ProSAFE Wireless-N Access Point WNAP320
Reference Manual
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.
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

<table>
<thead>
<tr>
<th>Publication Part Number</th>
<th>Publish Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>202-10724-03</td>
<td>November 2015</td>
<td>Revised the Support section on this page.</td>
</tr>
<tr>
<td>202-10724-02</td>
<td>October 2015</td>
<td>Removed the Notification of Compliance appendix and provided a Notification of Compliance link on this page.</td>
</tr>
<tr>
<td>202-10724-01</td>
<td>January 2011</td>
<td>First publication</td>
</tr>
</tbody>
</table>
Chapter 1  Introduction

About the ProSAFE Wireless-N Access Point WNAP320 ............................. 6
What Is In the Box? .................................................................................. 7
System Requirements ............................................................................. 7
Key Features and Standards ................................................................. 7
   Supported Standards and Conventions ........................................... 8
   Key Features ....................................................................................... 8
   802.11b/g/n Standards–Based Wireless Networking ...................... 10
   Autosensing Ethernet Connections with Auto Uplink .................... 10
Hardware Description ........................................................................... 10
   Top Panel ......................................................................................... 11
   Rear Panel ....................................................................................... 12
   Bottom Panel with Product Label .................................................. 13

Chapter 2  Installation and Basic Configuration

What You Need before You Begin .......................................................... 14
   Wireless Equipment Placement and Range Guidelines ................. 14
   Ethernet Cabling Requirements ...................................................... 15
   LAN Configuration Requirements .................................................. 15
   Computer Hardware Requirements ................................................. 15
Install and Configure the Wireless Access Point .................................. 16
   Connect the Wireless Access Point to Computer ......................... 16
   Log In to the Wireless Access Point ............................................... 18
   Configure Basic General System Settings and Time Settings ......... 19
   Configure IP Settings and Optional DHCP Server Settings .......... 21
   Configure Basic Wireless Settings ................................................. 23
Test Basic Wireless Connectivity ......................................................... 27
Mount the Wireless Access Point .......................................................... 28
   Ceiling Installation ......................................................................... 28
   Wall Installation .............................................................................. 30
   Desk Installation ............................................................................. 33

Chapter 3  Wireless Configuration and Security

Wireless Data Security Options .............................................................. 34
   Security Profiles ............................................................................. 36
   Before You Change the SSID, WEP, and WPA Settings ............... 38
   Configure and Enable Security Profiles ....................................... 39
   Configure RADIUS Server Settings .............................................. 48
   Restrict Wireless Access by MAC Address ................................... 50
Testing the LAN Path to Your Wireless Access Point .............. 101
Testing the Path from Your Computer to a Remote Device ....... 102
Problems with Date and Time ............................................. 103
Use the Packet Capture Tool ............................................. 103

Appendix A  Supplemental Information

Related Documents ......................................................... 105
Technical Specifications .................................................. 106
Factory Default Settings .................................................. 107

Appendix B  Command-Line Reference

Index
This chapter introduces the ProSAFE Wireless-N Access Point WNAP320 and describes some of the key features. This chapter includes the following sections:

• About the ProSAFE Wireless-N Access Point WNAP320 on this page
• What Is In the Box? on page 7
• System Requirements on page 7
• Key Features and Standards on page 7
• Hardware Description on page 10

About the ProSAFE Wireless-N Access Point WNAP320

The ProSAFE Wireless-N Access Point WNAP320 is the basic building block of a wireless LAN infrastructure. It provides connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices.

The wireless access point provides wireless connectivity to multiple wireless network devices within a fixed range or area of coverage—interacting with a wireless network interface card (NIC) through an antenna. Typically, an individual in-building wireless access point provides a maximum connectivity area of about a 500-foot radius. The ProSAFE Wireless-N Access Point WNAP320 can support up to 64 users simultaneously in a range of several hundred feet.

The ProSAFE Wireless-N Access Point WNAP320 acts as a bridge between the wired LAN and wireless clients. Connecting multiple wireless access points through a wired Ethernet backbone can further increase the wireless network coverage. As a mobile computing device moves out of the range of one wireless access point, it moves into the range of another. As a result, wireless clients can freely roam from one wireless access point to another and still maintain seamless connection to the network.

The autosensing capability of the ProSAFE Wireless-N Access Point WNAP320 allows packet transmission at up to 300 Mbps, or at reduced speeds to compensate for distance or electromagnetic interference.
What Is In the Box?

The product package should contain the following items:

- ProSAFE Wireless-N Access Point WNAP320
- Power adapter and cord (12 VCD, 1.0A)
- Straight-through Category 5 Ethernet cable
- NETGEAR ProSAFE WNAP320 Wireless-N Access Point Installation Guide
- Resource CD, which includes this manual
- Wall-mount kit made up of brackets and hardware

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

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


System Requirements

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

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

Key Features and Standards

The ProSAFE Wireless-N Access Point WNAP320 is easy to use and provides solid wireless and networking support. It also offers a wide range of security options.
Supported Standards and Conventions

The ProSAFE Wireless-N Access Point WNAP320 supports the following standards and conventions:

- **Standards compliance.** The wireless access point complies with the IEEE 802.11 b/g standards for wireless LANs, and is Wi-Fi certified for 802.11n standard.

- **Full WPA and WPA2 support.** The wireless access point provides WPA and WPA2 enterprise-class strong security with RADIUS and certificate authentication as well as dynamic encryption key generation. The WPA-PSK and WPA2-PSK preshared key authentication is without the overhead of RADIUS servers but with all of the strong security of WPA.

- **Multiple BSSIDs.** The wireless access point supports multiple BSSIDs. When a wireless access point is connected to a wired network and a set of wireless stations, it is called a basic service set (BSS). The basic service set identifier (BSSID) is a unique identifier attached to the header of packets sent over a WLAN that differentiates one WLAN from another when a mobile device tries to connect to the network.

  The multiple BSSID feature allows you to configure up to eight SSIDs on your wireless access point and assign different configuration settings to each SSID. All the configured SSIDs are active, and the network devices can connect to the wireless access point by using any of these SSIDs.

- **DHCP client support.** DHCP provides a dynamic IP address to PCs and other devices upon request. The wireless access point can act as a client and obtain information from your DHCP server; it can also act as a DHCP server and provide network information for wireless clients.


- **802.1Q VLAN (virtual LAN) support.** A network of computers that behave as if they are connected to the same network even though they might actually be physically located on different segments of a LAN. VLANs are configured through software rather than hardware, which makes them extremely flexible. VLANs are very useful for user and host management, bandwidth allocation, and resource optimization.

Key Features

The ProSAFE Wireless-N Access Point WNAP320 provides solid functionality, including the following features:

- **Multiple operating modes:**
  - **Wireless access point.** Operates as a standard 802.11b/g/n wireless access point.
  - **Point-to-point bridge.** In this mode, the wireless access point communicates only with another bridge-mode wireless station or wireless access point. Network authentication should be used to protect this communication.
  - **Point-to-multipoint bridge.** Select this only if this wireless access point is the master for a group of bridge-mode wireless stations. The other bridge-mode wireless stations
send all traffic to this master, and do not communicate directly with each other. Network authentication should be used to protect this traffic.

- **Wireless repeater.** In this mode, the wireless access point does not function as an access point but communicates only with wireless stations that function in repeater mode, point-to-point bridge mode, and point-to-multipoint-bridge mode. Network authentication should be used to protect this communication.

- **Client.** In this mode, the wireless access point functions as a client bridge only, and sends all traffic to a remote wireless access point or peer device.

- **Hotspot settings.** You can allow all HTTP (TCP, port 80) requests to be captured and redirected to the URL you specify.

- **Upgradeable firmware.** Firmware is stored in a flash memory. You can upgrade it easily, using only your Web browser, and you can upgrade it remotely. You can also use the command-line interface.

- **Rogue AP detection.** The Rogue AP filtering feature ensures that unknown APs are not given access to any part of the LAN.

- **Access control.** The Access Control MAC address filtering feature can ensure that only trusted wireless stations can use the wireless access point to gain access to your LAN.

- **Security profiles.** When using multiple BSSIDs, you can configure unique security settings (encryption, SSID, and so on) for each BSSID.

- **Hidden mode.** The SSID is not broadcast, assuring only clients configured with the correct SSID can connect.

- **Configuration backup.** Configuration settings can be backed up to a file and restored.

- **Secure and economical operation.** Adjustable power output allows more secure or economical operation.

- **Power over Ethernet.** Power can be supplied to the wireless access point over the Ethernet port from any 802.3af-compliant midspan or end-span source.

- **Autosensing Ethernet connection with Auto Uplink™ interface.** Connects to 10/100/1000 Mbps IEEE 802.3 Ethernet networks.

- **LED indicators.** Power/Test, Active, LAN, and WLAN for each radio mode are easily identified.

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

- **Quality of Service (QoS) support.** You can configure parameters that affect traffic flowing from the wireless access point to the client station and traffic flowing from the client station to the wireless access point. The QoS feature allows you to prioritize traffic, such as voice and video traffic, so that packets do not get dropped.

- **VLAN security profiles.** Each security profile is automatically allocated a VLAN ID when the security profile is modified.
802.11b/g/n Standards–Based Wireless Networking

The ProSAFE Wireless-N Access Point WNAP320 provides a bridge between wired Ethernet LANs and 802.11b/g- and 802.11n-compatible wireless LAN networks. It provides connectivity between wired Ethernet networks and radio-equipped wireless notebook systems, desktop systems, print servers, and other devices. Additionally, the wireless access point supports the following wireless features:

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

Autosensing Ethernet Connections with Auto Uplink

The ProSAFE Wireless-N Access Point WNAP320 can connect to a standard Ethernet network. The LAN interface is autosensing and capable of full-duplex or half-duplex operation.

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

Hardware Description

This section describes the top and rear hardware functions of the ProSAFE Wireless-N Access Point WNAP320.
Top Panel

The ProSAFE Wireless-N Access Point WNAP320 LEDs are described in the following figure and table:

![Top Panel Diagram](image)

Figure 1.

Table 1. Top Panel LEDs

<table>
<thead>
<tr>
<th>Item</th>
<th>LED</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image" alt="Power/Test LED" /></td>
<td><strong>Power/Test</strong></td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Power is off.</td>
</tr>
<tr>
<td></td>
<td>On (green)</td>
<td>Power is on.</td>
</tr>
<tr>
<td></td>
<td>Amber, then blinking green</td>
<td>A self-test is running or software is being loaded. During startup, the LED is first steady amber, then goes off, and then blinks green before turning steady green after about 45 seconds. If after 1 minute the LED remains amber or continues to blink green, it indicates a system fault.</td>
</tr>
<tr>
<td>2</td>
<td><img src="image" alt="Active LED" /></td>
<td><strong>Active</strong></td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>No Ethernet traffic is detected or no link is detected.</td>
</tr>
<tr>
<td></td>
<td>On or blinking (green)</td>
<td>Ethernet traffic is detected.</td>
</tr>
<tr>
<td>3</td>
<td><img src="image" alt="LAN LED" /></td>
<td><strong>LAN</strong></td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>10 Mbps or no link is detected.</td>
</tr>
<tr>
<td></td>
<td>Amber</td>
<td>10/100 Mbps link is detected.</td>
</tr>
<tr>
<td></td>
<td>Green</td>
<td>1000 Mbps link is detected.</td>
</tr>
<tr>
<td>4</td>
<td><img src="image" alt="WLAN LED" /></td>
<td><strong>WLAN</strong></td>
</tr>
<tr>
<td></td>
<td>Off</td>
<td>Wireless LAN is not ready or no wireless activity is detected.</td>
</tr>
<tr>
<td></td>
<td>On or blinking (green)</td>
<td>Wireless LAN is ready or wireless activity is detected.</td>
</tr>
</tbody>
</table>
Rear Panel

The rear panel functions of the ProSAFE Wireless-N Access Point WNAP320 are described in the following list:

1. Reverse SMA connector for an optional 2.4-GHz antenna.
2. Factory default Reset button. Using a sharp object, press and hold this button for about 5 seconds to reset the wireless access point to factory defaults settings. All configuration settings are lost, and the default password is restored. For more information, see Restore the Wireless Access Point to the Factory Default Settings on page 62.
3. Console port for connecting to an optional console terminal. The port has a DB9 male connector and supports the following settings: 9600 K default baud rate, (8) data bits, no (N) parity bit, and one (1) stop bit.
4. 10/100/1000BASE-T Gigabit Ethernet (RJ-45) port with Auto Uplink (Auto MDI-X) with IEEE 802.3af Power over Ethernet (PoE) support for connection to a switch or router.
5. Cable security lock receptacle for an optional lock.
6. Power socket for a 12 VDC, 1A power adapter.
7. Reverse SMA connector for an optional 2.4-GHz antenna.
Bottom Panel with Product Label

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

![Product Label Image]

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

- What You Need before You Begin on this page
- Install and Configure the Wireless Access Point on page 16
- Test Basic Wireless Connectivity on page 27
- Mount the Wireless Access Point on page 28

Note: In this chapter and in all further chapters, the WNAP320 is referred to as the wireless access point.

What You Need before You Begin

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

Wireless Equipment Placement and Range Guidelines

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

Note: Failure to follow these guidelines can result in significant performance degradation or inability to wirelessly connect to the wireless access point. For complete performance specifications, see Appendix A, Supplemental Information.
For best results, place your wireless access point according to the following general guidelines:

- Near the center of the area in which your PCs will operate.
- In an elevated location such as a high shelf where the wirelessly connected PCs have line-of-sight access (even if through walls).
- Away from sources of interference, such as PCs, microwaves ovens, and 2.4-GHz cordless phones.
- Away from large metal surfaces or water.
- Placing an external antenna in a vertical position provides best side-to-side coverage. Placing an external antenna in a horizontal position provides best up-and-down coverage. (An external antenna does not come standard with the WNAP320 wireless access point.)
- If you are using multiple wireless access points, it is better if adjacent wireless access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent wireless access points is five channels (for example, use channels 1 and 6, or 6 and 11, or 1 and 11).

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

**Ethernet Cabling Requirements**

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

**LAN Configuration Requirements**

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

**Note:** For assistance with DHCP configuration, see the *Preparing Your Network* document that you can access from Related Documents in Appendix A.

**Computer Hardware Requirements**

To connect to the wireless access point on your network, each computer must have a 802.11b/g or 802.11n wireless adapter installed.
Install and Configure the Wireless Access Point

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

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

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

1. Connect the Wireless Access Point to Computer on this page.
2. Log In to the Wireless Access Point on page 18.
4. Configure IP Settings and Optional DHCP Server Settings on page 21

Connect the Wireless Access Point to Computer

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

To set up the wireless access point:

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

6. Connect the power adapter to the wireless access point.

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

7. Verify the following:

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

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

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

   **WLAN LED.** The WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready.
Log In to the Wireless Access Point

The default IP address of your wireless access point is http://192.168.0.100. The wireless access point is set, by default, for the DHCP client to be disabled.

To log in to the wireless access point:

1. Open a Web browser such as Microsoft Internet Explorer 6.0 or later, or Mozilla Firefox 1.5 or later.
2. Connect to the wireless access point by entering its default address of http://192.168.0.100 into your browser.

The Login screen opens:

3. Enter the default user name of admin and the default password of password.
4. Click Login. The Web browser displays the basic General system settings screen under the Configuration tab of the main menu as shown in Figure 8 on page 19.

Web Management Interface

The navigation tabs across the top of the Web Management Interface provide access to all the configuration functions of the wireless access point, and remain constant. The menu items in the blue bar change according to the navigation tab that is selected.
The bottom right corner of all screens that allow you to make configuration changes show the Apply and Cancel buttons, and on several screens the Edit button.

Figure 7.

These buttons have the following functions:

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

**Configure Basic General System Settings and Time Settings**

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

To configure basic system settings:

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

Figure 8.
2. Specify the fields as explained in the following table:

Table 2. Basic General System Settings

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

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

To configure time settings:

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

![Time Screen](image)

   **Figure 9.**

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

Table 3. Time System Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time Zone</td>
<td>Select the time zone to match your location.</td>
</tr>
<tr>
<td>Current Time</td>
<td>This is a nonconfigurable field that displays the current date and time.</td>
</tr>
<tr>
<td>NTP Client</td>
<td>Enable the Network Time Protocol (NTP) client to synchronize the time of the wireless access point with an NTP server. By default the Enable radio button is selected.</td>
</tr>
</tbody>
</table>
Table 3. Time System Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Custom NTP Server</td>
<td>Select this check box to If you want to use a custom NTP server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must have an Internet connection to use an NTP server that is</td>
</tr>
<tr>
<td></td>
<td>not on your local network.</td>
</tr>
<tr>
<td>Hostname / IP Address</td>
<td>Enter the host name or IP address of the custom NTP server. The default is</td>
</tr>
<tr>
<td></td>
<td>time-b.netgear.com.</td>
</tr>
</tbody>
</table>

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

**Configure IP Settings and Optional DHCP Server Settings**

To configure the IP settings:

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

![IP Settings Screen](image)

Figure 10.

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

Table 4. IP Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Client</td>
<td>By default, the Dynamic Host Configuration Protocol (DHCP) client is disabled. If you have a DHCP server on your LAN and you select the Enable check box, the wireless access point will receive its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the wireless access point to your LAN.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of your wireless access point. The default IP address is <strong>192.168.0.100</strong>. To change the address, enter an unused IP address from the address range used on your LAN, or enable DHCP the server.</td>
</tr>
</tbody>
</table>
Table 4. IP Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Subnet Mask</td>
<td>Enter the network number portion of an IP address. Unless you are implementing subnetting, enter <strong>255.255.0.0</strong> as the subnet mask.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>Enter the IP address of the ISP’s router to which the wireless access point will connect.</td>
</tr>
<tr>
<td>Primary DNS Server</td>
<td>Enter the IP address of the primary and secondary DNS servers. A DNS server is a host on the Internet that translates Internet names (such as <a href="http://www.netgear.com">www.netgear.com</a>) to numeric IP addresses. Typically your ISP transfers the IP address of one or two DNS servers to your wireless access point during login. If the ISP does not transfer an address, you must obtain it from the ISP and enter it manually in this field.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td>Network Integrity Check Select this check box to validate that the upstream link is active before allowing wireless associations. Ensure that the default gateway is configured.</td>
</tr>
</tbody>
</table>

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

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

**To configure DHCP server settings:**

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

![DHCP Server Settings](image)

Figure 11.
2. Specify the fields as explained in the following table:

Table 5. LAN Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Select the <strong>DHCP Server</strong> check box to enable the DHCP server. Use the default settings or specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the wireless access point's LAN IP address.</td>
</tr>
<tr>
<td>DHCP Server VLAN ID</td>
<td>Enter the DHCP server VLAN ID. The VLAN ID range is between 1 and 4094.</td>
</tr>
<tr>
<td>Starting IP Address</td>
<td>Enter the first address in the range of IP addresses to be assigned to DHCP clients. The default address is 192.168.1.02.</td>
</tr>
<tr>
<td>Ending IP Address</td>
<td>Enter the last address in the range of IP addresses to be assigned to DHCP clients. The default address is 192.168.1.50.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the subnet mask to be used by DHCP clients. The default mask is 255.255.255.0.</td>
</tr>
<tr>
<td>Gateway IP Address</td>
<td>Enter the IP address of the default routing gateway to be used by DHCP clients. The default address is 192.168.0.1.</td>
</tr>
<tr>
<td>Primary DNS Address</td>
<td>Enter the IP address of the primary Domain Name Server (DNS) server available to DHCP clients.</td>
</tr>
<tr>
<td>Secondary DNS Address</td>
<td>Enter the IP address of the secondary DNS server available to DHCP clients.</td>
</tr>
<tr>
<td>Primary WINS Server</td>
<td>Enter the IP address of the primary WINS server for the network.</td>
</tr>
<tr>
<td>Secondary WINS Server</td>
<td>Enter the IP address of the secondary WINS server for the network.</td>
</tr>
<tr>
<td>Lease</td>
<td>Enter the period that the DHCP server grants to DHCP clients to use the assigned IP addresses. The default time is 1 day.</td>
</tr>
</tbody>
</table>

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

**Configure Basic Wireless Settings**

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

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

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

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

![Wireless Settings Configuration](image)

Figure 12.
2. Specify the fields as explained the following table:

**Table 6. Basic Wireless Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Mode</td>
<td>Select the wireless operating mode that you want to use by selecting one of the following radio buttons:</td>
</tr>
<tr>
<td></td>
<td>• <strong>11b</strong>. 802.11b wireless stations only.</td>
</tr>
<tr>
<td></td>
<td>• <strong>11bg</strong>. Both 802.11b and 802.11g wireless stations can be used.</td>
</tr>
<tr>
<td></td>
<td>• <strong>11ng</strong>. Both 802.11n and 802.11g wireless stations can be used. This is the default setting.</td>
</tr>
<tr>
<td>Turn Radio On</td>
<td>The radio is enabled by default. To turn off the radio, clear the <strong>Turn Radio On</strong> check box. Doing so disables access through the wireless access point, which can be helpful for configuration, network tuning, or troubleshooting activities.</td>
</tr>
<tr>
<td>Wireless Network Name (SSID)</td>
<td>Enter a 32-character (maximum) service set identifier (SSID); the characters are case-sensitive. The default is NETGEAR_11ng. The SSID assigned to a wireless device must match the wireless access point’s SSID for the wireless device to communicate with the wireless access point. If the SSIDs do not match, you will not get a wireless connection to the wireless access point.</td>
</tr>
<tr>
<td>Scheduler Status</td>
<td>This is a nonconfigurable field that show the status of the wireless scheduler. For more information, see <em>Schedule the Wireless Radio</em> on page 52.</td>
</tr>
<tr>
<td>Broadcast Wireless Network Name (SSID)</td>
<td>Select the <strong>Yes</strong> radio button to enable the wireless access point to broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point's SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the <strong>No</strong> radio button.</td>
</tr>
<tr>
<td>Channel / Frequency</td>
<td>From the drop-down list, select the channel you wish to use on your wireless LAN. The wireless channels to use in the United States and Canada are 1 to 11; for Europe and Australia, 1 to 13. The default setting is Auto.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). Should this happen, you might want to experiment with different channels to see which is the best. For more information, see the guidelines following this table.</td>
</tr>
<tr>
<td>11ng mode only</td>
<td><strong>Note:</strong> For most networks, the default settings will work fine.</td>
</tr>
<tr>
<td><strong>MCS Index / Data Rate</strong></td>
<td>From the drop-down list, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the wireless network. The default setting is Best. For a list of all options that you can select from in 11ng mode, see <em>Factory Default Settings</em> in Appendix A.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>From the drop-down list, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, or 40 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz.</td>
</tr>
<tr>
<td>Ext Protection Spacing</td>
<td>When you select a channel width of Dynamic 20/40 MHz or 40 MHz, you also need to select protection spacing for the extension channel from the Ext Protection Spacing drop-down list. In addition to the default value Auto, you can also select a value of 20 or 25.</td>
</tr>
</tbody>
</table>
Chapter 2. Installation and Basic Configuration

3. If you have changed the wireless mode and selected the Turn Radio On check box, a popup window appears: click OK to confirm your change.

4. Click Apply to save your settings.

You should not need to change the operating frequency (channel) unless you notice interference problems, or are setting up the wireless access point near another wireless access point. Observe the following guidelines:

- Wireless access points use a fixed channel. You can select a channel that provides the least interference and best performance. In the United States and Canada, 11 channels are available.

- If you are using multiple wireless access points, it is better if adjacent wireless access points use different channels to reduce interference. The recommended channel spacing between adjacent wireless access points is 5 channels (for example, use channels 1 and 6, or 6 and 11).

- In infrastructure mode, wireless stations normally scan all channels, looking for a wireless access point. If more than one wireless access point can be used, the one with the strongest signal is used. This can happen only when the wireless access points use the same SSID. The WNAP320 wireless access point functions in infrastructure mode by default.

### Table 6. Basic Wireless Settings (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>11ng mode only (continued)</td>
<td></td>
</tr>
<tr>
<td>Ext Channel Offset</td>
<td>When you select a channel width of Dynamic 20/40 MHz or 40 MHz, you also need to select the offset for the extension channel from the Ext Channel Offset drop-down list. In addition to the default value Auto, you can also select Upper or Lower.</td>
</tr>
<tr>
<td>Guard Interval</td>
<td>From the drop-down list, select the guard interval to protect transmissions from interference. In addition to the default value Auto, you can also select Long - 800 ns. Some legacy devices can operate only with a long guard interval.</td>
</tr>
<tr>
<td>11b and 11bg modes only</td>
<td></td>
</tr>
<tr>
<td>Data Rate</td>
<td>From the drop-down list, select the transmit data rate of the wireless network. The default setting is Best. For a list of all options that you can select from in 11b mode and 11bg mode, see Factory Default Settings in Appendix A.</td>
</tr>
<tr>
<td>Output Power</td>
<td>From the drop-down list, select the transmission power of the wireless access point. The default is Full.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Increasing the power improves performance, but if two or more wireless access points are operating in the same area, on the same channel, it can cause interference.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country.</td>
</tr>
<tr>
<td>Channel Bonding</td>
<td>This drop-down list lets you to specify channels to bond. The available options are 20 MHz, 20/40 MHz, and 40 MHz.</td>
</tr>
</tbody>
</table>
Test Basic Wireless Connectivity

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

To test for wireless connectivity:

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

WARNING!

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

In addition to wireless security and other wireless features, before you deploy the wireless access point in your network, configure any additional features as described in Chapter 4, Management and Chapter 5, Advanced Configuration.
After you have completed the configuration of the wireless access point, you can reconfigure the computer that you used for this process back to its original TCP/IP settings.

Mount the Wireless Access Point

This section includes the following subsections:

- Ceiling Installation on this page
- Wall Installation on page 30
- Desk Installation on page 33

Ceiling Installation

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

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

2. Detach the mounting plate from the wireless access point.
3. Attach the clamp to the ceiling rail.

4. Attach the mounting plate to the clamp.

5. Connect the cables to the wireless access point.
6. Attach the wireless access point to the mounting plate.

7. Attach the cover to the wireless access point.

Wall Installation

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

1. Verify the package content of the wall installation kit.
2. Detach the mounting plate from the wireless access point.

3. Attach the mounting plate to the wall.

4. Connect the cables to the wireless access point.
5. Attach the wireless access point to the mounting plate.

6. Attach the cover to the wireless access point.
Desk Installation

To install the wireless access point on a desk, attach the rubber feet to the holes in the bottom of the wireless access point.
This chapter describes how to configure the wireless features of your ProSAFE Wireless-N Access Point WNAP320. The chapter includes the following sections:

- **Wireless Data Security Options** on this page
- **Security Profiles** on page 36
- **Configure RADIUS Server Settings** on page 48
- **Restrict Wireless Access by MAC Address** on page 50
- **Schedule the Wireless Radio** on page 52
- **Configure Basic Wireless Quality of Service** on page 52

Before you set up wireless security and additional wireless features that are described in this chapter, connect the wireless access point, get the Internet connection working, and configure the 802.11b, 11bg, or 11ng wireless settings as described in *Chapter 2, Installation and Basic Configuration*. The wireless access point should work with an Ethernet LAN connection, and wireless connectivity should have been verified before you set up wireless security and additional wireless features. In planning your wireless network, consider the level of security required.

**WARNING!**

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

### Wireless Data Security Options

Indoors, computers can connect over 802.11n wireless networks at a maximum range of 300 feet. Typically, a wireless access point inside a building works best with devices within a 100 foot radius. Such distances can allow for others outside your immediate area to access your network.
Unlike wired network data, your wireless data transmissions can extend beyond your walls and can be received by anyone with a compatible adapter. For this reason, use the security features of your wireless equipment. The wireless access point provides highly effective security features that are covered in detail in this chapter. Deploy the security features appropriate to your needs.

Figure 13.

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

- **Use multiple BSSIDs combined with VLANs.** You can configure combinations of VLANs and BSSIDs with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network. For information about how to configure BSSIDs, see *Configure and Enable Security Profiles* on page 39.

- **Restrict access based by MAC address.** You can allow only trusted PCs to connect so that unknown PCs cannot wirelessly connect to the wireless access point. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see *Restrict Wireless Access by MAC Address* on page 50.

- **Turn off the broadcast of the wireless network name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn off broadcast of the SSID, see *Configure and Enable Security Profiles* on page 39.

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP shared key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK.

  For information about how to configure WEP, see *Configure and Enable Security Profiles* on page 39 and *Configure an Open System with WEP or Shared Key with WEP* on page 43.

- **Legacy 802.1X.** Legacy 80.1X uses RADIUS-based 802.1x authentication but no data encryption.
• **WPA and WPA-PSK (TKIP).** Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. The very strong authentication along with dynamic per frame rekeying of WPA make it virtually impossible to compromise.

WPA uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 39 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 45.

WPA-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 39 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 46.

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

WPA2 uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 39 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 45.

WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 39 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 46.

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

WPA & WPA2 uses RADIUS-based 802.1x authentication; for more information, see *Configure and Enable Security Profiles* on page 39 and *Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS* on page 45.

WPA-PSK & WPA2-PSK uses a pre-shared key (PSK) for authentication; for more information, see *Configure and Enable Security Profiles* on page 39 and *Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK* on page 46.

**Security Profiles**

Security profiles let you configure unique security settings for each SSID. The wireless access point supports up to eight BSSIDs that you can configure on the individual Edit Wireless Network screens that are accessible from the Edit Security Profile screen (see *Configure and Enable Security Profiles* on page 39).
To set up a security profile you select its network authentication type, data encryption, wireless client security separation, and VLAN ID:

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

  For information about the types of network authentication that the wireless access point supports, see *Configure and Enable Security Profiles* on page 39.

- **Data encryption**  
  Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data encryption settings are explained in *Configure and Enable Security Profiles* on page 39.

- **Wireless client security separation**  
  If enabled, the associated wireless clients (using the same SSID) will not be able to communicate with each other. This feature is useful for hotspots and other public access situations. By default, wireless client separation is disabled. For more information, see *Configure and Enable Security Profiles* on page 39.

- **VLAN ID**  
  If enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802.1Q) standard, the default VLAN ID for the wireless access point will be associated with each profile. The default VLAN ID must match the IDs that are used by the other network devices. For more information, see *Configure and Enable Security Profiles* on page 39.

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

- A basic service set (BSS) is a group of wireless stations and a single wireless access point, all using the same service set identifier (BSSID).
- An extended service set (ESS) is a group of wireless stations and multiple wireless access points, all using the same identifier (ESSID).
- Different wireless access points within an ESS can use different channels. To reduce interference, adjacent wireless access points should use different channels.
- Roaming is the ability of wireless stations to connect wirelessly when they physically move from one BSS to another within the same ESS. The wireless station automatically changes to the wireless access point with the least interference or best performance.
Before You Change the SSID, WEP, and WPA Settings

For a new wireless network, print or copy this form and fill in the settings. For an existing wireless network, the network administrator can provide this information. Be sure to set the Country/Region correctly as the first step. Store this information in a safe place.

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

  SSID: ___________________________________

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

- **WEP Key Size, Key Format Passphrase, and Authentication**
  Choose the key size by circling one: 64, 128, or 152 bits.
  Choose the key format by circling one: ASCII or HEX.
  Choose the authentication type by circling one: Open or Shared.

  Passphrase: ___________________________________

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

- **WPA-PSK (Pre-Shared Key) and WPA2-PSK**
  Record the WPA-PSK passphrase:

  WPA-PSK Passphrase: ____________________________

  Record the WPA2-PSK passphrase:

  WPA2-PSK Passphrase: ____________________________

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

  Server Name/IP Address: Primary __________ Secondary __________

  Port: ____________________________

  Shared Secret: ____________________________

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

  Server Name/IP Address: Primary __________ Secondary __________

  Port: ____________________________

  Shared Secret: ____________________________
Configure and Enable Security Profiles

To configure and enable a security profile:

1. Select Configuration > Security > Profile Settings. The Profile Settings screen displays, showing eight wireless security profiles:

![Profile Settings Screen]

Figure 14.

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>The unique name of the wireless security profile that makes it easy to recognize the profile.</td>
</tr>
<tr>
<td>SSID</td>
<td>The wireless network name (SSID) for the wireless security profile.</td>
</tr>
<tr>
<td>Security</td>
<td>The configured wireless authentication method for the wireless security profile.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The default VLAN ID that is associated with the wireless security profile.</td>
</tr>
<tr>
<td>Enable</td>
<td>The check box that lets you select the wireless security profile so you can enable it by clicking <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

2. To configure or edit a wireless security profile, select the corresponding radio button to the left of the wireless security profile. The Edit Security Profile screen opens for the selected wireless security profile (see the following figure). The first section on the screen is the Profile Definition section; the second section is the Authentication Settings section. These sections are explained separately.
3. Specify the settings of the Profile Definition section of the Edit Security Profile screen as explained in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Enter a unique name of the wireless security profile that makes it easy to recognize the profile. The default names are NETGEAR, NETGEAR-1, NETGEAR-2, and so on through NETGEAR-7. You can enter a value of up to 32 alphanumeric characters.</td>
</tr>
<tr>
<td>Wireless Network Name (SSID)</td>
<td>The wireless network name (SSID) for the wireless security profile. The default names are NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, and so on through NETGEAR_11ng-7.</td>
</tr>
<tr>
<td>Broadcast Wireless Network Name (SSID)</td>
<td>Select the Yes radio button to enable the wireless access point to broadcasts its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point’s SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button.</td>
</tr>
</tbody>
</table>

4. Specify the settings of the Authentication Settings section of the Edit Security Profile screen as explained in the following table.
The wireless access point is set by default as an open system with no authentication. When you configure network authentication, bear in mind the following:

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

### Table 9. Authentication Settings of the Edit Security Profile Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Note: The data encryption fields that are displayed on screen depend on your selection from the Network Authentication drop-down list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Authentication and Data Encryption</td>
<td>Open System This is the default setting. You can use an open system without any encryption or with WEP encryption. See Configure an Open System with WEP or Shared Key with WEP on page 43.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shared Key You must use WEP encryption and enter at least one shared key. See Configure an Open System with WEP or Shared Key with WEP on page 43.</td>
<td></td>
</tr>
<tr>
<td>Legacy 802.1x</td>
<td>You must configure the RADIUS server settings to use this option. See Configure Legacy 802.1X on page 45.</td>
<td></td>
</tr>
<tr>
<td>WPA with RADIUS</td>
<td>You must configure the RADIUS server settings to use this option. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA &amp; WPA2 with RADIUS on page 45.</td>
<td></td>
</tr>
<tr>
<td>WPA2 with RADIUS</td>
<td>Select this setting only if all clients support WPA2. If selected, you must use AES encryption and configure the RADIUS server settings. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA &amp; WPA2 with RADIUS on page 45.</td>
<td></td>
</tr>
<tr>
<td>WPA and WPA2 with RADIUS</td>
<td>Select this setting to allow clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and configure the RADIUS server settings. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA &amp; WPA2 with RADIUS on page 45.</td>
<td></td>
</tr>
<tr>
<td>WPA-PSK</td>
<td>You must use TKIP or TKIP + AES encryption and enter a WPA passphrase (network key). See Configure WPA-PSK, WPA2-PSK, and WPA-PSK &amp; WPA2-PSK on page 46.</td>
<td></td>
</tr>
</tbody>
</table>
Network Authentication and Data Encryption (continued)

- **WPA2-PSK**: Select this only if all clients support WPA2. If selected, you must use AES and TKIP + AES encryption and enter a WPA passphrase (network key). See Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 46.

- **WPA-PSK and WPA2-PSK**: Select this setting to allow clients to use either WPA (with TKIP) or WPA2 (with AES). If selected, you must use TKIP + AES encryption and enter a WPA passphrase (network key). See Configure WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK on page 46.

**Wireless Client Security Separation**

If you enable wireless client security separation by selecting **Enable** from the drop-down list, the associated wireless clients are not be able to communicate with each other. By default, **Disable** is selected from the drop-down list. This feature is intended for hotspots and other public access situations.

**Dynamic VLAN**

From the drop-down list, select how VLANs operate by making one of the following selections:

- **Disable**: Disables dynamic VLANs, and enables static VLANs. This is the default setting.
- **Optional**: Enables dynamic VLANs but if a RADIUS server does not return a VLAN ID, the wireless station is still allowed to connect to the wireless access point.
- **Required**: Enables dynamic VLANs. If a RADIUS server does not return a VLAN ID, the wireless station is not authenticated and cannot connect to the wireless access point.

For dynamic VLANs to operate (that is, the selection is Optional or Required), the following is required:

- The hubs and switches on your LAN must support the VLAN (802.1Q) standard.
- The authentication is set to any RADIUS type authentication: either the network authentication in the wireless security profile or the remote MAC address database authentication for the MAC Authentication feature can be used.

**VLAN ID**

Enter the default VLAN ID that must be associated with this wireless security profile. The default VLAN ID is 1. The VLAN ID must match the VLAN ID that is used by the other devices in your network.
5. Click **Apply** to save your settings.

**WARNING!**

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

For more information about wireless security options, see the *Wireless Networking Basics* document that you can access from **Related Documents** in Appendix A.

**Configure an Open System with WEP or Shared Key with WEP**

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

- **Open System with WEP**
  
  An open system can function without any encryption or with pre-shared WEP key encryption without RADIUS authentication. The security level of static WEP is not very strong.
When you select **Open System** from the Network Authentication drop-down list and any selection other than None from the Data Encryption drop-down list, the screen expands to display the WEP fields:

![Authentication Settings](image1)

**Figure 16.**

- **Shared Key with WEP**

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

  ![Authentication Settings](image2)

  **Figure 17.**

**Table 10. WEP Encryption Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
</table>
| **Data Encryption** | Select the encryption key size from the drop-down list:  
  - **64-bit WEP.** Standard WEP encryption, using 40/64-bit encryption.  
  - **128-bit WEP.** Standard WEP encryption, using 104/128-bit encryption.  
  - **152-bit WEP.** Proprietary WEP encryption mode, using 128+24 bits encryption. This mode functions only with other wireless station that support this mode. |
| **Passphrase**    | Enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive). The secret passphrase allows you to automatically generate the keys by clicking **Generate Keys**. The default passphrase is sharedsecret.  
  You can display the actual passphrase by selecting the **Show Passphrase in Clear Text** radio button. |
Configure Legacy 802.1X

To use legacy 802.1X security, you must define RADIUS server settings. For information about RADIUS servers, see Configure RADIUS Server Settings on page 48.

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

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

WPA, WPA2, and WPA & WPA2 security requires RADIUS-based 802.1x authentication, so you also must define RADIUS server settings. For information about RADIUS servers, see Configure RADIUS Server Settings on page 48.

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

- **WPA with RADIUS**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
</table>
| Encryption Key (Key1–Key4) | Either manually enter a key or allow the key to be automatically generated by clicking Generate Key.  
  • For ASCII format, depending on the key size selected, the manually entered encryption key must have a length of 5 (64-bit WEP), 13 (128-bit WEP), or 16 (152-bit WEP) characters.  
  • For HEX format, depending on the key size selected, the manually entered or automatically generated encryption key must have a length of 10 (64-bit WEP), 26 (128-bit WEP), or 32 (152-bit WEP) characters.  
  **Note:** Wireless stations must use the key to access the wireless access point.  
  **Note:** Not all wireless adapters support passphrase key generation. |
| Show Passphrase in Clear Text | Select the **Yes** radio button to display the actual passphrase in the Passphrase field. The default setting is **No**. |
• **WPA2 with RADIUS**

![Authentication Settings](image)

**Figure 20.**

• **WPA & WPA2 with RADIUS**

![Authentication Settings](image)

**Figure 21.**

Table 11. WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
</table>
| TKIP        | Temporal Key Integrity Protocol (TKIP) is the standard encryption method used with WPA. You can also use TKIP with WPA2.  
  **Note:** TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 authentication with AES encryption if you want to use the 11n rates and speed. |
| AES         | Advanced Encryption Standard (AES) is the standard encryption method used with WPA2.  
  **Note:** Although some wireless clients might support AES with WPA, the WNAP320 wireless access point does not support WPA with AES. |
| TKIP + AES  | The TKIP + AES encryption method is supported both for WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method. |

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

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

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

![Figure 22.](image)

• **WPA2-PSK**

![Figure 23.](image)

• **WPA-PSK & WPA2-PSK**

![Figure 24.](image)

**Table 12. WPA-PSK, WPA2-PSK, and WPA-PSK & WPA2-PSK Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption</td>
<td><strong>TKIP</strong> Temporal Key Integrity Protocol (TKIP) is the standard encryption method used with WPA. You can also use TKIP with WPA2.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> TKIP provides only legacy (slower) rates of operation. NETGEAR recommends WPA2 authentication with AES encryption if you want to use the 11n rates and speed.</td>
</tr>
<tr>
<td></td>
<td><strong>AES</strong> Advanced Encryption Standard (AES) is the standard encryption method used with WPA2.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Although some wireless clients might support AES with WPA, the WNAP320 wireless access point does not support WPA with AES.</td>
</tr>
<tr>
<td></td>
<td><strong>TKIP + AES</strong> TKIP + AES supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA &amp; WPA2 mixed mode, TKIP + AES is the only supported data encryption method.</td>
</tr>
</tbody>
</table>
Configure RADIUS Server Settings

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

To configure the RADIUS server settings:

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

![Configure RADIUS Server Settings](image)

Figure 25.

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passphrase</td>
<td>Enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive). The default passphrase is sharedsecret. You can display the actual passphrase by selecting the <strong>Show Passphrase in Clear Text</strong> radio button.</td>
</tr>
<tr>
<td>Show Passphrase in Clear Text</td>
<td>Select the <strong>Yes</strong> radio button to display the actual passphrase in the Passphrase field. The default setting is No.</td>
</tr>
</tbody>
</table>
2. Specify the settings as explained in the following table:

**Table 13. RADIUS Server Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RADIUS Server Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Primary Authentication Server</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the primary RADIUS server for authentication.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the UDP port number of the wireless access point that is used to access the primary RADIUS server for authentication. The default port number is 1812.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the shared key that is used between the wireless access point and the primary RADIUS server during authentication.</td>
</tr>
<tr>
<td>Secondary Authentication Server</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the secondary RADIUS server for authentication.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the UDP port number of the wireless access point that is used to access the secondary RADIUS server for authentication. The default port number is 1812.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the shared key that is used between the wireless access point and the secondary RADIUS server during authentication.</td>
</tr>
<tr>
<td>Primary Accounting Server</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the primary RADIUS server for accounting.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the UDP port number of the wireless access point that is used to access the primary RADIUS server for accounting. The default port number is 1813.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the shared key that is used between the wireless access point and the primary RADIUS server during the accounting process.</td>
</tr>
<tr>
<td>Secondary Accounting Server</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the secondary RADIUS server for accounting.</td>
</tr>
<tr>
<td>Authentication Port</td>
<td>Enter the UDP port number of the wireless access point that is used to access the secondary RADIUS server for accounting. The default port number is 1813.</td>
</tr>
<tr>
<td>Secret</td>
<td>Enter the shared key that is used between the wireless access point and the secondary RADIUS server during the accounting process.</td>
</tr>
<tr>
<td><strong>Authentication Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Reauthentication Time (Seconds)</td>
<td>The interval in seconds after which the supplicant is reauthenticated with the RADIUS server. The default interval is 3600 seconds (1 hour). Enter 0 to disable reauthentication.</td>
</tr>
<tr>
<td>Update Global Key Every (Seconds)</td>
<td>Select the check box to allow the global key update, and enter the interval in seconds. The check box is selected by default, and the default interval is 1800 seconds (30 minutes). Clear the check box to prevent the global key update.</td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings.
Restrict Wireless Access by MAC Address

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

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

To restrict access based on MAC addresses:

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

![MAC Authentication Screen](image)

**Figure 26.**

2. Select the **Turn Access Control On** check box to enable the access control feature.

3. From the Select Access Control Database drop-down list, select one of the following database options:
   - **Local MAC Address Database**. The wireless access point uses the local MAC address database for access control. This is the default setting.
   - **Remote MAC Address Database**. The wireless access point uses the MAC address database on an external RADIUS server on the LAN for access control. If you select this database, you first must configure the RADIUS server settings (see *Configure RADIUS Server Settings* on page 48).
4. Click **Refresh** to refresh the Available Wireless Stations table. The wireless access point places the MAC addresses of the attached wireless stations in this table.

5. Populate the Trusted Wireless Stations table by one of the following methods:
   • Select MAC addresses from the Available Wireless Stations table:
     a. Select individual check boxes for MAC addresses, or select all MAC addresses by selecting the check box in the heading.
     b. Click **Move** to transfer the MAC addresses from the Available Wireless Stations table to the Trusted Wireless Stations table.
   • Enter MAC addresses manually:
     a. Enter a MAC address directly in the Trusted Wireless Stations table.
     b. Click **Add**.

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

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

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

**WARNING!**

When configuring the wireless access point from a wireless computer whose MAC address is not in the access control list, you will lose your wireless connection when you click **Apply**. You must then access the wireless access point from a wired computer or from a wireless computer which is on the access control list to make any further changes.
Schedule the Wireless Radio

Scheduled Wireless On/Off is a green feature that allows you to turn off the wireless radio during scheduled vacations, office shutdowns, on evenings, or on weekends.

To schedule the radio:

1. Select Configuration > Wireless > Basic > Scheduled Wireless ON-OFF. The Scheduled Wireless ON-OFF screen displays:

![Scheduled Wireless ON-OFF Screen]

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Wireless on-off</td>
<td>Select the On radio button to enable the timer. By default, the Off radio button is selected.</td>
</tr>
<tr>
<td>Radio off schedule</td>
<td>Select check boxes to specify the days when you want to schedule the radio to be turned off. By default, Saturday and Sunday are selected.</td>
</tr>
<tr>
<td>Radio ON Time</td>
<td>Fill in the time that you want the radio to be turned back on. Use 24-hour time format.</td>
</tr>
<tr>
<td>Radio OFF Time</td>
<td>Fill in the time that you want the radio to be turned off. Use 24-hour time format.</td>
</tr>
</tbody>
</table>

3. Click Apply to save your settings.

Configure Basic Wireless Quality of Service

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

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

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

- **Voice.** The highest priority queue with minimum delay, which makes it ideal for applications like VoIP and streaming media.
- **Video.** The second highest priority queue with low delay is given to this queue. Video applications are routed to this queue.
- **Best Effort.** The medium priority queue with medium delay is given to this queue. Most standard IP application use this queue.
- **Background.** Low priority queue with high throughput. Applications, such as FTP, that are not time-sensitive but require high throughput can use this queue.

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

---

**Note:** For information about how to configure advanced wireless QoS, that is, to configure specific Enhanced Distributed Channel Access (EDCA) settings, see *Configure Advanced QoS Settings* on page 81.

---

**To configure basic wireless QoS:**

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

![QoS Settings](image)

Figure 28.
2. Enable or disable the WMM features:
   • Enable Wi-Fi Multimedia (WMM). To enable this feature, select the Enable radio button, which is the default setting. Select the Disable button to disable the feature.
   • WMM Powersave. To enable this feature, select the Enable radio button, which is the default setting. Select the Disable button to disable the feature.

3. Click Apply to save your settings.
Enable Remote Management

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

To set up an SNMP management interface:

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

![SNMP Settings Screen](image)

   **Figure 29.**

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

   **Table 15. SNMP Settings**

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

3. Click **Apply** to save your settings.
Secure Shell and Telnet Management

To configure remote console features:

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

![Remote Console Screen](image)

**Figure 30.**

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

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

To manage the wireless access point over a Telnet connection:

1. Open a secure Telnet session from your computer to the wireless access point. A screen similar to the following should display:

![Telnet Session](image)

**Figure 31.**

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

   After successful login, the > prompt should appear preceded by the name of the wireless access point. In this example, the prompt is netgear334408.
3. Enter the CLI commands that you want to use. You can enter `show configuration` to display the available CLI commands. The CLI commands are also listed in Appendix B, Command-Line Reference.

## Upgrade the Wireless Access Point Software

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

- **Web Browser Upgrade Procedure** on page 59
- **TFTP Server Upgrade Procedure** on page 59

---

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

---

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

---

**WARNING!**

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

---

**IMPORTANT:**

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

To use a Web browser to upgrade the wireless access point firmware:

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

![Firmware Upgrade Screen]

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

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

7. Verify that the new software file has been installed by selecting Monitoring > System. The System screen displays (see Figure 40 on page 66). The firmware version is shown in the Access Point Information section of the screen.

TFTP Server Upgrade Procedure

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

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

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

![Firmware Upgrade TFTP Screen](image)

**Figure 33.**

5. Specify the following information:
   - **Firmware File Name**. The name of the unzipped software file.
   - **TFTP Server IP**. The IP address of your TFTP server.

6. Click **Apply** to initiate the upgrade process.

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

7. Verify that the new software file has been installed by selecting **Monitoring > System**. The System screen displays (see **Figure 40** on page 66). The firmware version is shown in the Access Point Information section of the screen.

**Manage the Configuration File or Reset to Factory Defaults**

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

**Save the Configuration**

**To save your settings:**

1. Select **Maintenance > Upgrade > Backup Settings**. The Backup Settings screen displays (see the following figure).

2. Click **Backup**. Your browser extracts the configuration file (the file name is config) from the wireless access point and prompts you for a location on your computer to store the file.

3. Follow the instructions of your browser to save the file.
Figure 34.

Restore the Configuration

**IMPORTANT:**

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

To restore your settings from a saved configuration file:

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

   Figure 35.

   2. Click Browse and locate the saved configuration file (the file name is config).

   3. Click Apply to initiate the restoration process. During the restoration process, the wireless access point automatically restarts. The restoration process typically takes about 1 minute. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.
Restore the Wireless Access Point to the Factory Default Settings

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

- Use the Web Management Interface to Restore Factory Default Settings on this page
- Use the Reset Button to Restore Factory Default Settings on page 63

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

Use the Web Management Interface to Restore Factory Default Settings

IMPORTANT:

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

To restore the factory default settings using the Web Management Interface:

1. Select Maintenance > Reset > Restore Defaults. The Restore Defaults screen displays (see the following figure).
2. Select the Yes radio button. (By default, the No radio button is selected.)
3. Click Apply to reset the wireless access point to the factory default settings.

During the restoration process, the wireless access point automatically restarts. The restoration process typically takes about 1 minute. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.
Use the Reset Button to Restore Factory Default Settings

To restore the factory default settings when you do not know the login user name, login password, or IP address, you must use the Reset button on the rear panel of the wireless access point (see Figure 2 on page 12).

To restore the factory default settings using the Reset button:

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

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

2. Release the Reset button.

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

Reboot the Wireless Access Point without Restoring the Default Configuration

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

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

2. Select the Yes radio button. (By default, the No radio button is selected.)

3. Click Apply to reboot the wireless access point.

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

Change the Administrator Password

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

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

To change the administrator password:

1. Select Maintenance > Password > Change Password. The Change Password screen displays:
2. Take one of the following actions:
   • Enter a new password twice: once in the New Password field and again in the Repeat New Password field.
   • Next to Restore Default Password, select the Yes radio button to restore the default password. By default, the No radio button is selected.

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

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

---

**Enable the Syslog Server**

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

**To enable a syslog server:**

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

   ![Syslog Screen](image)

   **Figure 39.**

   Specify the settings as explained in the following table:

   **Table 16. Syslog Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Syslog</td>
<td>Select the check box to enable the syslog option. By default, the syslog option is disabled.</td>
</tr>
<tr>
<td>Syslog Server IP Address</td>
<td>Enter the IP address of the syslog server to which the wireless access point sends the syslog files.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Enter the port number that is configured on the syslog server. The default port number is 514.</td>
</tr>
</tbody>
</table>

2. Click **Apply** to save your settings.
Monitor the Wireless Access Point

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

- **View System Information** on page 66
- **Monitor Wireless Stations** on page 68
- **View the Activity Log** on page 70
- **Traffic Statistics** on page 71

View System Information

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

To view the System screen, select **Monitoring > System**:

![System Screen](image)

Figure 40.
The following table explains the fields of the System screen:

**Table 17. System Screen Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Point Information</strong></td>
<td></td>
</tr>
<tr>
<td>Access Point Name</td>
<td>The NetBIOS name. For information about how to change the default name, see <em>Configure Basic General System Settings and Time Settings on page 19</em>.</td>
</tr>
<tr>
<td>Ethernet MAC Address</td>
<td>The MAC address of the wireless access point’s Ethernet port.</td>
</tr>
<tr>
<td>Wireless MAC Address</td>
<td>The MAC address of the wireless access point’s wireless card.</td>
</tr>
<tr>
<td>Country/Region</td>
<td>The country or region for which the wireless access point is licensed for use. For information about how to change the country or region, see <em>Configure Basic General System Settings and Time Settings on page 19</em>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> It might not be legal to operate this wireless access point in a country or region other than one of those identified in this field.</td>
</tr>
<tr>
<td>Firmware Version</td>
<td>The version of the firmware that is currently installed.</td>
</tr>
<tr>
<td>Current Time</td>
<td>The current time. For information about how to change the time settings, see <em>Configure Basic General System Settings and Time Settings on page 19</em>.</td>
</tr>
<tr>
<td><strong>Current IP Settings</strong></td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the wireless access point.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask for the wireless access point.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The default gateway for the wireless access point communication.</td>
</tr>
<tr>
<td>DHCP Client</td>
<td>Enabled indicates that the current IP address was obtained from a DHCP server on your LAN network. Disabled indicates a static IP configuration.</td>
</tr>
<tr>
<td><strong>Current Wireless Settings for 802.11n/g</strong></td>
<td></td>
</tr>
<tr>
<td>Access Point Mode</td>
<td>The operating mode of the wireless access point. One of the following modes is indicated:</td>
</tr>
<tr>
<td></td>
<td>• Access Point</td>
</tr>
<tr>
<td></td>
<td>• Point-to-Point Bridge</td>
</tr>
<tr>
<td></td>
<td>• Point-to-Point Bridge with Access Point</td>
</tr>
<tr>
<td></td>
<td>• Multi-Point Bridge with/without client association</td>
</tr>
<tr>
<td></td>
<td>For information about how to change the mode, see <em>Configure Wireless Bridging on page 84</em>.</td>
</tr>
<tr>
<td>Channel / Frequency</td>
<td>The channel the wireless port is using. 11 is the default channel when the setting is Auto. For information about how to change the channel and frequency, see <em>Configure Basic Wireless Settings on page 23</em>.</td>
</tr>
<tr>
<td>Rogue AP Detection</td>
<td>Enabled indicates that rogue AP detection is enabled; Disabled indicates that it is not.</td>
</tr>
</tbody>
</table>
Monitor Wireless Stations

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

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

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

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

![Wireless Stations Screen](image)

Figure 41.

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

For each device, the Available Wireless Stations table shows the MAC address, BSSID, SSID, channel, rate, state, type, AID, mode, and status. For information about these and more fields, see the following table.
2. To view details of a wireless station, select the corresponding radio button, and then click Details. The Wireless Stations Details screen displays:

![Figure 42.](image)

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

**Table 18. Wireless Stations Details Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address of the wireless station.</td>
</tr>
<tr>
<td>BSSID</td>
<td>The BSSID that the wireless station is using.</td>
</tr>
<tr>
<td>SSID</td>
<td>The SSID that the wireless station is using.</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel that the wireless station is using.</td>
</tr>
<tr>
<td>Rate</td>
<td>The transmit data rate in Mbps of the wireless station.</td>
</tr>
<tr>
<td>State</td>
<td>The features that are enabled on the wireless station.</td>
</tr>
<tr>
<td>Type</td>
<td>The authentication and encryption type that the wireless station is using.</td>
</tr>
<tr>
<td>AID</td>
<td>The associated identifier (AID) of the wireless station.</td>
</tr>
<tr>
<td>Mode</td>
<td>The wireless mode in which the wireless station is operating.</td>
</tr>
</tbody>
</table>
View the Activity Log

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

To display the activity log and save it:

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

![Figure 43](image)

Table 18. Wireless Stations Details Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The wireless status of the wireless station (Associated).</td>
</tr>
<tr>
<td>RSSI</td>
<td>The received signal strength indicator (RSSI) of the wireless station.</td>
</tr>
<tr>
<td>Idle Time</td>
<td>The time since the last frame was received from the wireless station.</td>
</tr>
<tr>
<td>Tx Sequence</td>
<td>The sequence number of the last frame that was transmitted to the wireless station.</td>
</tr>
<tr>
<td>Rx Sequence</td>
<td>The sequence number of the last frame that was received from the wireless station.</td>
</tr>
<tr>
<td>Capability</td>
<td>The capability summary of the wireless station that was detected during association.</td>
</tr>
<tr>
<td>Cipher</td>
<td>The cipher that is used by the wireless station and that defines the type of encryption.</td>
</tr>
<tr>
<td>SNR</td>
<td>The signal-to-noise ratio (SNR) that indicates how much the signal of the wireless station has been corrupted by noise.</td>
</tr>
<tr>
<td>Recv. Bytes</td>
<td>The number of bytes received on the wireless station since it last started up.</td>
</tr>
<tr>
<td>Trans. bytes</td>
<td>The number of bytes transmitted by the wireless station since it last started up.</td>
</tr>
<tr>
<td>Assoc. Time Stamp</td>
<td>The time when these details of the wireless station were retrieved.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the wireless station.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>The channel width at which the wireless station operates.</td>
</tr>
</tbody>
</table>
2. Click **Save As** to save the log contents to a file on your computer or to a disk drive.

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

**Traffic Statistics**

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

To display the Statistics screen, select **Monitoring > Statistics**:

![Statistics Screen](image)

**Figure 44.**

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

The following table explains the fields of the Statistics screen:

**Table 19. Statistics Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wired Ethernet</strong></td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>The number of packets received and transmitted over the Ethernet connection since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Bytes</td>
<td>The number of bytes received and transmitted over the Ethernet connection since the wireless access point was restarted.</td>
</tr>
</tbody>
</table>
Enable Rogue AP Detection and Monitor Access Points

Enable and Configure Rogue AP Detection

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

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

Table 19. Statistics Fields (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Wireless 802.11b, Wireless 802.11bg, or Wireless 801.11ng</strong></td>
<td>The section heading depends on the configured wireless mode.</td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>The number of unicast packets received and transmitted over the wireless connection since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Broadcast Packets</td>
<td>The number of broadcast packets received and transmitted over the wireless connection since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Multicast Packets</td>
<td>The number of multicast packets received and transmitted over the wireless connection since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Total Packets</td>
<td>The total number of packets received and transmitted over the wireless connection since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>The total number of bytes received and transmitted over the wireless connection since the wireless access point was restarted.</td>
</tr>
<tr>
<td><strong>Client Association</strong></td>
<td>The number of associated clients connected to the radio in the configured wireless mode.</td>
</tr>
</tbody>
</table>

| 802.11b Radio, 802.11bg Radio, or 802.11ng Radio | The number of associated clients connected to the radio in the configured wireless mode. |
To enable and configure rogue AP detection:

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

![Figure 45.](image)

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

3. In the Unknown AP List, select individual check boxes for access points, or select all access points by selecting the check box in the column heading.

4. Click **Move** to transfer the access points from the Unknown AP List to the Known AP List.

5. Select the **Turn Rogue AP Detection On** check box to enable rogue AP detection.

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

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

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

2. Click **Delete**.

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

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

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

### View and Save Access Point Lists

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

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

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

![Unknown AP List Screen](image-url)

**Figure 46.**

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address of the unknown AP.</td>
</tr>
<tr>
<td>SSID</td>
<td>The SSID that the unknown AP is using.</td>
</tr>
<tr>
<td>Privacy</td>
<td>Indicates whether or not security is enabled (1 means enabled; 0 means</td>
</tr>
<tr>
<td>Channel</td>
<td>disabled).</td>
</tr>
<tr>
<td>Rate</td>
<td>The transmit data rate in Mbps of the unknown the AP.</td>
</tr>
<tr>
<td>Beacon Int.</td>
<td>The interval for each beacon transmission in ms.</td>
</tr>
<tr>
<td># of Beacons</td>
<td>The number of beacons transmitted by the unknown AP that the wireless</td>
</tr>
<tr>
<td>Last Beacon</td>
<td>The timestamp that indicates the time when the most recent beacon was</td>
</tr>
<tr>
<td></td>
<td>detected.</td>
</tr>
</tbody>
</table>
3. Click **Save** to export the list of unknown or known APs to a file. A window opens so you can browse to the location where you want to save the file. The default file name is macList.txt.

If you wish, you can now import the saved list into the Known AP List on the Rogue AP screen (see *Enable and Configure Rogue AP Detection* on page 72).

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

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

![Known AP List Screen](image)

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

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address</td>
<td>The MAC address of the known AP.</td>
</tr>
<tr>
<td>SSID</td>
<td>The SSID that the known AP is using.</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel that the known AP is using.</td>
</tr>
</tbody>
</table>

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

You can now import the saved list into the Known AP List on the Rogue AP screen (see *Enable and Configure Rogue AP Detection* on page 72).
This chapter describes how to configure the advanced features of your ProSAFE Wireless-N Access Point WNAP320. The chapter includes the following sections:

- **Spanning Tree Protocol and 802.1Q VLAN** on this page
- **Hotspot Settings** on page 78
- **Configure Advanced Wireless Settings** on page 79
- **Configure Advanced QoS Settings** on page 81
- **Configure Wireless Bridging** on page 84

### Spanning Tree Protocol and 802.1Q VLAN

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

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

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

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

**Note**: Select the **Untagged VLAN** check box only if the hubs and switches on your LAN support the 802.1Q VLAN protocol. Likewise, change the untagged VLAN value only if the hubs and switches on your LAN support the 802.1Q VLAN protocol. Selecting the Un tagged VLAN check box or changing the untagged VLAN value will result in a loss of IP connectivity if the hubs and switches on your LAN have not yet been configured with the corresponding VLAN.
• **Tagged VLAN.** When you clear the Untagged VLAN check box, the wireless access point tags all frames that are sent from its Ethernet interface. Only incoming frames that are tagged with known VLAN IDs are accepted.

• **Management VLAN.** The management VLAN can be active only when the wireless access point functions as a point-to-point or point-to-multipoint bridge (see *Configure Wireless Bridging* on page 84). The management VLAN is used for managing traffic (Telnet, SNMP, and HTTP) to and from the wireless access point.

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

To configure STP and VLANs:

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

![Configuration screen](image)

   **Figure 47.**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Spanning Tree Protocol</strong></td>
<td>Select the <strong>Enable</strong> radio button to enable STP to prevent path redundancy. By default, the <strong>Disable</strong> radio button is selected.</td>
</tr>
<tr>
<td>Untagged VLAN</td>
<td>Select the <strong>Untagged VLAN</strong> check box to configure one VLAN as an untagged VLAN. By default, the Untagged VLAN check box is selected. Specify a VLAN ID. The default VLAN ID is 1.</td>
</tr>
</tbody>
</table>
3. Click **Apply** to save your settings.

**Hotspot Settings**

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

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

**To set up a hotspot server:**

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

   ![Hotspot Screen](image)

   **Figure 48.**

2. To enable HTTP redirection, select the **Enable** radio button. By default, the Disable radio button is selected.

3. In the Redirect URL field, enter the URL of the Web server to which you wish to redirect HTTP requests.

---

**Table 22. STP and VLAN Settings (Continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management VLAN</td>
<td>Specify an ID for the VLAN from which the wireless access point can be managed. The default VLAN ID is 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you configure the VLAN ID as 0 (zero), the wireless access point can be managed over any VLAN, and frames that belong to the management VLAN are not tagged with an 802.1Q header when sent over the trunk.</td>
</tr>
</tbody>
</table>
4. Click **Apply** to save your settings. All HTTP requests are now redirected to the specified URL.

**Configure Advanced Wireless Settings**

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

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

**To configure advanced wireless settings:**

1. Select **Configuration > Wireless > Advanced > Wireless Settings**. The advanced Wireless Settings screen displays. (The following figure shows the 11ng settings—see the wireless icon that is displayed next to ng.)

![Figure 49. Advanced Wireless Settings screen](image)

Figure 49.
Specify the settings as explained in the following table:

**Table 23. Advanced Wireless Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTS Threshold (0–2347)</td>
<td>Enter the Request to Send (RTS) threshold. The default setting is 2347. If the packet size is equal to or less than the RTS threshold, the wireless access point uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) mechanism, and the data frame is transmitted immediately after the silence period. If the packet size is larger than the RTS threshold, the wireless access point uses the CSMA with Collision Avoidance (CSMA/CA) mechanism. In this situation, the transmitting station sends an RTS packet to the receiving station, and waits for the receiving station to return a Clear to Send (CTS) packet before sending the actual packet data.</td>
</tr>
<tr>
<td>Fragmentation Length (256–2346)</td>
<td>Enter the maximum packet size that is used for the fragmentation of data packets. Packets that are larger than the specified fragmentation length are broken up into smaller packets before being transmitted. The fragmentation length must be an even number. The default setting is 2346.</td>
</tr>
<tr>
<td>Beacon Interval (100–1000)</td>
<td>Enter the interval between 100 ms and 1000 ms for each beacon transmission, which allows the wireless access point to synchronize the wireless network. The default setting is 100.</td>
</tr>
<tr>
<td>Aggregation Length (1024–65535)</td>
<td>Enter the maximum length of Aggregated MAC Protocol Data Unit (AMPDU) packets. Larger aggregation lengths could lead to better network performance. Aggregation is a mechanism used to achieve higher throughput. The default setting is 65535.</td>
</tr>
<tr>
<td>AMPDU</td>
<td>Select the Enable radio button to allow the aggregation of several MAC frames into a single large frame to achieve higher throughput. Enabling Aggregated MAC Protocol Data Unit (AMPDU) could lead to better network performance. By default, the Enable radio button is selected.</td>
</tr>
<tr>
<td>RIFS Transmission</td>
<td>Select the Enable radio button to allow transmission of successive frames at different transmit powers. Enabling Reduced Interframe Space (RIFS) could lead to better network performance. By default, the Disable radio button is selected.</td>
</tr>
<tr>
<td>DTIM Interval (1–255)</td>
<td>Enter the Delivery Traffic Indication Message (DTIM) interval, also referred to as the data beacon rate, which indicates the beacon delivery traffic indication message period in multiples of beacon intervals. This value must be between 1 and 255. The default setting is 3.</td>
</tr>
</tbody>
</table>
| Preamble Type                | Select one of the following radio buttons to specify the preamble type:  
  • **Long.** A long transmit preamble might provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance.  
  • **Auto.** The Auto settings automatically handles both long and short preambles. The default setting is Auto. |
Configure Advanced QoS Settings

For most networks, the default Quality of Service (QoS) queue settings work well. For information about how to configure basic QoS, see Configure Basic Wireless Quality of Service on page 52.

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

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

- **AP EDCA parameters.** Specify the access point (AP) Enhanced Distributed Channel Access (EDCA) settings for different types of data transmitted from the wireless access point to wireless clients.

- **Station EDCA parameters.** Specify the station EDCA parameters for different types of data transmitted from the wireless clients to the wireless access point. If WMM is disabled, you cannot configure the Station EDCA parameters. (For information about how to enable WMM, see Configure Basic Wireless Quality of Service on page 52.)

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

- **Data 0 (Best Effort)**. Medium priority queue, medium throughput and delay. Most traditional IP data is sent to this queue.

- **Data 1 (Background)**. Lowest priority queue, high throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).

- **Data 2 (Video)**. Highest priority queue, minimum delay. Time-sensitive video data is automatically sent to this queue.

- **Data 3 (Voice)**. Highest priority queue, minimum delay. Time-sensitive data such as VoIP and streaming media are automatically sent to this queue.

**To configure advanced QoS:**

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

![Figure 50.](image-url)
2. Specify the settings as explained in the following table:

### Table 24. EDCA Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AP EDCA parameters</strong></td>
<td></td>
</tr>
</tbody>
</table>
| AIFS | Enter the Arbitration Inter-Frame Spacing (AIFS) interval that specifies the wait time (in milliseconds) between data frames. A higher AIFS value means a higher priority for a queue. Valid values for AIFS are 0 through 8.  
The default values are: Data 0: 3; Data 1: 7; Data 2: 1; Data 3: 1. |
| cwMin | Enter the Minimum Contention Window (cwMin) value that specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for cwMin must be lower than the value for cwMax. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023.  
The default values are: Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3. |
| cwMax | Enter the Maximum Contention Window (cwMax) value that specifies the upper limit (in milliseconds) for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for cwMax must be higher than the value for cwMin. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023.  
The default values are: Data 0: 63; Data 1: 1023; Data 2: 15; Data 3: 7. |
| Max. Burst | Enter the maximum burst value that specifies the maximum burst length (in microseconds) allowed for packet bursts on the wireless network. A packet burst is a collection of multiple frames transmitted without header information. Decreasing this value increases the priority of the queue. Valid values for maximum burst length are all multiples of 32 between 0 and 8192, inclusive of 0 and 8192.  
The default values are: Data 0: 0; Data 1: 0; Data 2: 3008; Data 3: 1504. |
| **Station EDCA parameters** | |
| AIFS | Enter the Arbitration Inter-Frame Spacing (AIFS) interval that specifies the wait time (in milliseconds) between data frames. A higher AIFS value means a higher priority for a queue. Valid values for AIFS are 0 through 8.  
The default values are: Data 0: 3; Data 1: 7; Data 2: 2; Data 3: 2. |
| cwMin | Enter the Minimum Contention Window (cwMin) value that specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for cwMin must be lower than the value for cwMax. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1023.  
The default values are: Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3. |
3. Click **Apply** to save your settings.

### Configure Wireless Bridging

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

- **Wireless point-to-point bridge.** In this mode, the wireless access point can communicate with another bridge-mode wireless station and, as an option, also with wireless clients. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see *Configure a Point-to-Point Wireless Network* on page 85.

- **Wireless point-to-multipoint bridge.** In this mode, the wireless access point is the master for a group of bridge-mode wireless stations. As an option, the wireless access point can also communicate with wireless clients. You can configure up to four profiles. The other bridge-mode wireless stations must be set to point-to-point bridge mode, using the MAC address of the master wireless access point. Rather than communicating directly with each other, all other bridge-mode wireless stations send their traffic to the master wireless access point. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see *Configure a Point-to-Multipoint Wireless Network* on page 88.

- **Repeater mode.** In this mode, this wireless access point operates as a repeater only, and sends all traffic to a remote access point. Repeater mode does not support communication with wireless clients, that is, wireless clients cannot associate with the wireless access point when the wireless access point operates as a repeater. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see *Configure the Wireless Access Point for Repeater Mode* on page 92.
• **Client mode.** In this mode, the wireless access point operates as a client bridge only, and sends all traffic to the remote wireless access point or peer device. You can enable MAC cloning in client mode. For information about how to configure this mode, see *Configure the Wireless Access Point for Client Mode* on page 96.

**Configure a Point-to-Point Wireless Network**

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

![Diagram](image)

**Figure 51.**

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

1. Configure the wireless access point (AP1 on LAN Segment 1 in the previous figure) as a point-to-point bridge:
   a. Select *Configuration > Wireless Bridge*. The Bridging screen displays (see *Figure 52* on page 86).
   b. Select the **Enable Wireless Bridging** check box. The Local MAC Address field is a nonconfigurable field that shows the MAC address of the wireless access point.
   c. Select the **Wireless Point-to-Point Bridge** radio button.
   d. If you want to enable wireless client association while the wireless access point functions as a point-to-point bridge, select the **Enable Wireless Client Association** check box.
e. Click **Edit** to configure the security profile settings. The Edit Security Profile screen displays:

![Edit Security Profile Screen](image)

**Figure 53.**

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

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile Definition</strong></td>
<td></td>
</tr>
<tr>
<td>Profile Name</td>
<td>Enter a profile name that is easy to remember. The default name is NETGEAR-WDS-1.</td>
</tr>
<tr>
<td>Remote MAC Address</td>
<td>Enter the MAC address of the remote wireless access point (the MAC address of AP2 on LAN Segment 1 in <em>Figure 51</em> on page 85).</td>
</tr>
</tbody>
</table>
g. Click **Apply** to save your security profile settings. The Bridging screen displays again.

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

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

2. Configure a second wireless access point (AP2) on LAN Segment 2 (see **Figure 51** on page 85) in point-to-point bridge mode.

   AP1 must have AP2’s MAC address in its Remote MAC Address field, and AP2 must have AP1’s MAC address in its Remote MAC Address field.
3. Configure and verify the following settings for both wireless access points:
   • Verify the LAN network configuration of the wireless access points. Both must be configured to operate in the same LAN network address range as the LAN devices.
   • Both wireless access points must use the same channel, authentication mode, and security settings.

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

Configure a Point-to-Multipoint Wireless Network

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

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

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

1. Configure the security profiles on the wireless access point (AP1 on LAN Segment 1 in the previous figure):
   a. Select Configuration > Wireless Bridge. The Bridging screen displays:

   ![Bridging Screen](image)

   Figure 55.

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

   c. Select the Wireless Point-to-Multi-Point Bridge radio button.

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

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

   ![Edit Security Profile](image)

   Figure 56.
f. Specify the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Definition</td>
<td></td>
</tr>
<tr>
<td><strong>Profile Name</strong></td>
<td>Enter a profile name that is easy to remember. The default names for the four security profiles are NETGEAR-WDS-1, NETGEAR-WDS-2, NETGEAR-WDS-3, and NETGEAR-WDS-4.</td>
</tr>
<tr>
<td><strong>Remote MAC Address</strong></td>
<td>Enter the MAC address of the remote wireless access point (the MAC address of AP2 or AP 3 on LAN Segment 1 in Figure 54 on page 88).</td>
</tr>
<tr>
<td>Authentication Settings</td>
<td></td>
</tr>
<tr>
<td><strong>Network Authentication</strong> and <strong>Data Encryption</strong></td>
<td>From the Network Authentication drop-down list, select <strong>Open System</strong>, <strong>WPA-PSK</strong>, or <strong>WPA2-PSK</strong>. Your selection determines the options that the Data Encryption drop-down list provides, and whether or not the WPA Passphrase (Network Key) field displays.</td>
</tr>
<tr>
<td><strong>Open System</strong></td>
<td>Although you can use the bridge communication without any authentication and encryption, NETGEAR recommends that you use WEP if you do select an open system. From the Data Encryption drop-down list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>. No authentication and encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>64-bit WEP</strong>. Standard WEP encryption, using 40/64-bit encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>128-bit WEP</strong>. Standard WEP encryption, using 104/128-bit encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>152-bit WEP</strong>. Proprietary WEP encryption mode, using 128+24 bits encryption. This mode functions only with other wireless stations that support this mode.</td>
</tr>
<tr>
<td><strong>WPA-PSK</strong></td>
<td>TKIP (Temporal Key Integrity Protocol) is the standard encryption method used with WPA-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive).</td>
</tr>
<tr>
<td><strong>WPA2-PSK</strong></td>
<td>AES (Advanced Encryption Standard) is the standard encryption method used with WPA2-PSK and the only selection possible from the Data Encryption drop-down list. In the WPA Passphrase (Network Key) field, enter a passphrase. The passphrase length must be between 8 and 63 characters (inclusive).</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>NETGEAR recommends WPA2-PSK authentication with AES encryption if you want to use the 11n rates and speed.</td>
</tr>
</tbody>
</table>


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

h. Repeat step b through step g for any other security profile that you want to edit.
For example, first configure security profile NETGEAR-WDS-1 with the MAC address of AP2, and then configure security profile NETGEAR-WDS-2 with the MAC address of AP3 (see Figure 54 on page 88).

2. Activate the wireless access point (AP1 on LAN Segment 1 in Figure 54 on page 88) as a point-to-multipoint bridge (that is, it is the master in the wireless network):
   a. On the Bridging screen, select the Enable Wireless Bridging check box.
   b. Select the Wireless Point-to-Multi-Point Bridge radio button.
   c. Select the Enable Wireless Client Association check box to enable wireless client association.

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

   d. If the correct profile names and security options are displayed in the table, select the check boxes in the Enable column for all security profiles that you want to enable.
   e. Click Apply in the Bridging screen to activate your point-to-multipoint bridge settings.

3. Configure AP2 on LAN Segment 2 (see Figure 54 on page 88) in point-to-point bridge mode with the remote MAC address of AP1.

4. Configure AP3 on LAN Segment 3 (see Figure 54 on page 88) in point-to-point bridge mode with the remote MAC address of AP1.

5. Verify the following for all wireless access points:
   - Only AP1 on LAN Segment 1 is configured in point-to-multipoint bridge mode, and all others APs are configured in point-to-point bridge mode.
   - AP2 and AP3 (the point-to-point APs) must have AP1’s MAC address in their Remote MAC Address field.
   - All APs must be on the same LAN, that is, the LAN IP addresses of all APs must be in the same network as the LAN devices.
   - If you use DHCP, all wireless access points must obtain an IP address automatically (as a DHCP client). For more information, see Configure IP Settings and Optional DHCP Server Settings on page 21.
   - All wireless access points must use the same channel, authentication mode, and security settings.

6. Verify connectivity across the LANs:
   - A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the three LAN segments.
Note: You can extend this multipoint bridging configuration by adding additional wireless access points that are configured in point-to-point mode for each additional LAN segment. Furthermore, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.

Configure the Wireless Access Point for Repeater Mode

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

The following figure shows an example in which AP1, AP2, and AP3 function in repeater bridge mode. AP2 requires a security profile for AP1 and another one for AP3:
To configure the wireless access point as a wireless repeater:

1. Configure the security profiles on the wireless access point (AP2 in the previous figure):
   a. Select **Configuration > Wireless Bridge**. The Bridging screen displays:

   ![Bridging Screen](image)

   **Figure 58.**

   b. Select the **Enable Wireless Bridging** check box. The Local MAC Address field is a nonconfigurable field that shows the MAC address of the wireless access point.
   c. Select the **Wireless Point-to-Multi-Point Bridge** radio button.
   d. The profile table shows four security profiles. Choose a security profile to edit by selecting the corresponding radio button to the left of the profile.
   e. Click **Edit** to configure the selected security profile settings. The Edit Security Profile screen displays for the selected security profile. (The following figure contains some examples.)

   ![Edit Security Profile](image)

   **Figure 59.**
f. Specify the settings as explained in the following table:

**Table 27. Repeater Profile and Authentication Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile Definition</strong></td>
<td></td>
</tr>
<tr>
<td>Profile Name</td>
<td>Enter a profile name that is easy to remember. The default names for the four</td>
</tr>
<tr>
<td></td>
<td>security profiles are NETGEAR-WDS-1, NETGEAR-WDS-2, NETGEAR-WDS-3, and NETGEAR-</td>
</tr>
<tr>
<td></td>
<td>WDS-4.</td>
</tr>
<tr>
<td>Remote MAC Address</td>
<td>Enter the MAC address of the remote wireless access point (the MAC</td>
</tr>
<tr>
<td></td>
<td>address of AP1 or AP3 in Figure 57 on page 92).</td>
</tr>
<tr>
<td><strong>Authentication Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Network Authentication and</td>
<td>From the Network Authentication drop-down list, select <strong>Open System</strong>,</td>
</tr>
<tr>
<td>Data Encryption</td>
<td><strong>WPA-PSK</strong>, or <strong>WPA2-PSK</strong>. Your selection determines the options that the</td>
</tr>
<tr>
<td></td>
<td>Data Encryption drop-down list provides, and whether or not the WPA</td>
</tr>
<tr>
<td></td>
<td>Passphrase (Network Key) field displays.</td>
</tr>
<tr>
<td>Open System</td>
<td>Although you can use the bridge communication without any authentication and</td>
</tr>
<tr>
<td></td>
<td>encryption, NETGEAR recommends that you use WEP if you do select an open</td>
</tr>
<tr>
<td></td>
<td>system. From the Data Encryption drop-down list, select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>None</strong>. No authentication and encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>64-bit WEP</strong>. Standard WEP encryption, using 40/64-bit encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>128-bit WEP</strong>. Standard WEP encryption, using 104/128-bit encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>152-bit WEP</strong>. Proprietary WEP encryption mode, using 128+24 bits</td>
</tr>
<tr>
<td></td>
<td>encryption. This mode functions only with other wireless station that</td>
</tr>
<tr>
<td></td>
<td>support this mode.</td>
</tr>
<tr>
<td>WPA-PSK</td>
<td><strong>TKIP</strong> (Temporal Key Integrity Protocol) is the standard encryption method</td>
</tr>
<tr>
<td></td>
<td>used with WPA-PSK and the only selection possible from the Data Encryption</td>
</tr>
<tr>
<td></td>
<td>drop-down list. In the WPA Passphrase (Network Key) field, enter a</td>
</tr>
<tr>
<td></td>
<td>passphrase. The passphrase length must be between 8 and 63 characters</td>
</tr>
<tr>
<td></td>
<td>(inclusive).</td>
</tr>
<tr>
<td>WPA2-PSK</td>
<td><strong>AES</strong> (Advanced Encryption Standard) is the standard encryption method</td>
</tr>
<tr>
<td></td>
<td>used with WPA2-PSK and the only selection possible from the Data Encryption</td>
</tr>
<tr>
<td></td>
<td>drop-down list. In the WPA Passphrase (Network Key) field, enter a</td>
</tr>
<tr>
<td></td>
<td>passphrase. The passphrase length must be between 8 and 63 characters</td>
</tr>
<tr>
<td></td>
<td>(inclusive).</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: NETGEAR recommends WPA2-PSK authentication with AES encryption if</td>
</tr>
<tr>
<td></td>
<td>you want to use the 11n rates and speed.</td>
</tr>
</tbody>
</table>

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

h. Repeat *step b* through *step g* for any other security profile that you want to edit.
For example, first configure security profile NETGEAR-WDS-1 with the MAC address of AP1, and then configure security profile NETGEAR-WDS-2 with the MAC address of AP3 (see Figure 57 on page 92).

2. Activate repeater mode on the wireless access point (AP2 in Figure 57 on page 92):
   a. On the Bridging screen, select the Enable Wireless Bridging check box.
   b. Select the Wireless Point-to-Multi-Point Bridge radio button.
   c. Clear the Enable Wireless Client Association check box to disable wireless client association (see the red circle in Figure 58 on page 93).

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

   d. If the correct profile names and security options are displayed in the table, select the check boxes in the Enable column for all security profiles that you want to enable.
   e. Click Apply in the Bridging screen to activate your repeater settings.

3. Configure AP1 on LAN Segment 1 (see Figure 57 on page 92) in repeater mode with the remote MAC address of AP2.

4. Configure AP3 on LAN Segment 3 (see Figure 57 on page 92) in repeater mode with the remote MAC address of AP2.

5. Verify the following for all wireless access points:
   • All APs must be on the same LAN, that is, the LAN IP addresses of all APs must be in the same network as the LAN devices.
   • If you use DHCP, all wireless access points must obtain an IP address automatically (as a DHCP client). For more information, see Configure IP Settings and Optional DHCP Server Settings on page 21.
   • All wireless access points must use the same channel, authentication mode, and security settings.

6. Verify connectivity across the LANs:
   • A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other PCs or servers connected to any of the two LAN segments.

   **Note:** You can extend the repeating functionality by adding up to two more wireless access points that are configured in repeater mode. However, since repeaters communicate in half-duplex mode, the bandwidth decreases as you add repeaters to the network. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.
Configure the Wireless Access Point for Client Mode

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

**To configure the wireless access point for client mode:**

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

   ![Bridging Screen](image)

   **Figure 60.**

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

3. Select the **Client** radio button. (The Edit button becomes nonoperational after you have selected the Client button.)

4. As an option, you can now enable MAC cloning, which allows only wireless connections to computers or wireless stations for which you have added the MAC address to the Trusted Wireless Stations table. For more information, see *Restrict Wireless Access by MAC Address* on page 50.

   To enable MAC cloning:
   
   a. Next to MAC Clone, select the **Enable** radio button. By default, the Disable radio button is selected.
   
   b. In the MAC Clone Address field, enter the MAC address.

5. Click **Apply** to save your settings.
This chapter provides information about troubleshooting your ProSAFE Wireless-N Access Point WNAP320. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the wireless access point on?
  Go to Basic Functioning on page 98.

- Have I connected the wireless access point correctly?
  Go to Basic Functioning on page 98.

- I cannot access the Internet or the LAN.
  Go to You Cannot Access the Internet or the LAN from a Wireless-Capable Computer on page 99.

- I cannot access the wireless access point from a browser.
  Go to You Cannot Configure the Wireless Access Point from a Browser on page 100.

- A time-out occurs.
  Go to When You Enter a URL or IP Address a Time-Out Error Occurs on page 101.

- I cannot remember the wireless access point’s configuration password.
  Go to Change the Administrator Password on page 64.

- I want to clear the configuration and start over again.
  Go to Restore the Wireless Access Point to the Factory Default Settings on page 62.

- The date or time is not correct.
  Go to Problems with Date and Time on page 103.

The wireless access point provides a packet capture tool that enables you to perform problem diagnoses. For information about how to use this tool, go to Use the Packet Capture Tool on page 103.
Basic Functioning

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

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

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

No LEDs Are Lit on the Wireless Access Point

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

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

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

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

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

There is a hardware connection problem.

**Check these items:**

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

The WLAN LED Does Not Light Up

The wireless access point's antenna is not working.

**Check these items:**

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

Contact NETGEAR technical support if the WLAN LED remains off.

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

There is a configuration problem.

**Check these items:**

- You might not have restarted the computer with the wireless adapter to allow TCP/IP changes take effect. Restart the computer.
- The computer with the wireless adapter might not have the correct TCP/IP settings to communicate with the network. Restart the computer and check that TCP/IP is set up correctly for that network. In Windows, the usual setting for Network Properties is to obtain an IP address automatically.
- The wireless access point's default values might not work with your network. Check the wireless access point’s default configuration against the configuration of other devices in your network.
- Make sure that the SSID, network authentication, and data encryption settings of the computer with the wireless adapter are the same as those of the wireless access point.
• Ping the IP address of the wireless access point to verify that there is a wireless connection between the computer with the wireless adapter and the wireless access point. If the ping fails, check the network configuration (for the wireless access point, see Configure IP Settings and Optional DHCP Server Settings on page 21).

• Ping the default gateway to verify that there is a path from the computer with the wireless adapter to the default gateway. If the ping fails, check the network configuration or call the Internet Service Provider (ISP).

You Cannot Configure the Wireless Access Point from a Browser

Check these items:

• The wireless access point is correctly installed, it is powered on, and LAN connections are okay. Check that the Active LED and LAN LED are on to verify that the Ethernet connection is okay.

• If your computer uses a fixed (static) IP address, ensure that it is using an IP address in the range of the wireless access point. The wireless access point’s default IP address is 192.168.0.100, and its subnet mask is 255.255.255.0 with DHCP disabled. Make sure that your network configuration settings are correct.

• If you are using the NetBIOS name of the wireless access point to connect, ensure that your computer and the wireless access point are on the same network segment or that there is a WINS server on your network.

• If your computer is set to Obtain an IP address automatically (DHCP client), restart it.

• Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click Refresh to be sure that the Java applet is loaded.

• Try quitting the browser and launching it again.

• Make sure that you are using the correct login information. The factory default login name is admin, and the password is password. Make sure that Caps Lock is off when entering this information.

If the wireless access point does not save changes you have made in the Web Management Interface, check the following:

• When entering configuration settings, be sure to click the Apply button before moving to another screen or tab, or your changes are lost.

• Click the Refresh or Reload button in the Web browser. The changes might have occurred, but the Web browser might be caching the old configuration.
When You Enter a URL or IP Address a Time-Out Error Occurs

A number of things could be causing this.

Try the following troubleshooting steps:

• Check whether other computers on the LAN work correctly. If they do, ensure that your computer’s TCP/IP settings are correct. If you use a fixed (static) IP address, check the subnet mask, default gateway, DNS, and IP addresses of the wireless access point (see Configure IP Settings and Optional DHCP Server Settings on page 21).
• If the computer is configured correctly but still not working, ensure that the wireless access point is connected and turned on. Access it and check its settings. If you cannot connect to the wireless access point, check the LAN and power connections.
• If the wireless access point is configured correctly, check your Internet connection (for example, your cable modem) to make sure that it is working correctly.

Troubleshooting a TCP/IP Network Using the Ping Utility

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

Testing the LAN Path to Your Wireless Access Point

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

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

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

   ping 192.168.0.229

3. Click OK.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

   If the path is working, you see this message:

   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx
If the path is not working, you see this message:

Request timed out

If the path is not functioning correctly, you could have one of the following problems:

- **Wrong physical connections:**
  - Make sure that the Active LED and LAN LED are on. If one or both of these LEDs are off, follow the instructions in *The Active LED or the LAN LED Is Not Lit* on page 99.
  - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and wireless access point.

- **Wrong network configuration:**
  - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.
  - Verify that the IP address for your wireless access point and your workstation are correct and that the addresses are on the same subnet.

**Testing the Path from Your Computer to a Remote Device**

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

1. From the Windows toolbar, click the **Start** button, and select **Run**.
2. In the Windows Run window, type:
   
   Ping -n 10 IP address
   
   where **IP address** is the IP address of a remote device such as your ISP's DNS server.

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

- Check that your computer has the IP address of your router listed as the default wireless access point. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer's Network Control Panel. Verify that the IP address of the router is listed as the default wireless access point as described in the Preparing your Network document that you can access from *Related Documents* in Appendix A.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the basis General system settings screen (see *Configure Basic General System Settings and Time Settings on page 19*).

Problems with Date and Time

The Time Settings screen that is accessible through the Configuration > System > Basic > Time menu choices displays the current date and time of day. The wireless access point uses the Network Time Protocol (NTP) to obtain the current time from a network time servers on the Internet that you specify in the Time Settings screen (see Configure Basic General System Settings and Time Settings on page 19). Each entry on the Logs screen is stamped with the date and time of day. Problems with the date and time function can include:

- Date and time shown is Fri Dec 31 00:00:00 1999 or a similar incorrect date and time. Cause: The wireless access point has not yet successfully reached the network time server. Check that your Internet access settings are configured correctly. If you have just completed configuring the wireless access point, wait at least 5 minutes and check the date and time again.

- The day is correct or one day ahead or behind, and the hours are ahead or behind. Cause: You have selected an incorrect time zone for your area. Specify the correct time zone in the basic General system settings screen (see Configure Basic General System Settings and Time Settings on page 19).

Use the Packet Capture Tool

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

To capture packets:

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

   ![Packet Capture Screen](imageurl)

   Figure 61.

2. Click Start to start capturing wireless packets leaving or entering the wireless access point on the active operating channel. Packets on the 2.4-GHz interface are captured. Normal functioning of the wireless access point is not affected during the packet capture process.
If any previously captured packets exist, you are prompted to delete them, and only then can you capture new packets.

3. Click **Stop** to stop capturing packets.

4. Click **Save as** to save the packet.pcap file on your computer or to a disk drive.
This appendix provides related documentation, factory default settings, and technical specifications for the ProSAFE Wireless-N Access Point WNAP320.

- Related Documents on this page
- Technical Specifications on page 106
- Factory Default Settings on page 107

Related Documents

This appendix provides links to reference documents you can use to gain a more complete understanding of the technologies used in your NETGEAR product.

Table 28. Related Documents

<table>
<thead>
<tr>
<th>Document</th>
<th>Link</th>
</tr>
</thead>
</table>
## Technical Specifications

### Table 29. ProSAFE Wireless-N Access Point WNAP320 Technical Specifications

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11g data rates</td>
<td>1, 2, 5.5, and 11 Mbps (auto-rate capable)</td>
</tr>
<tr>
<td>802.11bg data rates</td>
<td>1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, and 54 Mbps (auto-rate capable)</td>
</tr>
</tbody>
</table>
| 802.11ng MCS index and data rates | Data rates for a 20 MHz channel width and a short guard interval short (400 ms): Best, 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 130 Mbps, 15 / 144.44 Mbps  
Data rates for a 40 MHz channel width and a short guard interval (400 ms): Best, 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps |
| 802.11b/bg/ng operating frequencies | • 2.412–2.462 GHz (US)  
• 2.457–2.462 GHz (Spain)  
• 2.41–2.484 (Japan 11b)  
• 2.41–2.472 (Japan 11ng)  
• 2.457–2.472 GHz (France)  
• 2.412–2.472 GHz (Europe ETSI) |
| 802.11 b/bg/ng encryption | • 64-bit, 128-bit, and 52-bit WEP  
• AES  
• TKIP |
| Network management | • Remote configuration and management through Web Management Interface, SNMP, or Telnet with command-line interface (CLI)  
• SNMP management supports SNMP MIB I, MIB II, 802.11 MIB and proprietary configuration MIB |
| Maximum clients | Limited by the amount of wireless network traffic generated by each node; maximum 64 supported |
| Status LEDs | • Power/Test LED  
• Link speed LED  
• Ethernet LAN  
• Wireless LAN |
| Power adapter | 12 VDC, 1A; plug is localized to country of sale |
| Physical specifications | • Dimensions (h x w x d): 253.75 x 253.75 x 54.76 mm (10.0 x 10.0 x 2.16 in)  
• Weight: 0.886 kg (1.95 lb) |
Factory Default Settings

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

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

---

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

---

### Table 30. ProSAFE Wireless-N Access Point WNAP320 Default Configuration Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login</strong></td>
<td></td>
</tr>
<tr>
<td>User login URL</td>
<td>192.168.0.100</td>
</tr>
<tr>
<td>User name (case-sensitive)</td>
<td>admin</td>
</tr>
<tr>
<td>Login password (case-sensitive)</td>
<td>password</td>
</tr>
<tr>
<td><strong>Ethernet Connection</strong></td>
<td></td>
</tr>
<tr>
<td>Static IP address</td>
<td>192.168.0.210</td>
</tr>
<tr>
<td>Ethernet MAC address</td>
<td>See bottom label.</td>
</tr>
<tr>
<td>Port speed</td>
<td>10/100/1000</td>
</tr>
</tbody>
</table>
Table 30. ProSAFE Wireless-N Access Point WNAP320 Default Configuration Settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Local Network (LAN)</strong></td>
<td></td>
</tr>
<tr>
<td>LAN IP address</td>
<td>192.168.0.100</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Gateway address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>DHCP server</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCP client</td>
<td>Disabled</td>
</tr>
<tr>
<td>Time zone</td>
<td>USA-Pacific</td>
</tr>
<tr>
<td>SNMP</td>
<td>Disabled</td>
</tr>
<tr>
<td>Spanning Tree Protocol</td>
<td>Disabled</td>
</tr>
<tr>
<td>Secure Shell (SSH)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Secure Telnet</td>
<td>Disabled</td>
</tr>
<tr>
<td><strong>Wireless Local Network (WLAN)</strong></td>
<td></td>
</tr>
<tr>
<td>Operating mode</td>
<td>Access point, infrastructure mode</td>
</tr>
<tr>
<td>Wireless access point name</td>
<td>netgearxxxxxx where xxxxxx is the last 6 digits of the wireless access point MAC address.</td>
</tr>
<tr>
<td>Wireless communication</td>
<td>Enabled</td>
</tr>
<tr>
<td>11 b/g/n wireless network name (SSID)</td>
<td>NETGEAR_11ng</td>
</tr>
<tr>
<td>Broadcast network name SSID</td>
<td>Enabled</td>
</tr>
<tr>
<td>Security</td>
<td>Disabled (open system)</td>
</tr>
<tr>
<td>Transmission speed</td>
<td>Best&lt;sup&gt;a&lt;/sup&gt;</td>
</tr>
<tr>
<td>Country and region</td>
<td>Varies by region</td>
</tr>
<tr>
<td>802.11ng radio frequency channel</td>
<td>Auto</td>
</tr>
<tr>
<td>Output power</td>
<td>Full</td>
</tr>
<tr>
<td>Wireless card access list</td>
<td>All wireless stations allowed</td>
</tr>
<tr>
<td>WMM support</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

<sup>a</sup> 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.
The ProSAFE Wireless-N Access Point WNAP320 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.

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-backup-configuration</td>
</tr>
<tr>
<td></td>
<td>-config&gt;</td>
</tr>
<tr>
<td></td>
<td>-apname</td>
</tr>
<tr>
<td></td>
<td>-country</td>
</tr>
<tr>
<td></td>
<td>-dhcp&gt;</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>-macacl-add</code></td>
<td>add wireless access control (ACL)</td>
</tr>
<tr>
<td><code>-macacl-database</code></td>
<td>delete wireless access control (ACL) database</td>
</tr>
<tr>
<td><code>-macacl-del</code></td>
<td>delete wireless access control (ACL)</td>
</tr>
<tr>
<td><code>-mcsrate</code></td>
<td>transmit data rate</td>
</tr>
<tr>
<td><code>-mode</code></td>
<td>enable wireless access control (ACL)</td>
</tr>
<tr>
<td><code>-operation-mode</code></td>
<td>wireless operation mode</td>
</tr>
<tr>
<td><code>-power</code></td>
<td>wireless transmit power</td>
</tr>
<tr>
<td><code>-preamble</code></td>
<td>wireless preamble (only effect on 802.11b rates)</td>
</tr>
<tr>
<td><code>-radio</code></td>
<td>enable wireless radio</td>
</tr>
<tr>
<td><code>-rate</code></td>
<td>wireless transmission date rate</td>
</tr>
<tr>
<td><code>-rifs-transmission</code></td>
<td>enable successive frame transmission at different transmit powers</td>
</tr>
<tr>
<td><code>-rogue-ap-detection</code></td>
<td>enable rogue access point detection</td>
</tr>
<tr>
<td><code>-security-threshold</code></td>
<td>wireless RTS/CTS threshold</td>
</tr>
<tr>
<td><code>-security-profile&gt;</code></td>
<td>create security profile</td>
</tr>
<tr>
<td><code>-1&gt;</code></td>
<td>1st security profile</td>
</tr>
<tr>
<td><code>-authentication</code></td>
<td>authentication type</td>
</tr>
<tr>
<td><code>-encryption</code></td>
<td>data encryption</td>
</tr>
<tr>
<td><code>-hide-network-name</code></td>
<td>hide network name</td>
</tr>
<tr>
<td><code>-key1</code></td>
<td>wireless wep key 1</td>
</tr>
<tr>
<td><code>-key2</code></td>
<td>wireless wep key 2</td>
</tr>
<tr>
<td><code>-key3</code></td>
<td>wireless wep key 3</td>
</tr>
<tr>
<td><code>-key4</code></td>
<td>wireless wep key 4</td>
</tr>
<tr>
<td><code>-keyno</code></td>
<td>key number</td>
</tr>
<tr>
<td><code>-name</code></td>
<td>profile name</td>
</tr>
<tr>
<td><code>-presharedkey</code></td>
<td>pre-shared key</td>
</tr>
<tr>
<td><code>-security-separation</code></td>
<td>disable associated wireless client communication</td>
</tr>
<tr>
<td><code>-ssid</code></td>
<td>network name (1-32 chars)</td>
</tr>
<tr>
<td><code>-status</code></td>
<td>profile status</td>
</tr>
<tr>
<td><code>-vlan-id</code></td>
<td>VLAN id</td>
</tr>
<tr>
<td><code>-wep-pass-phrase</code></td>
<td>wireless wep passphrase key</td>
</tr>
<tr>
<td><code>-wepkeytype</code></td>
<td>wireless wep key type</td>
</tr>
<tr>
<td><code>-2&gt;</code></td>
<td>2nd security profile</td>
</tr>
<tr>
<td><code>-authentication</code></td>
<td>authentication type</td>
</tr>
<tr>
<td><code>-encryption</code></td>
<td>data encryption</td>
</tr>
<tr>
<td><code>-hide-network-name</code></td>
<td>hide network name</td>
</tr>
<tr>
<td><code>-key1</code></td>
<td>wireless wep key 1</td>
</tr>
<tr>
<td><code>-key2</code></td>
<td>wireless wep key 2</td>
</tr>
<tr>
<td><code>-key3</code></td>
<td>wireless wep key 3</td>
</tr>
<tr>
<td><code>-key4</code></td>
<td>wireless wep key 4</td>
</tr>
<tr>
<td><code>-keyno</code></td>
<td>key number</td>
</tr>
<tr>
<td><code>-name</code></td>
<td>profile name</td>
</tr>
<tr>
<td><code>-presharedkey</code></td>
<td>pre-shared key</td>
</tr>
<tr>
<td><code>-security-separation</code></td>
<td>disable associated wireless client communication</td>
</tr>
<tr>
<td><code>-ssid</code></td>
<td>network name (1-32 chars)</td>
</tr>
</tbody>
</table>
| | | | | | 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
-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
-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
- `--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 authentication server port
| | | | -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 TrapCommunity
| | | | -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
## Numerics

- 11b, 11bg, 11ng (wireless modes) 25
- 2.4-GHz antenna, connector for 12
- 802.11d support 81
- 802.1Q VLAN 8

## A

- access control, wireless stations 43
- access point EDCA parameters 83
- access, restricting by MAC address 50
- accounting, RADIUS servers 48, 49
- Active LED
  - behavior 17
  - description 11
  - troubleshooting 99
- ActiveX 100
- activity log 70
- admin password
  - changing or restoring 64
  - default 107
- Advanced Encryption Standard (AES) 36, 46, 47
- Aggregated MAC Protocol Data Unit (A-MPDU) frames 80
- aggregation length 80
- antenna
  - enabling internal or external 81
  - external orientation 15
- Arbitration Inter-Frame Spacing (AIFS) interval 83
- associated identifier (AID) 69
- associations, clients 72
- Australia, channels/frequency 25
- authentication
  - network 37
  - RADIUS servers 48, 49
- autosensing over Ethernet 9

## B

- background traffic
  - advanced QoS 82
  - WMM QoS 53
- backing up 60
- basic service set (BSS) 37
- basic service set identifier (BSSID)
  - combining with VLANs 35
  - number supported 36
- beacon interval 80
- beacons, unknown access points 74
- best effort traffic
  - advanced QoS 82
  - WMM QoS 53
- bridging, wireless 84
- broadcasting packets, transmitted and received 72
- broadcasting, wireless network name (SSID) 25, 35, 40
- browsers, recommended 18
- BSS (basic service set) 37
- BSSID (basic service set identifier)
  - combining with VLANs 35
  - number supported 36
- bytes, received and transmitted
  - over Ethernet connection 71
  - over wireless connection 70

## C

- Canada, channels/frequency 25
- capturing packets 103
- Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) 80
- Carrier Sense Multiple Access with Collision Detection (CSMA/CD) 80
- Category 5 Ethernet cable 7
- channel bonding 26
- channel width and offset (11ng only) 25, 26
- channels
  - defaults 25
  - wireless spacing 15
- Clear to Send (CTS) packets 80
- CLI command sets 109
- client mode, bridging
  - configuring 96
  - description 85
- clients
  - associations 72
  - DHCP 21
isolation 81
maximum number 81
NTP 20
wireless separation 37, 42
compliance
electromagnetic 107
configuration file, backing up or restoring 60
connectors and ports, rear panel 12
console port 12
cwMax (Maximum Contention Window) value 83
cwMin (Minimum Contention Window) value 83

data encryption
key generation, WEP 45
key size, WEP 44
WPA and WPA2 47
data rate (11b and 11bg only) 26
data rates 106
date, troubleshooting 103
defaults
channels 25
DHCP gateway 23
factory settings 107
factory, restoring to 62
frequency 25
IP address 18
ISP gateway 22
login password 107
password 18
SNMP 56
subnet mask 22, 108
user name 18, 107
Delivery Traffic Indication Message (DTIM) interval 80
DHCP
clients 21
servers 23
DNS servers
DHCP 23
ISP 22
documents, reference 105
dynamic and static VLANs 42

electromagnetic compliance 107
encryption
key generation, WEP 45
key size, WEP 44
WPA and WPA2 47
Enhanced Distributed Channel Access (EDCA) parameters 81
environmental specifications 107
Ethernet cabling requirements 15
Europe, channels/frequency 25
Extended Service Set (ESS) 37
external antenna, enabling 81

F
factory default settings 107
firmware
backing up 60
factory defaults 62
restoring 61
upgrade 59
version 67
flash memory 58
fragmentation length 80
frequency, defaults 25
FTP traffic
advanced QoS 82
WMM QoS 53

gateways
default (ISP) 22
DHCP 23
generating keys, WEP 44
Gigabit Ethernet (RJ-45) port 12
glossary, link to 105
graphical user interface (GUI)
description 18
troubleshooting 100
guard interval (11ng only) 26

H
half-duplex mode 95
hotspot, server 78
HTTP redirect, enabling 78

I
idle time 70
importing, file with known access points 73
infrastructure mode 26
installation kits 28
installation order 16
interference
channels 15
sources of 15
internal antenna, disabling 81
Internet browsing, troubleshooting 99
IP addresses
  default, 18, 21
  DHCP DNS servers, 23
  DHCP ranges, 23
  DHCP WINS servers, 23
  ISP DNS servers, 22
  LAN, 108
  NTP servers, 21
  RADIUS servers, 49
  SNMP manager, 56
  static, 107
  syslog server, 65
  TFTP server, 60
isolation, clients, 81

J
Java and Javascript, 100

K
key update, RADIUS servers, 49
keys, generation, WEP, 45

L
LAN
  configuration requirements, 15
  IP address, 108
  troubleshooting, 99
LAN LED
  behavior, 17
  description, 11
  troubleshooting, 99
LAN path, troubleshooting, 101
lease, DHCP, 23
LEDs
  behavior, 17
  description, 11
  startup procedure, 98
  troubleshooting, 98
legacy 802.1X (wireless security), 41, 45
local MAC addresses, 50
location, country, and region, 20
log, activities, 70
logging in, 18
login URL, name, and password, 107
losing, wireless connection, 51

M
MAC addresses
  Ethernet port, 67

known access points, 75
restricting access by, 35, 50
unknown access points, 74
wireless access point, 20
wireless card, 67
management VLAN, 77
management, options, 55
maximum burst value, 83
Maximum Contention Window (cwMax) value, 83
maximum number of clients, 81
MCS, index and data rate (11ng only), 25
Minimum Contention Window (cwMin) value, 83
mixed mode. See WPA and WPA2 mixed mode.
Modulation and Coding Scheme (MCS), 25
mounting plate
  ceiling, 28
  wall, 30
multicast packets, transmitted and received, 72

N
name, wireless access point, 20
names, profiles, 40
NetBIOS name, 20
network
  authentication, 37
  configuration, troubleshooting, 102
  integrity check, 22
Network Time Protocol (NTP), client and server, 20

O
open system, 41
operating frequencies, 106
order of installation and configuration, 16
output power, transmission, 26

P
package contents, 7
packets
  capturing, 103
  Ethernet, received and transmitted, 71
  wireless, received and transmitted, 72
passphrase
  WEP, 44
  WPA, WPA2, and mixed mode, 48
password
  changing or restoring, 64
  default, 18
  login, 107
physical connections, 102
physical specifications 106
pinging, wireless access point 100, 101
placement, wireless equipment 14
point-to-multipoint bridge
configuring 88
description 84
point-to-point bridge
configuring 85
description 84
policy, access control 43
port and connectors, rear panel 12
ports
  RADIUS servers 49
  SNMP manager, traps 56
  syslog server 65
power adapter 106
Power over Ethernet (PoE) 9, 17
Power/Test LED
  behavior 17
  description 11
  troubleshooting 98
powersaving, WMM 54
preamble type 80
pre-shared key (PSK). See WPA, see WPA2, and see WPA and WPA2 mixed mode.
priority queues
  advanced QoS 82
  WMM QoS 53
profile settings 40
profiles, security
  creating and configuring 39
  description 36
protection spacing (11ng only) 25

Q
QoS (quality of service)
  advanced 81
  WMM 53

R
radio
  scheduling 52
  turning off 25
RADIUS servers, configuring 48
range guidelines, wireless equipment 14
read-only name, read-write name, SNMP 56
rear panel 12
reauthentication time, RADIUS servers 49
rebooting, from Web Management Interface 64
received signal strength indicator (RSSI) 70
redirecting, HTTP requests 78
Reduced Interframe Space (RIFS) transmission 80
reference documents 105
remote devices, troubleshooting 102
remote MAC addresses 50
remote management, options 55
repeater mode, bridging
  configuring 92
  description 84
Request to Send (RTS) threshold 80
Reset button 12, 63, 107
restoring
  factory defaults 62
  password 65
  settings 61
restricting access, by MAC address 35
RIFS (Reduced Interframe Space) transmission 80
roaming 37
rogue access points, detection of 72
RSSI (received signal strength indicator) 70
RTS (Request to Send) threshold 80
Rx sequence 70

S
scheduling, wireless radio 52
Secure Shell (SSH), enabling 57
security lock 12
security profiles
  creating and configuring 39
  description 36
security, wireless options 34
separation, wireless clients 37, 42
servers
  DHCP 23
  DNS 22
  hotspot 78
  NTP 21
  RADIUS 48
  syslog 65
service set identifiers. See SSIDs.
shared key 41, 44
shared secrets, RADIUS servers 49
show configuration, CLI command 58
signal-to-noise ratio (SNR) 70
SMA connectors 12
SNMP
  defaults 56
  manager, IP address 56
software
  backing up 60
factory defaults 62
restoring 61
upgrading 59
version 67
Spanning Tree Protocol (STP), enabling 77
specifications
environmental 107
physical 106
SSH (Secure Shell), enabling 57
SSIDs
broadcasting 25, 35
changing 25, 40
matching 26
static and dynamic VLANs 42
station EDCA parameters 83
statistics, traffic 71
STP (Spanning Tree Protocol), enabling 77
streaming media
advanced QoS 82
WMM QoS 53
subnet mask
default 108
DHCP clients 23
wireless access point 22
supported standards 8
syslog 65
system requirements 7
T
tagged VLAN 77
TCP/IP network, troubleshooting 101
technical specifications 106
Telnet, enabling 57
Temporal Key Integrity Protocol (TKIP) 36
TFTP server, upgrade procedure 59
time and time zone
configuring 20
troubleshooting 103
time-out error 101
TKIP (Temporal Key Integrity Protocol) 36, 46, 47
TKIP + AES (WPA & WPA2 mixed mode) 46
top panel 11
traffic
advanced QoS 82
patterns, analyzing 103
statistics 71
WMM QoS 53
Transmission Opportunity (TXOP) limit 84
transmission output power 26
trap community name 56
traps, SNMP 56
troubleshooting 102
basic functioning 98
browser configuration 100
capturing packets 103
date 103
Internet and LAN connection 99
LAN path 101
LEDs 98
network configuration 102
path to remote device 102
physical connections 102
pinging 100, 101
PoE connection 98
power cord 98
TCP/IP settings 99
time and time zone 103
time-out error 101
trusted, wireless stations 51
Tx sequence 70
TXOP (Transmission Opportunity) limit 84
U
unicast packets
encryption methods 46
transmitted and received 72
Unites States, channels/frequency 25
untagged VLAN 76
upgrading, software 59
URLs, redirecting 78
user name, default 18, 107
V
version, software 67
video traffic
advanced QoS 82
WMM QoS 53
VLANs
dynamic and static 42
identifiers (IDs) 37, 42
tagged, untagged, and management, enabling 76
VoIP traffic
advanced QoS 82
WMM QoS 53
W
web browsers, recommended 18
Web Management Interface
description 18
troubleshooting 100
WEP
configuring with a shared key 41, 44
configuring with RADIUS 41, 45
data encryption, key size 44
legacy 802.1X 45
open system 43
passphrase 44
types of encryption 35
Wi-Fi Multimedia (WMM) 9, 52, 54
Wi-Fi protected access. See WPA and see WPA2.
WINS servers 23
wired equivalent privacy. See WEP.
wireless adapters, 802.11b/g and 802.11n 15
wireless bridging 84
wireless clients, separation 37, 42
wireless connection, losing 51
wireless equipment, placement and range 14
wireless modes 25
wireless network name (SSID)
  broadcasting 25
  changing 25, 40
wireless security
  options 34
  settings 41
wireless stations
  access control 43
  trusted 51
WLAN LED
  behavior 17
  description 11
  troubleshooting 99
WMM (Wi-Fi Multimedia) 9, 52, 54
WPA
  adapter restrictions 41
  configuring with PSK 41, 47
  configuring with RADIUS 41, 45
  encryption 47
  passphrase 47, 48
  TKIP 46, 47
  types of encryption 36
WPA and WPA2 mixed mode
  adapter restrictions 41
  configuring with PSK 42, 47
  configuring with RADIUS 41, 46
  encryption 47
  passphrase 47, 48
  TKIP + AES 46, 47
  types of encryption 36
WPA2
  adapter restrictions 41
  AES 46, 47
  configuring with PSK 42, 47
  configuring with RADIUS 41, 46
  encryption 47
  passphrase 47, 48
  types of encryption 36