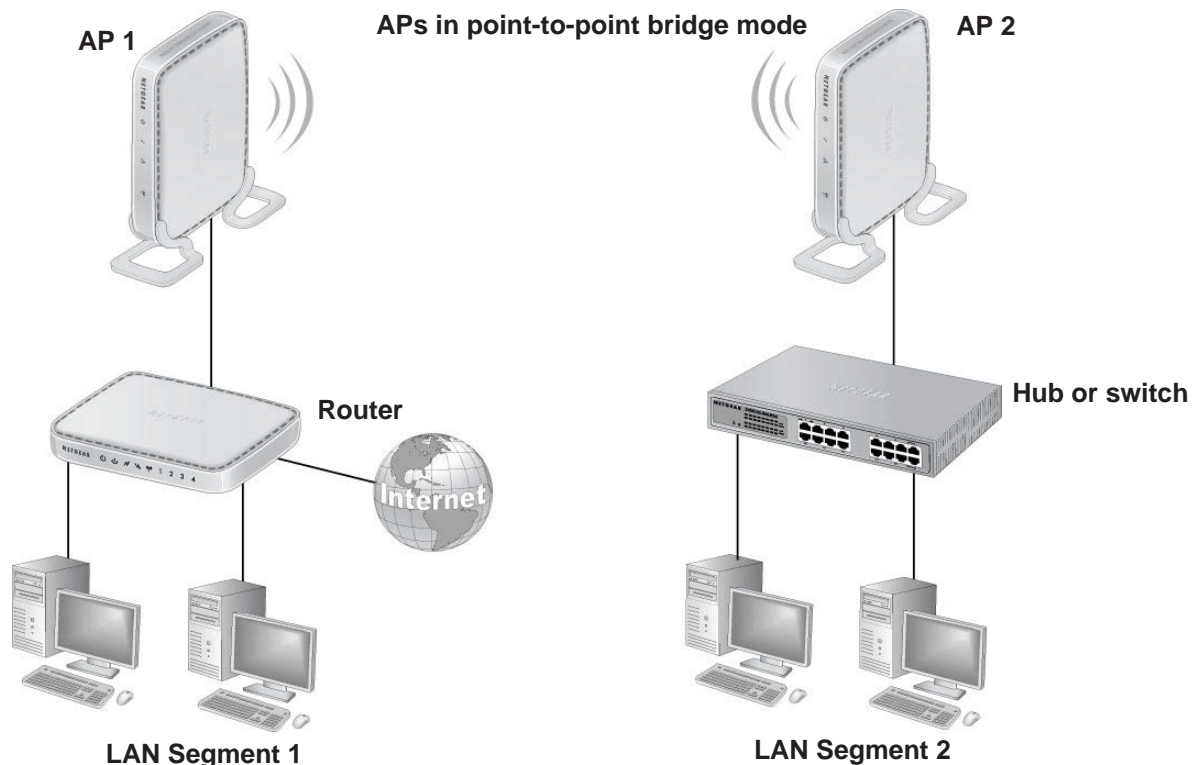


Figure 3. Point-to-point bridge mode

➤ **To configure a point-to-point bridge:**

1. Select **Configuration > Wireless Bridge > Bridging and Repeating**. The Bridging and Repeating screen displays.

The screenshot shows the 'Bridging and Repeating' configuration page. The 'Enable Wireless Bridging and Repeating' checkbox is checked. The 'Local MAC Address' is 00:22:3f:8b:1b:90. The 'Wireless Point-to-Point Bridge' radio button is selected. The 'Enable Wireless Client Association' checkbox is checked. A table shows a profile named 'NETGEAR-WDS-1' with 'Open System' security and 'Enable' status.

#	Profile Name	Security	Enable
1	NETGEAR-WDS-1	Open System	<input checked="" type="checkbox"/>

2. Select the **Enable Wireless Bridging and Repeating** check box. This allows you to select a bridging mode.
3. Select **Wireless Point-to-Point Bridge**, and click **Apply**.
4. Configure the first access point (AP 1) on LAN Segment 1 in point-to-point bridge mode.

5. Configure the other access point (AP 2) on LAN Segment 2 in point-to-point bridge mode.

AP 1 needs to have AP 2's MAC address in its Remote MAC Address field, and AP 2 needs to have AP 1's MAC address in its Remote MAC Address field.

6. Configure and verify the following parameters for both access points:
 - Verify that both access points are configured to operate in the same LAN network address range as the LAN devices.
 - Both use the same ESSID, channel, authentication mode, if any, and security settings.
7. Verify connectivity across 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.

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

Point-to-Multi-Point Wireless Bridge

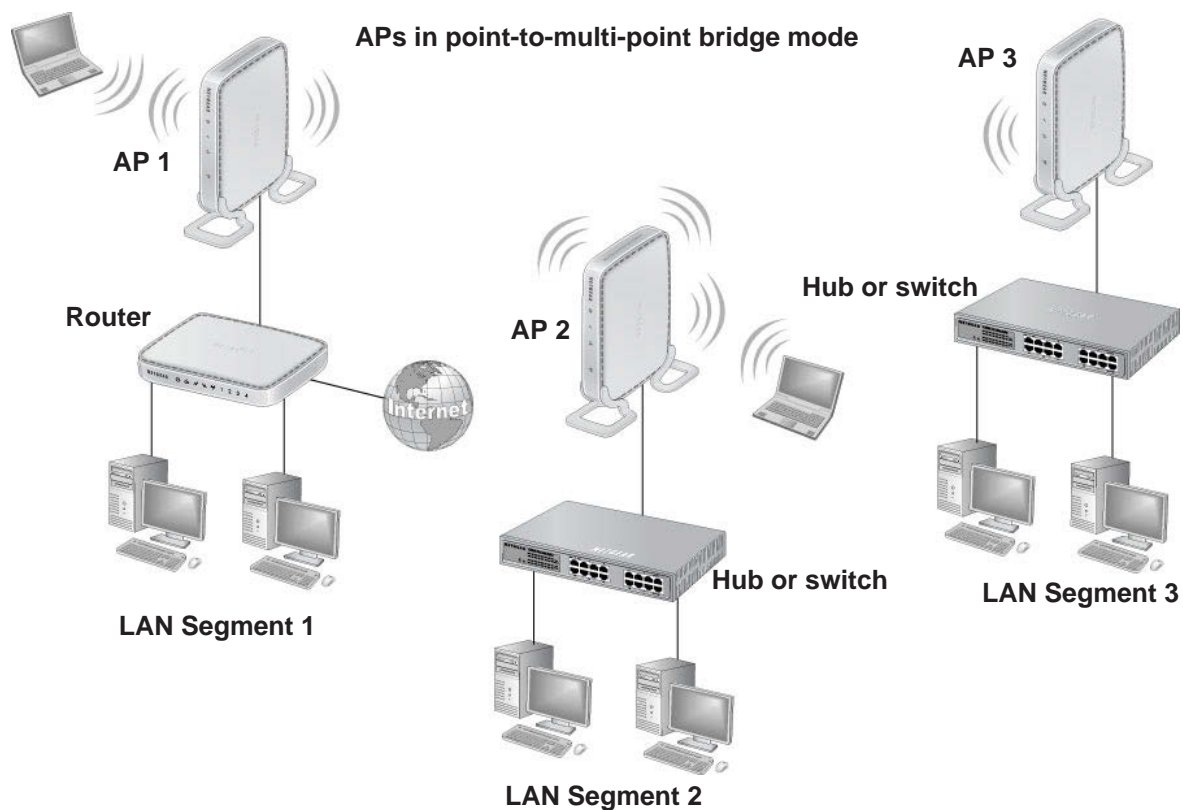


Figure 4. Point-to-multi-point-bridge mode

➤ **To configure a point-to-multi-point wireless bridge:**

1. For the first access point (AP 1) on LAN Segment 1, select **Configuration > Wireless Bridge > Bridging and Repeating**. The Bridging and Repeating screen displays.
2. Select the **Enable Wireless Bridging and Repeating** check box. This allows you to select a bridging mode.
3. Select **Wireless Point-to-Point Bridge**, and configure enter the remote MAC address of AP 2. Click **Apply**.
4. Because it is in the central location, configure the second access point (AP 2) on LAN Segment 2 in point-to-multi-point bridge mode. The MAC addresses of the adjacent APs are required in AP 2.
5. Configure the third access point (AP 3) on LAN 3 in point-to-point bridge mode with the remote MAC address of AP 2.
6. Verify the following parameters for all access points:
 - All access points are configured to operate in the same LAN network address range as the LAN devices.
 - Only one access point is configured in point-to-multi-point bridge mode, and all the others are in point-to-point bridge mode.
 - All access points have to be on the same LAN. That is, all the LAN IP addresses of the APs must be in the same network.
 - If you are using DHCP, all the access points should be set to Obtain an IP address automatically (DHCP Client). See [Set Basic IP Options](#) on page 13.
 - All access points use the same SSID, channel, authentication mode, if any, and encryption.
 - All point-to-point access points need to have the AP 2 MAC address in their Remote AP MAC Address fields.
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 computers or servers connected to any of the three LAN segments.
 - Wireless stations should be able to connect to the access points as shown in the previous illustration. If you require wireless stations to access any LAN segment, you can add additional access points configured in wireless bridge mode to any LAN segment.
8. Click **Apply** to save your settings.

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

Wireless Repeater

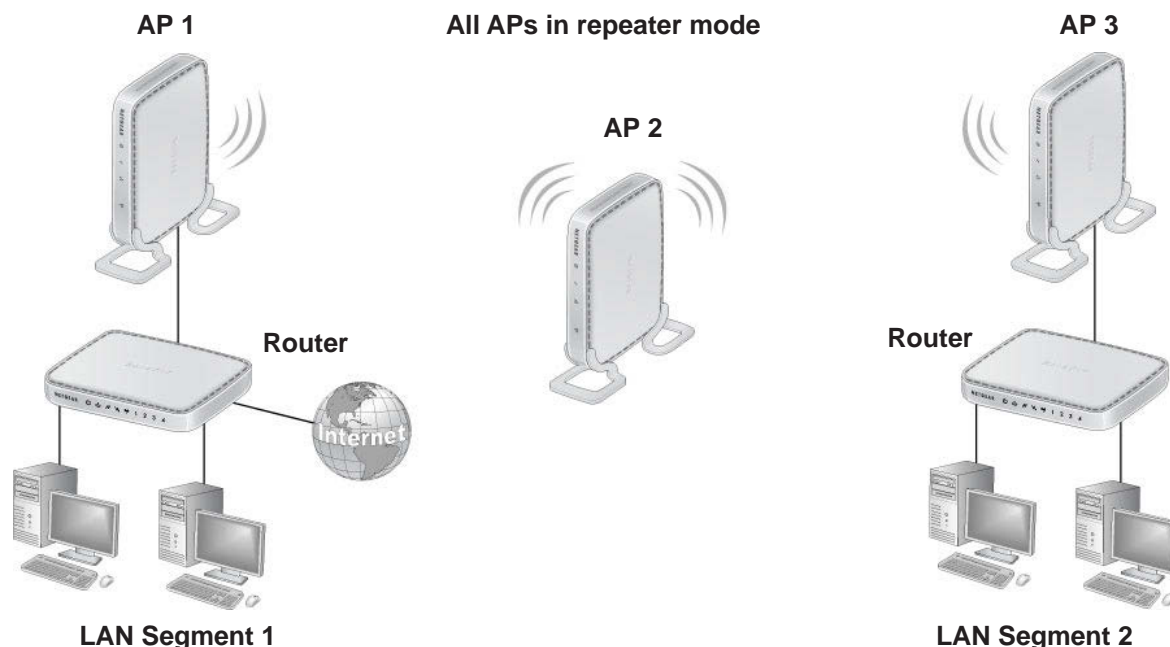


Figure 5. Wireless repeater

- To configure the access point as a wireless repeater:
1. For the first access point (AP 1) on LAN Segment 1, select **Configuration > Wireless Bridge > Bridging and Repeating**. The Bridging and Repeating screen displays.
 2. Select the **Enable Wireless Bridging and Repeating** check box. This allows you to select a bridging mode.
 3. Select **Repeater**, and configure enter the remote MAC address of AP 2. Click **Apply**.
 4. Configure the second access point (AP 2) in repeater mode with MAC addresses of AP 1 and AP 3.
 5. Configure the third access point (AP 3) in repeater mode with the remote MAC address of AP 2.
 6. Verify the following parameters for all access points:
 - The access points are configured to operate in the same LAN network address range as the LAN devices.
 - All access points need to be on the same LAN. That is, all the LAN IP addresses of the access points have to be in the same network.
 - If you are using DHCP, all access points should be set to Obtain an IP address automatically (DHCP Client). See [Set Basic IP Options](#) on page 13.
 - All access points use the same SSID, channel, authentication mode, if any, and encryption.
 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 computers or servers connected to any of the three WLAN segments.

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

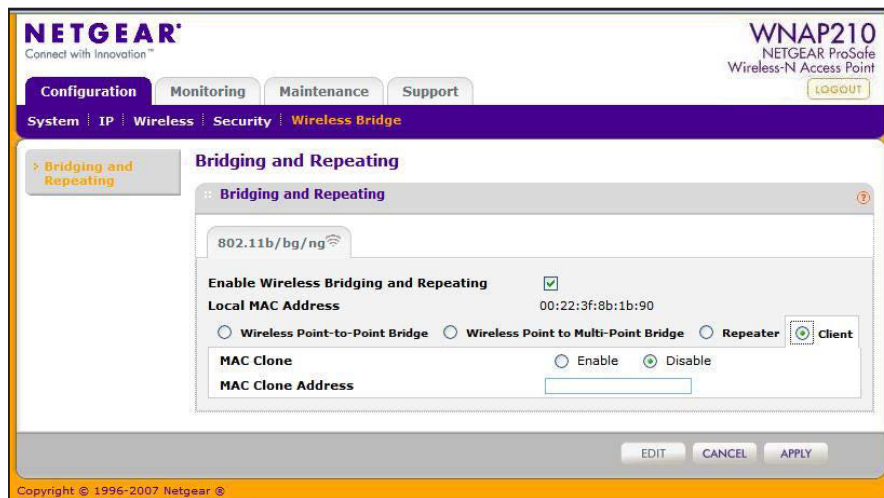
You can extend repeating by adding up to two additional access points configured in repeater mode. However, since repeater configurations communicate in half-duplex mode, the bandwidth decreases as you add repeaters to the network.

Client Mode

In client mode the access point operates as a client bridge only and sends traffic to the selected remote AP or peer device.

- To configure the access point for client mode:

1. Select **Configuration > Wireless Bridge > Bridging and Repeating**. The Bridging and Repeating screen displays.



2. Select the **Enable Wireless Bridging and Repeating** check box. This allows you to select a bridging mode.
3. Select **Client**. You can now enable the MAC clone feature. The default is Disable. If you enable the MAC clone feature, enter the MAC clone address.
4. Click **Apply**.

6 Troubleshooting and Debugging

6

This chapter includes the following sections:

- *Troubleshooting with the LEDs*
- *Cannot Connect to the Access Point to Configure It*
- *Wireless Access to the Network*
- *Time-Out Error for URL or IP Address*

Note: For up-to-date WNAP210 installation details and troubleshooting guidance, visit <http://support.netgear.com>.

Troubleshooting with the LEDs

All LEDs Are Off

It takes a few seconds for the Power LED to light. Wait a minute and check the Power LED on the access point.

If the access point has no power:

- Make sure that the power cord is connected to the 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 supplied with your access point.

LAN LED Is Off

There is a hardware connection problem. Check these items:

- Make sure that the cable connectors are securely plugged in at the access point and the network device (hub, switch, or router). A switch, hub, or router has to be installed between the access point and the Ethernet LAN or broadband modem.
- The LAN LED does not light if the link is 10 Mbps. In such cases, the LAN LED blinks if there is activity.
- 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.

WLAN LED Is Off

The wireless radio is turned off (see [Basic Wireless Setting Fields](#) on page 16), or the access point antennas are not working.

- If the WLAN LED stays off when the wireless radio is on, disconnect the adapter from its power source, and then plug it in again.
- Make sure that the antennas are securely connected to the access point.
- Contact NETGEAR technical support if the WLAN LED remains off.

Cannot Connect to the Access Point to Configure It

Check these items:

- The access point is installed correctly, LAN connections are OK, and it is powered on. Check that the LAN port LED is green to verify that the Ethernet connection is OK.
- The default configuration of the access point is for a static IP address of 192.168.0.236 and a subnet mask of 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 access point to connect, ensure that your computer and the 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.
- If your computer uses a fixed (static) IP address, ensure that it is using an IP address in the range of the access point. The default IP address is 192.168.0.236, and the default subnet mask is 255.255.255.0.

Wireless Access to the Network

If you cannot connect wirelessly, the wireless radio could be turned off in the Basic Wireless Settings screen (see *Basic Wireless Setting Fields* on page 16), or there could be a configuration problem. For a configuration problem, check these items:

- You might not have restarted the computer with the wireless adapter to have 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 Obtain an IP address automatically (DHCP client).

- The access point's default values might not work with your network. Check the access point default configuration against the configuration of other devices in your network.

Time-Out Error for URL or IP Address

A number of things could be causing this. Try the following troubleshooting steps.

- Check whether other computers on the network work without errors. If they do, ensure that your computer's TCP/IP settings are correct. If you are using a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses.
- If the computers are configured correctly, but still not working, ensure that the access point is connected and turned on. Connect to it, and check its settings. If you cannot connect to it, check the LAN and power connections.

- If the access point is configured correctly, check your Internet connection (DSL or cable modem, and so on.) to make sure that it is working correctly.
- Try again.

A Supplemental Information

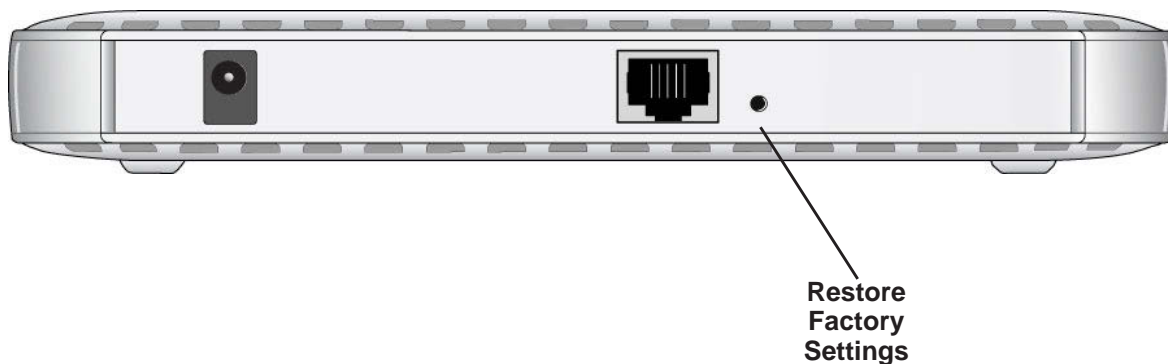


This chapter includes the following topics:

- *Factory Default Settings*
- *Technical Specifications*

Factory Default Settings

You can use the Restore Factory Settings button on the rear panel to reset all settings to their factory defaults. This is called a hard reset. Pressing this button for a shorter period of time simply causes your device to reboot.



➤ **To perform a hard reset:**

1. Use something with a small point, such as a pen, to press the **Restore Factory Settings** button in and hold it in for at least 5 seconds (until the Test LED blinks rapidly).
2. Release the button.

Your device returns to the factory configuration settings shown in the following table.

Table 5. Access point default configuration settings

Feature	Default setting
Login URL	192.168.0.236
User name (case-sensitive)	admin
Login password (case-sensitive)	password
Static IP address	192.168.0.210
Ethernet MAC address	See bottom label.
Port speed	10/100/1000
LAN IP	192.168.0.236
Subnet mask	255.255.255.0
Gateway address	0.0.0.0
DHCP client	Disabled
Time zone	USA-Pacific
Time zone adjusted for daylight saving time	Disabled
SNMP	Enabled, but trap forwarding disabled

Table 5. Access point default configuration settings (continued)

Feature	Default setting
Spanning Tree Protocol	Disabled
Secure Telnet	Enabled
Wireless operating mode	Access Point
Access point name	netgearxxxxxx, where xxxxxx represents 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
Transmission speed	Best ^a
Country/Region	Varies by region
802.11gn 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.

Technical Specifications

Table 6. Technical specifications

Feature	Description
802.11g data rates	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, & 54 Mbps (Auto-rate capable)
802.11ng data rates, channel width 20 MHz and Guard Interval short (400 ms)	Best, 7.2 Mbps, 14.4 Mbps, 21.7 Mbps, 28.9 Mbps, 43.3 Mbps, 57.8 Mbps, 65 Mbps, 72.2 Mbps, 14.44 Mbps, 28.88 Mbps, 43.33 Mbps, 57.77 Mbps, 86.66 Mbps, 115.56 Mbps, 130 Mbps, 144.44 Mbps
802.11ng data rates, channel width 40 MHz and Guard Interval short (400 ms)	Best, 15 Mbps, 30 Mbps, 45 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 135 Mbps, 150 Mbps, 30 Mbps, 60 Mbps, 90 Mbps, 120 Mbps, 180 Mbps, 240 Mbps, 270 Mbps, 300 Mbps
802.11b/bg/ng operating frequencies	<ul style="list-style-type: none"> • 2.412–2.462 GHz (US) • 2.457–2.462 GHz (Spain), • 2.412–2.484 GHz (Japan) • 2.457–2.472 GHz (France) • 2.412–2.472 GHz (Europe ETSI)
802.11 b/bg/ng encryption	64 bits, 128 and 152 bits WEP, AES, TKIP data encryption
Network management	Web-based configuration and status monitoring
Maximum number of clients	Limited by the amount of wireless network traffic generated by each node; maximum 64 supported.
Status LEDs	Power, Test, Ethernet LAN, Wireless LAN
Power adapter	12V DC, 1.0 A
Electromagnetic compliance	FCC Part 15 Class B and Class E, CE, and C-TICK
Environmental specifications	Operating temperature: 0 to 50° C Operating humidity: 5–95%, non-condensing

B. Command Line Reference

B

The ProSAFE Wireless-N Access Point WNAP210 (AP) 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 connection.

Command Sets

Keyword	Description
-----	-----
-backup-configuration	--backup configuration
-config>	--configuration setting
-apname	--access point name
-country	--country/region
-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 data 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
| | | | |
| | | | |
| | | | |
| | | | |
| | -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
-log	--system log
-system	--system setting

Index

Numerics

192.168.0.210, static IP address **11**

255.255.255.0 default subnet **11**

A

access control **30**

access point default name **18**

access point mode **40**

access point, deployment of **19**

access points, placement of multiple **10**

activity logs **44**

aggregation length **49**

AMPDU **49**

AP EDCA parameters **50**

AP lists **43**

authentication **22**

B

beacon interval **49**

C

Channel **17**

CLI command sets **66**

configuration

 backup file **36**

 erasing **37**

 restoring **36**

 retrieving configuration file **37**

 saving **37**

country **12, 40**

D

data rate **17**

default gateway **40**

default password **12**

default settings **63**

default subnet mask **11**

deployment **19**

DHCP client **14, 40**

DTIM interval **50**

dynamic IP addresses, enabling **14, 18**

E

equipment placement **10**

Ethernet RJ-45 port **8**

F

factory default settings **63**

factory default settings, restoring **37**

firmware upgrade **35**

firmware version **40**

fragmentation length **49**

frequency **17**

front panel **7**

G

gateway, default address **14**

guard interval **17**

H

hotspot settings **48**

I

installation **10**

interference sources, wireless **10**

IP address **40**

IP address, default **11, 14**

IP settings **14**

IP subnet mask, default **14**

K

known AP list **42**

L

LAN port **8**

LEDs **7**

LEDs, troubleshooting with **59**
 logs, activity **44**
 logs, syslog **37**

M

MAC address **11, 12, 40**
 restricting access **20, 29**
 MAC authentication **30**
 MCS Index **17**

N

NetBIOS name **12, 40**
 NetBIOS name, logging in **11**
 network authentication **22**
 network traffic statistics **44**
 NTP, enabling **13**

O

output power **18**

P

package contents **6**
 password
 changing **32**
 default **12**
 performance degradation, causes of **10**
 point-to-point bridge, configuring **53**
 power adapter **8**
 power, output **18**
 preamble type **50**
 primary DNS server **14**

Q

QoS **18**

R

RADIUS server settings **24, 26**
 rear panel **8**
 region **12, 40**
 remote management **32, 33**
 repeater **52**
 repeater, wireless **56**
 restore configuration **36**
 restore default settings **37**
 restricting access by MAC address **29**

RIFS transmission **50**
 rogue AP detection **41, 42**
 RTS threshold **49**

S

secondary DNS server **14**
 security options **20**
 security options, described **20**
 security profiles **21**
 authentication settings **22**
 definition **21**
 SNMP, default setting **33**
 SSID **16**
 SSID broadcast, disabling **20**
 static IP address **11**
 station EDCA parameters **50**
 statistics **44**
 syslog **37**
 system information **40**
 system requirements **6**

T

Telnet **32**
 time, setting **13**
 troubleshooting
 LAN activity **59**
 timeout error **60**
 wireless Internet connection **60**
 troubleshooting, connecting to the access point **60**
 troubleshooting, using LEDs **59**
 trusted wireless stations **30**

U

upgrade firmware **35**
 user name **12**

W

Wi-Fi Multimedia **18**
 wireless bridging **52**
 wireless bridging, client mode **52**
 wireless channel **17**
 wireless client security separation **28**
 wireless connectivity, testing **15**
 wireless mode **16**
 wireless network name **16**
 wireless radio, turning off and on **16**
 wireless range **10**

wireless repeater, configuring **56**

wireless security options **20**

wireless settings, advanced **49**

wireless stations **41**

wireless stations, trusted **30**

WPA with RADIUS **27**