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>202-10983-04</td>
<td>November 2015</td>
<td>Revised the Support section on this page.</td>
</tr>
<tr>
<td>202-10983-03</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>202-10983-02 (v2.0)</td>
<td>October 2012</td>
<td>Minor nontechnical revisions</td>
</tr>
<tr>
<td>202-10983-02 (v1.0)</td>
<td>September 2012</td>
<td>• Added and refined information (no new features added)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Appendix B, Command-Line Reference</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Added Index</td>
</tr>
<tr>
<td>202-10983-01</td>
<td>August 2012</td>
<td>First publication.</td>
</tr>
</tbody>
</table>
This chapter introduces the NETGEAR® ProSAFE® Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620 and describes some of the key features. The chapter includes the following sections:

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

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

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

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

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

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

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

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

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

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

What Is in the Box?

The product package contains the following items:

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

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

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

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

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

Key Features and Standards

- **Supported Standards and Conventions**
- **Key Features**
- **802.11b/g/n and 802.11a/n Standards–Based Wireless Networking**
- **Autosensing Ethernet Connections with Auto Uplink**

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

Supported Standards and Conventions

The wireless access point supports the following standards and conventions:

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

The multiple BSSID feature allows you to configure up to 16 SSIDs (8 per radio, but only one radio can be active at a time) on your wireless access point and assign different configuration settings to each SSID. All the configured SSIDs are active, and the network devices can connect to the wireless access point by using any of these SSIDs.
• **DHCP server and client.** The DHCP server of the wireless access point can provide a dynamic IPv4 or IPv6 address to wireless clients. The wireless access point can also act as a client and obtain an IPv4 or IPv6 address from a DHCP server on the LAN.

• **SNMP.** The wireless access point supports Simple Network Management Protocol (SNMP) for Management Information Base (MIB) management.

• **STP and LLDP.** The wireless access point supports Spanning Tree Protocol (STP) and Ethernet Link Layer Discovery Protocol (LLDP). LLDP is enabled by default.

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

**Key Features**

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

• **Dual band.** The wireless access point can operate either in the 2.4 GHz band or the 5 GHz band. The choice of band is reflected in the wireless modes that you can select and the administration screens that are displayed in the web management interface.

• **IPv4 and IPv6.** The wireless access point is manageable from either an IPv4 or IPv6 address, it can function as an IPv4 or IPv6 DHCP client, and its DHCP server can allocate either IPv4 or IPv6 addresses.

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

• **WMM.** Wi-Fi Multimedia (WMM) is a subset of the 802.11e standard. WMM allows wireless traffic to have a range of priorities, depending on the kind of data. Time-dependent information, like video or audio, has a higher priority than normal traffic. For WMM to function correctly, wireless clients also need to support WMM.
• **QoS.** Quality of Service (QoS) support lets you configure parameters that affect traffic flowing from the wireless access point to the client station and traffic flowing from the client station to the wireless access point:
  - The QoS settings let you prioritize traffic, such as voice and video traffic, so that packets do not get dropped.
  - The QoS policies let you configure classifications (match clauses) and apply traffic to eight priority queues based on IP precedence, DSCP, MAC address, IP address, and other information that might be present in Layer 2 and Layer 3 packet headers.

• **Wireless IDS/IPS.** The wireless intrusion detection system (IDS) and intrusion prevention system (IPS) can detect and prevent a variety of wireless attacks. Attacks are covered by preconfigured policy rules. When an attack occurs, the wireless access point can notify a network administrator through an email.

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

• **Rogue AP and ad hoc network detection.** Rogue AP filtering and ad hoc network detection ensure that unknown APs and networks are not given access to any part of the secured wireless and wired LAN.

• **Access control.** MAC address filtering can ensure that only trusted wireless stations can use the wireless access point to gain access to the wireless and wired LAN.

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

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

• **Secure Telnet command-line interface.** The secure Telnet command-line interface (CLI) enables direct secure access over the serial port and easy scripting of configuration of multiple wireless access points across an extensive network through the Ethernet interface. A Secure Shell (SSH) client is required.

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

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

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

• **PoE support.** Using Power over Ethernet (PoE), any 802.3af-compliant midspan or end-span source can supply power to the wireless access point over its Ethernet port.

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

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

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

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

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

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

Autosensing Ethernet Connections with Auto Uplink

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

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

Hardware Description

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

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

Top Panel

The LEDs of the wireless access point are described in the following figure and table:
Table 1. Top panel LEDs

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

Figure 2.

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

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

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

Bottom Panel with Product Label

The product label on the bottom of the wireless access point's enclosure displays factory default settings, regulatory compliance, and other information:
Register the Wireless Access Point

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

➢ To register the wireless access point with NETGEAR:

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

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

Figure 3.

Figure 4.
Figure 5.

3. Enter the information in the blank fields. The serial number, model number, and date of purchase are entered automatically.

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

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

What You Need Before You Begin

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

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

Wireless Equipment Placement and Range Guidelines

The range of your wireless connection can vary significantly based on the location of the wireless access point. The latency, data throughput performance, and power consumption of wireless adapters also vary depending on your configuration choices.
**Note:** Failure to follow these guidelines can result in significant performance degradation or inability to connect wirelessly to the wireless access point. For complete performance specifications, see *Appendix A, Supplemental Information*.

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

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

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

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

**Ethernet Cabling Requirements**

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

**LAN Configuration Requirements**

For the initial configuration of your wireless access point, you need to connect a computer to the wireless access point.
Hardware Requirements for Computers on Your LAN

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

Operating Frequency (Channel) Guidelines

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

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

Requirements for Entering IP Addresses

IPv4

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

IPv6

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

The following errors invalidate an IPv6 address:

- More than eight groups of hexadecimal quartets
- More than four hexadecimal characters in a quartet
- More than two colons in a row
Install and Configure the Wireless Access Point

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

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

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

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

Connect the Wireless Access Point to a Computer

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

➢ To set up the wireless access point:

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

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

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

7. Verify the following:

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

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

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

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

   - **5 GHz WLAN LED.** The 5 GHz WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready.
Log In to the Wireless Access Point

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

➢ To log in to the wireless access point:

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

![Login Screen](image)

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

Web Management Interface

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

![Menu Bars](image)

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.
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 11](image-url)
2. Configure the settings as explained in the following table:

**Table 2. Basic general system settings**

<table>
<thead>
<tr>
<th>Setting</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, in which xxxxxx represents the last 6 digits of the wireless access point MAC address. You can replace the default name with a unique name up to 15 characters long. The access point name can be retrieved through SNMP.</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:

![Figure 12.](image)

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

**Table 3. Time system settings**

<table>
<thead>
<tr>
<th>Setting</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>
</tbody>
</table>
3. Click **Apply** to save your settings.

### Configure the IPv4 Settings

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

**WARNING:**

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

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

- To configure the IPv4 settings:
  1. Select **Configuration > IP > IP Settings**. The IP Settings screen displays:
2. Configure the IPv4 settings as explained in the following table:

### Table 4. IPv4 settings

<table>
<thead>
<tr>
<th>Setting</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 receives its IP address, subnet mask, and default gateway settings automatically from the DHCP server on your network when you connect the wireless access point to your LAN.</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>
<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 gateway to which the wireless access point connects.</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 need to obtain it from the ISP and enter it manually in this field.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td></td>
</tr>
<tr>
<td>Network Integrity Check</td>
<td>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.
Configure the Optional DHCPv4 Server

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

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

To configure DHCPv4 server settings:

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

   ![DHCP Server Settings](image)

   **Figure 14.**

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

   **Table 5. DHCP server settings for IPv4**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the <strong>DHCPv4 Server</strong> check box to enable the DHCP server. Use the default settings or specify the pool of IPv4 addresses to be assigned by setting the starting IPv4 address and ending IPv4 address. These addresses should be part of the same IPv4 address subnet as the wireless access point’s LAN IPv4 address.</td>
<td></td>
</tr>
<tr>
<td>DHCP Server VLAN ID</td>
<td>Enter the VLAN ID for the DHCP server. The VLAN ID range is from 1 to 4094. The default VLAN is 1.</td>
</tr>
</tbody>
</table>
Configure the Basic Wireless Settings

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

**WARNING:**

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

### Table 5. DHCP server settings for IPv4 (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Starting IPv4 Address</td>
<td>Enter the first address in the range of IPv4 addresses to be assigned to DHCP clients. The default address is 192.168.1.02.</td>
</tr>
<tr>
<td>Ending IPv4 Address</td>
<td>Enter the last address in the range of IPv4 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 IPv4 Address</td>
<td>Enter the IPv4 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 System (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, if there is any.</td>
</tr>
<tr>
<td>Secondary WINS Server</td>
<td>Enter the IP address of the secondary WINS server for the network, if there is any.</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 one day.</td>
</tr>
</tbody>
</table>

3. Click **Apply** to save your settings.
Configure 802.11b/bg/ng Wireless Settings

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

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

   ![Wireless Settings Screen]

   **Figure 15.**

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

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

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

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

   **Note:** Under normal conditions, you want the radio to be turned on. Turning off the radio disables access through the wireless access point, which can be helpful for configuration, network tuning, or troubleshooting activities.
4. Click **OK** to confirm the change of wireless mode. The change does not take effect until you click the Apply button after you have completed the wireless configuration.

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

**Table 6. Basic 2.4 GHz band wireless settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<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 needs to match the wireless access point’s SSID for the wireless device to communicate with the wireless access point. If the SSIDs do not match, you do not get a wireless connection to the wireless access point.</td>
</tr>
<tr>
<td>Wireless On-Off Status</td>
<td>This field is not configurable. It shows the status of the wireless scheduler. For more information, see <a href="#">Schedule the Wireless Radio to Be Turned Off</a> on page 61.</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 broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point’s SSID. <strong>Yes</strong> is the default setting. To prevent the SSID from being broadcast, select the <strong>No</strong> radio button.</td>
</tr>
</tbody>
</table>
| Channel / Frequency                               | From the drop-down list, select the channel you wish to use for your wireless LAN. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto.  
**Note:** It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see [Operating Frequency (Channel) Guidelines](#) on page 19.  
**Note:** For more information about available channels and frequencies, see [Technical Specifications](#) on page 139. |

**11ng mode only**  
**Note:** For most networks, the default settings work fine.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCS Index / Data Rate</td>
<td>From the drop-down list, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the wireless network. The default setting is Best. For a list of all options that you can select from in 11ng mode, see <a href="#">Factory Default Settings</a> on page 142.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>From the drop-down list, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, and 40 MHz. The default is 20 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz.</td>
</tr>
<tr>
<td>Guard Interval</td>
<td>From the drop-down list, select the guard interval to protect transmissions from interference. The default is Auto, or you can select Long - 800 ns. Some legacy devices can operate only with a long guard interval.</td>
</tr>
</tbody>
</table>
Table 6. Basic 2.4 GHz band wireless settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>11b and 11bg modes only</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 on page 142.</td>
</tr>
</tbody>
</table>
| Output Power                | From the drop-down list, select the transmission power of the wireless access point: Full, Half, Quarter, Eighth, Minimum. The default is Full.  
  **Note:** Increasing the power improves performance, but if two or more wireless access points are operating in the same area and on the same channel, interference can occur.  
  **Note:** Make sure that you comply with the regulatory requirements for total radio frequency (RF) output power in your country. |

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

---

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

---

**Configure 802.11a/na Wireless Settings**

➢ To configure the 802.11a/na wireless settings:

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

---

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

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

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

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

4. Click OK to confirm the change of wireless mode. The change does not take effect until you click the Apply button after you have completed the wireless configuration.
5. Specify the remaining wireless settings as explained in the following table:

Table 7. Basic 5 GHz band wireless settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<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_11na. The SSID assigned to a wireless device needs to match the wireless access point's SSID for the wireless device to communicate with the wireless access point. If the SSIDs do not match, you do not get a wireless connection to the wireless access point.</td>
</tr>
<tr>
<td>Wireless On-Off Status</td>
<td>This is a nonconfigurable field that shows the status of the wireless scheduler. For more information, see Schedule the Wireless Radio to Be Turned Off on page 61.</td>
</tr>
<tr>
<td>Broadcast Wireless Network Name (SSID)</td>
<td>Select the Yes radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point’s SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the No radio button.</td>
</tr>
</tbody>
</table>
| Channel / Frequency           | From the drop-down list, select the channel you wish to use on your wireless LAN. The wireless channels and frequencies depend on the country and wireless mode. The default setting is Auto. 

**Note:** It should not be necessary to change the wireless channel unless you experience interference (indicated by lost connections or slow data transfers). If this happens, you might want to experiment with different channels to see which is the best. For more information, see the guidelines following this table.  

**Note:** For more information about available channels and frequencies, see Technical Specifications on page 139.

11na mode only

**Note:** For most networks, the default settings work fine.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCS Index / Data Rate</td>
<td>From the drop-down list, select a Modulation and Coding Scheme (MCS) index and transmit data rate for the wireless network. The default setting is Best. For a list of all options that you can select from in 11na mode, see Factory Default Settings on page 142.</td>
</tr>
<tr>
<td>Channel Width</td>
<td>From the drop-down list, select a channel width. The options are Dynamic 20/40 MHz, 20 MHz, and 40 MHz. The default is Dynamic 20/40 MHz. A wider channel improves the performance, but some legacy devices can operate only in either 20 MHz or 40 MHz.</td>
</tr>
<tr>
<td>Guard Interval</td>
<td>From the drop-down list, select the guard interval to protect transmissions from interference. The default is Auto, or you can select Long – 800 ns. Some legacy devices can operate only with a long guard interval.</td>
</tr>
</tbody>
</table>
Table 7. Basic 5 GHz band wireless settings (continued)

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

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

---

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

---

**Test Basic Wireless Connectivity**

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

> **To test for wireless connectivity:**

1. Configure the 802.11b/g/n or 802.11a/n wireless adapters of your computers so that they all have the same SSID and channel that you have configured on the wireless access point.

2. Verify that your computers have a wireless link to the wireless access point. If you have enabled the DHCP server on the wireless access point, verify that your computers are able to obtain an IP address through DHCP from the wireless access point.

3. Verify network connectivity by using a browser such as Internet Explorer 6.0 or later or Mozilla Firefox 1.5 or later to browse the Internet, or check for file and printer access on your network.

---

**Note:** If you have trouble connecting to the wireless access point, see Chapter 6, Troubleshooting.
NETGEAR recommends that you complete the following tasks before you deploy the wireless access point in your network:

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

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

Mount the Wireless Access Point

- Ceiling Installation
- Wall Installation
- Desk Installation

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

**Note:** The figures in the procedures in this section do not show theWNDAP620 wireless access point. However, the procedures are generic and do apply to the WNDAP620 wireless access point.

Ceiling Installation

The best location for ceiling installation is at the center of your wireless coverage area, and within line of sight of all mobile devices. Make sure the top (the dome side) of the wireless access point is directed toward the users and not the ceiling.
Note: Do not place the wireless access point in a false ceiling space facing up.

➢ To install the wireless access point using the ceiling installation kit:
   1. Verify the package contents of the ceiling installation kit.
   2. Detach the mounting plate from the wireless access point.
   3. Attach the clamp to the ceiling rail.
4. Attach the mounting plate to the clamp.

5. Connect the cables to the wireless access point.

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

Wall Installation

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

➢ To install the wireless access point using the wall installation kit:
   1. Verify the package contents of the wall installation kit.
2. Detach the mounting plate from the wireless access point.

3. Attach the mounting plate to the wall.

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

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

➢ To install the wireless access point on a desk:
   Attach the rubber feet to the holes in the bottom of the wireless access point.
This chapter describes how to configure the wireless features of the wireless access point. The chapter includes the following sections:

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

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

**WARNING:**

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

### Wireless Data Security Options

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

Figure 17.

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

- **Use multiple BSSIDs combined with VLANs.** You can configure combinations of VLANs and BSSIDs (security profiles) with stronger or less restrictive access security according to your requirements. For example, visitors could be given wireless Internet access but be excluded from any access to your internal network. For information about how to configure BSSIDs, see *Configure and Enable Security Profiles* on page 48.

- **Restrict access based by MAC address.** You can allow only trusted devices to connect so that unknown devices cannot wirelessly connect to the wireless access point. Restricting access by MAC address adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed. For information about how to restrict access by MAC address, see *Restrict Wireless Access by MAC Address* on page 60.

- **Turn off the broadcast of the wireless network name (SSID).** If you disable broadcast of the SSID, only devices that have the correct SSID can connect. This nullifies the wireless network discovery feature of some products, such as Windows XP, but the data is still exposed. For information about how to turn off broadcast of the SSID, see *Configure and Enable Security Profiles* on page 48.

- **WEP.** Wired Equivalent Privacy (WEP) data encryption provides data security. WEP shared key authentication and WEP data encryption block all but the most determined eavesdropper. This data encryption mode has been superseded by WPA-PSK and WPA2-PSK. For information about how to configure WEP, see *Configure and Enable Security Profiles* on page 48 and *Configure an Open System with WEP or Shared Key with WEP* on page 53.

- **Legacy 802.1X.** Legacy 802.1X uses RADIUS-based 802.1x authentication but no data encryption. For information about how to configure Legacy 802.1X, see *Configure and Enable Security Profiles* on page 48 and *Configure Legacy 802.1X* on page 54.
• **WPA and WPA-PSK (TKIP).** Wi-Fi Protected Access (WPA) data encryption provides strong data security with Temporal Key Integrity Protocol (TKIP) encryption. The very strong authentication along with dynamic per-frame rekeying of WPA makes it virtually impossible to compromise.

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

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

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

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

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

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

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

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

### Security Profiles

• *Before You Change the SSID, WEP, and WPA Settings*

• *Configure and Enable Security Profiles*

Security profiles let you configure unique security settings for each SSID on each radio of the wireless access point. For each radio, the wireless access point supports up to eight security profiles (BSSIDs) that you can configure on the individual Edit Wireless Network screens that are accessible from the Edit Security Profile screen (see *Configure and Enable Security Profiles* on page 48).
To set up a security profile, select its network authentication type, data encryption, wireless client security separation, and VLAN ID:

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

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

- **Data encryption**
  Select the data encryption that you want to use. The available options depend on the network authentication setting described earlier (otherwise, the default is None). The data encryption settings are explained in *Configure and Enable Security Profiles* on page 48.

- **Wireless client security separation**
  If this feature is enabled, the associated wireless clients (using the same SSID) are not able to communicate with each other. This feature is useful for hotspots and other public access situations. By default, wireless client separation is disabled. For more information, see *Configure and Enable Security Profiles* on page 48.

- **VLAN ID**
  If this feature is enabled and if the network devices (hubs and switches) on your LAN support the VLAN (802.1Q) standard, the default VLAN ID for the wireless access point is associated with each profile. The default VLAN ID needs to match the IDs that are used by the other network devices. For more information, see *Configure and Enable Security Profiles* on page 48.

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

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

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

Form for 802.11b/bg/ng Modes

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

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

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

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

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

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

  Record the WPA2-PSK passphrase:
  WPA2-PSK passphrase: ________________________________

- **WPA RADIUS settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:
  Server name/IP address: Primary ________________ Secondary ________________
  Port: ___________________________________
  Shared secret: ___________________________________

- **WPA2 RADIUS settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:
  Server name/IP address: Primary ________________ Secondary ________________
  Port: ___________________________________
  Shared secret: ___________________________________
Form for 802.11a/an Modes

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

- **SSID**: The service set identifier (SSID) identifies the wireless local area network. You can customize it by using up to 32 alphanumerics characters. Write your SSID on the line.
  
  SSID: ___________________________________
  
  The SSID in the wireless access point is the SSID you configure on the wireless adapter card. All wireless nodes in the same network need to be configured with the same SSID.

- **WEP key size and authentication**
  Choose the key size by circling one: 64, 128, or 152 bits.
  Choose the authentication type by circling one: open system or shared key.
  
  Passphrase: ________________________________
  
  **Note**: If you select shared key, the other devices in the network cannot connect unless they are set to shared key and have the same keys in the same positions as those in the wireless access point.

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

- **WPA RADIUS settings**
  For WPA, record the following settings for the primary and secondary RADIUS servers:
  
  Server name/IP address: Primary ________________ Secondary ________________
  
  Port: ________________________________
  
  Shared secret: ________________________________

- **WPA2 RADIUS settings**
  For WPA2, record the following settings for the primary and secondary RADIUS servers:
  
  Server name/IP address: Primary ________________ Secondary ________________
  
  Port: ________________________________
  
  Shared secret: ________________________________
Configure and Enable Security Profiles

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

- For 802.11b/bg/ng modes, the 2.4 GHz radio needs to be enabled (see Configure 802.11b/bg/ng Wireless Settings on page 29).
- For 802.11a/na modes, the 5 GHz radio needs to be enabled. (see Configure 802.11a/na Wireless Settings on page 31).

To configure and enable a security profile:

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

   ![Profile Settings Screen](image)

   Figure 18.

2. Optional: To display the Profile Settings screen for the 802.11a/na modes, click the 802.11a/na tab. This screen also shows eight wireless security profiles. (If the 5 GHz radio is disabled, the Enable column is masked out.)
Figure 19.

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

Table 8. Profile settings

<table>
<thead>
<tr>
<th>Setting</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>

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

---

Wireless Configuration and Security

49
4. Specify the settings of the Profile Definition section of the Edit Security Profile screen as explained in the following table:

**Table 9. Profile definition settings**

<table>
<thead>
<tr>
<th>Setting</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 depend on the selected radio band:</td>
</tr>
<tr>
<td></td>
<td>• <strong>802.11b/bg/ng.</strong> The default names are NETGEAR_11ng, NETGEAR_11ng-1, NETGEAR_11ng-2, and so on, through NETGEAR_11ng-7 for the eighth profile.</td>
</tr>
<tr>
<td></td>
<td>• <strong>802.11a/na.</strong> The default names are NETGEAR_11na, NETGEAR_11na-1, NETGEAR_11na-2, and so on, through NETGEAR_11na-7 for the eighth profile.</td>
</tr>
</tbody>
</table>
5. Specify the settings of the Authentication Settings section of the Edit Security Profile screen as explained in the following table.

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

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

### Table 9. Profile authentication settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Authentication and Data Encryption</td>
<td>This is the default setting. Use an open system without any encryption or with WEP encryption. See Configure an Open System with WEP or Shared Key with WEP on page 53.</td>
</tr>
<tr>
<td><strong>Note:</strong> The data encryption fields that display onscreen depend on your selection from the Network Authentication drop-down list.</td>
<td></td>
</tr>
<tr>
<td>Shared Key</td>
<td>Use WEP encryption and enter at least one shared key. See Configure an Open System with WEP or Shared Key with WEP on page 53.</td>
</tr>
<tr>
<td>Legacy 802.1X</td>
<td>Configure the RADIUS server settings. Encryption is not supported. See Configure Legacy 802.1X on page 54.</td>
</tr>
<tr>
<td>WPA with Radius</td>
<td>Configure the RADIUS server settings and select TKIP or TKIP + AES encryption. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA &amp; WPA2 with RADIUS on page 55.</td>
</tr>
<tr>
<td>WPA2 with Radius</td>
<td>Configure the RADIUS server settings and select AES or TKIP + AES encryption. See Configure WPA with RADIUS, WPA2 with RADIUS, and WPA &amp; WPA2 with RADIUS on page 55.</td>
</tr>
</tbody>
</table>

### Table 10. Profile definition settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Broadcast Wireless Network Name (SSID)</td>
<td>Select the <strong>Yes</strong> radio button to enable the wireless access point to broadcast its SSID, allowing wireless stations that have a null (blank) SSID to adopt the wireless access point’s SSID. Yes is the default setting. To prevent the SSID from being broadcast, select the <strong>No</strong> radio button.</td>
</tr>
</tbody>
</table>
6. Optional: In the QoS Policies section of the screen, select a QoS policy from the Incoming drop-down list, Outgoing drop-down list, or both. Depending on your selection, the policy is applied to incoming packets, outgoing packets, or both incoming and outgoing packets, and is displayed in the Policy Details fields.

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

7. Click Apply to save your settings.
WARNING:

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

➢ To change the QoS policy selection on the Edit Security Profile screen:
  1. From the drop-down list from which you want select another QoS policy, select None.
  2. Click Apply to remove the old policy from the security profile.
  3. Select the new QoS policy from the same drop-down list.
  4. Click Apply to save your settings.

Configure an Open System with WEP or Shared Key with WEP

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

• Open system with WEP

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

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

  ![Figure 21.](image)

• 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:
Configure Legacy 802.1X

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

When you select Legacy 802.1X from the Network Authentication drop-down list, the Data Encryption drop-down list is automatically set to None. To use legacy 802.1X security, you need to define the RADIUS servers only.
Configure WPA with RADIUS, WPA2 with RADIUS, and WPA & WPA2 with RADIUS

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

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

- **WPA with RADIUS**

- **WPA2 with RADIUS**

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

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

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

- **WPA-PSK**

  - **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, theWNDAP620 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.

- **WPA2-PSK**

  - **AES**
    - Advanced Encryption Standard (AES) is the standard encryption method used with WPA2.
    - **Note**: Although some wireless clients might support AES with WPA, the WNDAP620 wireless access point does not support WPA with AES.

  - **TKIP + AES**
    - The TKIP + AES encryption method is supported both for WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA & WPA2 mixed mode, TKIP + AES is the only supported data encryption method.
• WPA-PSK & WPA2-PSK

![Configuration Settings](image)

Figure 29.

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption</td>
<td>TKIP 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>AES 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 WNDAP620 wireless access point does not support WPA with AES.</td>
</tr>
<tr>
<td></td>
<td>TKIP + AES TKIP + AES supports both WPA and WPA2. Broadcast packets use TKIP. For unicast (point-to-point) transmissions, WPA clients use TKIP, and WPA2 clients use AES. For the WPA &amp; WPA2 mixed mode, TKIP + AES is the only supported data encryption method.</td>
</tr>
<tr>
<td>Passphrase</td>
<td>Enter a passphrase. The passphrase length needs to be between 8 and 63 characters (inclusive). The default passphrase is sharedsecret. The default setting is No. You can display the actual passphrase by selecting the Show Passphrase in Clear Text Yes radio button.</td>
</tr>
<tr>
<td>Show Passphrase in Clear Text</td>
<td>Select the Yes radio button to display the actual passphrase in the Passphrase field. The default setting is No.</td>
</tr>
</tbody>
</table>

**Configure RADIUS Server Settings**

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

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


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

**Table 14. RADIUS server settings for IPv4 and IPv6**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius Server Settings</td>
<td></td>
</tr>
<tr>
<td>Primary Authentication Server</td>
<td>IPv4 Address or IPv6 Address Enter the IP address of the primary RADIUS server for authentication.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the UDP port on the wireless access point that is used to access the primary RADIUS server for authentication. The default port number is 1812.</td>
</tr>
<tr>
<td>Shared Secret</td>
<td>Enter the shared key that is used between the wireless access point and the primary RADIUS server during authentication.</td>
</tr>
</tbody>
</table>
### Table 14. RADIUS server settings for IPv4 and IPv6 (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Secondary Authentication Server</strong></td>
<td>IPv4 Address or IPv6 Address</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the number of the UDP port on the wireless access point that is used to access the secondary RADIUS server for authentication. The default port number is 1812.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></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><strong>Primary Accounting Server</strong></td>
<td>IPv4 Address or IPv6 Address</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the number of the UDP port on the wireless access point that is used to access the primary RADIUS server for accounting. The default port number is 1813.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></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><strong>Secondary Accounting Server</strong></td>
<td>IPv4 Address or IPv6 Address</td>
</tr>
<tr>
<td><strong>Port</strong></td>
<td>Enter the number of the UDP port on the wireless access point that is used to access the secondary RADIUS server for accounting. The default port number is 1813.</td>
</tr>
<tr>
<td><strong>Shared Secret</strong></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>
</tbody>
</table>

**Authentication Settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<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 connect wirelessly to the wireless access point. MAC address filtering adds an obstacle against unwanted access to your network, but the data broadcast over the wireless link is fully exposed.

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

To restrict access based on MAC addresses:

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

![MAC Authentication Screen](image)

2. Optional: To display the MAC Authentication screen for the 802.11a/na modes, click the 802.11a/na tab.

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

4. From the Select Access Control Database drop-down list, select one of the following database options:
   - **Local MAC Address Database**. The wireless access point uses the local MAC address database for access control. This is the default setting.
   - **Remote MAC Address Database**. The wireless access point uses the MAC address database on an external RADIUS server on the LAN for access control. If you select this database, you first need to configure the RADIUS server settings (see **Configure RADIUS Server Settings** on page 57).
5. Click **Refresh** to refresh the Available Wireless Stations table. The wireless access point places the MAC addresses of the attached wireless stations in this table.

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

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

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

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

**WARNING:**

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

### Schedule the Wireless Radio to Be Turned Off

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

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

1. Select **Configuration > Wireless > Basic > Wireless On-Off**. The Wireless On-Off screen displays:
2. Specify the settings as explained in the following table:

Table 15. Wireless radio on/off settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>Enter 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>Enter 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 also need to support WMM.

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

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

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

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

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

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

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

➢ **To configure basic wireless QoS:**

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

![QoS Settings Screen](image)

   *Figure 33.*

2. Optional: To display the basic QoS Settings screen for the 802.11a/na modes, click the **802.11a/na** tab.

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

4. Click **Apply** to save your settings.
This chapter describes how to use the management and monitoring features of the wireless access point. The chapter includes the following sections:

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

Enable Remote Management

- SNMP Management
- Secure Shell and Telnet Management

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

**SNMP Management**

- To set up an SNMP management interface:
  1. Select Maintenance > Remote Management > SNMP. The SNMP screen displays:
2. Specify the settings as explained in the following table:

**Table 16. SNMP settings**

<table>
<thead>
<tr>
<th>Setting</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>Enter 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>Enter the IP address of the SNMP manager to receive traps sent from the wireless access point.</td>
</tr>
<tr>
<td>Trap Port</td>
<td>Enter the number of the SNMP manager port 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 35.

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

3. Click Apply to save your settings.

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

1. Connect an Ethernet cable to the console port of the wireless access point.

2. Connect the other end of the cable to a VT100/ANSI terminal or a workstation.

   If you attach a PC, Apple Macintosh, or UNIX workstation, start a secure terminal emulation program, and configure the terminal emulation program to use the following settings:
   - Baud rate: 9600 bps
   - Data bits: 8
   - Parity: none
   - Stop bit: 1
   - Flow control: none

3. Start a secure Telnet session from the terminal or workstation to the wireless access point. A screen similar to the following displays:
4. Enter the login name and password (admin and password are the defaults).

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

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

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

Upgrade the Wireless Access Point Software

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

• Web Browser Upgrade Procedure
• TFTP Server Upgrade Procedure

Note: The web browser that you use to upload new firmware into the wireless access point needs to support HTTP uploads. Use a browser such as Microsoft Internet Explorer 6.0 or later or Mozilla 1.5 or later.
Note: You cannot perform the software upgrade from a computer that is connected to the wireless access point over a wireless link. You need to use a computer that is connected to the wireless access point over an Ethernet cable.

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

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

Web Browser Upgrade Procedure

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

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

![Firmware Upgrade Screen](image)

Figure 37.
5. Click **Browse** and locate the image (.zip) upgrade file.

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

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

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

### TFTP Server Upgrade Procedure

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

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

1. Download the new software file from the NETGEAR website and save it to your hard disk.

2. Place the software file in your TFTP server location. (You do not need to unzip the file.)

3. If available, read the release notes before upgrading the software.

4. Select **Maintenance > Upgrade > Firmware Upgrade TFTP**. The Firmware Upgrade TFTP screen displays:

   ![Figure 38](image)

5. Specify the following information:

   - **Firmware File Name**. The name of the unzipped software file.
   - **TFTP Server IP**. The IP address of your TFTP server.

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

   During the upgrade process, the wireless access point automatically restarts. The upgrade process typically takes several minutes. When the Test LED turns off, wait a few more seconds before doing anything with the wireless access point.
7. Verify that the new software file has been installed by selecting **Monitoring > System**. The System screen displays (see Figure 46 on page 78). The firmware version is shown in the Access Point Information section of the screen.

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

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

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

### Save the Configuration

➢ **To save your settings:**

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

![Backup Settings](image)

Figure 39.
Restore the Configuration

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

➢ To restore your settings from a saved configuration file:
1. Select **Maintenance > Upgrade > Restore Settings**. The Restore Settings screen displays:

![Restore Settings](image)

 Figure 40.

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

**Restore the Wireless Access Point to the Factory Default Settings**

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

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

Use the Web Management Interface to Restore Factory Default Settings

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

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

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

   ![Restore Defaults Screen](image)

   Figure 41.

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

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

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

To restore the factory default settings using the Reset button:

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

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

2. Release the Reset button.

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

Reboot the Wireless Access Point without Restoring the Default Configuration

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

To reboot the wireless access point:

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

   ![Reboot AP Screen]

   Figure 42.

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

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

**Change the Administrator Password**

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

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

➢ **To change the administrator password:**

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

![Change Password Screen](image)

   **Figure 43.**

2. Take one of the following actions:

   - Enter a new password twice, once in the New Password field and again in the Repeat New Password field.
   - Next to Restore Default Password, select the **Yes** radio button to restore the default password. By default, the No radio button is selected.

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

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

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

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

➢ To add a new user account:

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

   ![User Accounts Screen](image)

   **Figure 44.**

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

   **Table 17. Add user account settings**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>Enter a new user name</td>
</tr>
<tr>
<td>Password</td>
<td>Enter a password between 4 and 12 characters in length.</td>
</tr>
<tr>
<td>Privilege</td>
<td>From the Privilege drop-down list, select <strong>Read Write</strong> or <strong>Read Only</strong>.</td>
</tr>
</tbody>
</table>

3. Click **Add**.

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

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

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

---

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

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

---

Enable the Syslog Server

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

To enable a syslog server:
1. Select Configuration > System > Advanced > Syslog. The Syslog screen displays:
Specify the settings as explained in the following table:

### Table 18. Syslog settings

<table>
<thead>
<tr>
<th>Setting</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

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

## View System Information

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

![System Screen](image)

Figure 46.
The following table explains the fields of the System screen:

**Table 19. System screen fields**

<table>
<thead>
<tr>
<th>Setting</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</em> on page 23.</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>Ethernet LLDP</td>
<td>Enabled indicates that LLDP is enabled. Disabled indicates that it is not.</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</em> on page 23.</td>
</tr>
<tr>
<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>
<td></td>
</tr>
<tr>
<td>Firmware Version</td>
<td>The version of the firmware that is currently installed.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The serial number of the wireless access point.</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</em> on page 23.</td>
</tr>
<tr>
<td><strong>Current IPv4 Settings</strong></td>
<td>For information about how to change any of these IP settings, see <em>Configure the IPv4 Settings</em> on page 25.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IPv4 address of the wireless access point.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The subnet mask for the address of the wireless access point.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The default IPv4 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 DHCPv4 server on your LAN network. Disabled indicates a static IP configuration.</td>
</tr>
<tr>
<td><strong>Current IPv6 Settings</strong></td>
<td>For information about how to change any of these IP settings, see <em>Configure IPv6 Settings and Optional DHCPv6 Server Settings</em> on page 99.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The default IPv6 address of the wireless access point.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>The prefix length for the address of the wireless access point.</td>
</tr>
<tr>
<td>Dynamic IPv6 Address</td>
<td>The dynamically assigned IPv6 address if the DHCPv6 server has the stateful option enabled.</td>
</tr>
<tr>
<td>Default Gateway</td>
<td>The default IPv6 gateway for the wireless access point communication.</td>
</tr>
<tr>
<td>LAN IPv6 Link-Local Address</td>
<td>This is an automatically generated IPv6 address that uses the IPv4 address in the interface portion of its address.</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 or 802.11a or 802.11na).

Note: The section heading depends on the configured wireless mode.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Wireless Settings for 802.11b, 802.11g, or 802.11ng or Current Wireless Settings for 802.11a or 802.11na</td>
<td>The operating mode of the wireless access point. One of the following modes is indicated: • Access Point • Point-to-Point Bridge • Point-to-Point Bridge with Access Point • Multi-Point Bridge with/without client association For information about how to change the mode, see Configure Wireless Bridging on page 118.</td>
</tr>
<tr>
<td>Access Point Mode</td>
<td>The channel that the wireless port is using. For information about how to change the channel and frequency, see Configure 802.11b/bg/ng Wireless Settings on page 29 and Configure 802.11a/na Wireless Settings on page 31.</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 for the 2.4-GHz band, or 802.11a or 802.11na for the 5-GHz band).

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

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

1. Select Monitoring > Wireless Stations. The Wireless Stations screen displays:
To update the list, click **Refresh**. If the wireless access point is rebooted, the wireless station data is lost until the wireless access point rediscovers the devices. To force the wireless access point to look for associated devices, click **Refresh**.

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

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

**Table 20. Wireless stations details fields**

<table>
<thead>
<tr>
<th>Setting</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>
<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 summary of the capability of the wireless station that was detected during association.</td>
</tr>
<tr>
<td>Cipher</td>
<td>The cipher that the wireless station is using 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>
View the Activity Log

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

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

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

![Logs Screen](image)

   Figure 49.

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

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

Traffic Statistics

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

➢ **To display the Statistics screen:**

Select **Monitoring > Statistics**.
Figure 50.

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

The following table explains the fields of the Statistics screen:

**Table 21. Statistics fields**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wired Ethernet</td>
<td></td>
</tr>
<tr>
<td>Packets</td>
<td>The number of packets received and transmitted over the Ethernet connection</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Wireless 802.11ng</td>
<td></td>
</tr>
<tr>
<td>Unicast Packets</td>
<td>The number of unicast packets received and transmitted over the wireless</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>connection since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Multicast Packets</td>
<td></td>
</tr>
<tr>
<td>Total Packets</td>
<td>The number of packets received and transmitted over the wireless connection</td>
</tr>
<tr>
<td></td>
<td>since the wireless access point was restarted.</td>
</tr>
<tr>
<td>Total Bytes</td>
<td>The number of bytes received and transmitted over the wireless connection</td>
</tr>
<tr>
<td></td>
<td>since the wireless access point was restarted.</td>
</tr>
</tbody>
</table>

**Wireless 802.11b, Wireless 802.11bg, Wireless 801.11ng, Wireless 802.11a, or Wireless 802.11na**

**Note:** The section heading depends on the configured wireless mode.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast Packets</td>
<td>The number of unicast packets received and transmitted over the wireless</td>
</tr>
<tr>
<td></td>
<td>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
- View and Save Access Point Lists

Enable and Configure Rogue AP Detection

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

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

To enable and configure rogue AP detection:

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

Table 21. Statistics fields (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>Client Association</td>
<td>The number of associated clients connected to the radio in the configured wireless modes.</td>
</tr>
</tbody>
</table>

| 802.11b Radio, 802.11bg Radio, or 802.11ng Radio 802.11na Radio or 802.11a Radio | The number of associated clients connected to the radio in the configured wireless modes. |
2. Optional: To enable and configure rogue AP detection for the 802.11a/na modes, click the 802.11a/na tab.

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

4. Specify the detection policy by making a selection from the Rogue AP Detection Policy drop-down list:
   - **Mild.** The wireless access point scans for rogue access points every 10 seconds.
   - **Moderate.** The wireless access point scans for rogue access points every 5 seconds. This is the default setting.
   - **Aggressive.** The wireless access point scans for rogue access points every second.

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

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

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

8. Click Apply to save your settings.

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

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

2. Click Delete.

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

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

2. Click **Browse** and locate the file that contains the list of access points. This file needs to be a simple text file with one MAC address per line.

3. Select the file, and click **Open**.

4. Click **Apply** to upload the list of access points to the Known AP List.

### View and Save Access Point Lists

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

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

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

![Unknown AP List](image)

**Figure 52.**

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

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

**Table 22. Unknown AP List fields**

<table>
<thead>
<tr>
<th>Setting</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 security is enabled (1 means enabled; 0 means disabled).</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel that the unknown AP is using.</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>
</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 85).

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

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

![Known AP List Screen](image)

Figure 53.

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

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

<table>
<thead>
<tr>
<th>Setting</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 85).
Configure Wireless Intrusion Detection and Prevention

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

Configure Wireless Intrusion Detection and Prevention Policy Settings

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

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

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

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

Table 24. IDS/IPS policies and policy rules

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Policy Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Threshold</td>
<td>Notification</td>
</tr>
<tr>
<td>Authentication flood</td>
<td><strong>Attack.</strong> Multiple authentication requests (5 or more) that use spoofed MAC addresses of legitimate clients are sent to the wireless access point.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td><strong>Result.</strong> The client association table overflows, causing authentication requests from legitimate clients to be denied.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Solution.</strong> The oldest clients that are stuck in the authentication phase are removed from the table.</td>
<td></td>
</tr>
<tr>
<td>Association flood</td>
<td><strong>Attack.</strong> Multiple association requests (5 or more) that use spoofed MAC addresses of legitimate clients are sent to the wireless access point.</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td><strong>Result.</strong> The client association table overflows, causing association requests from legitimate clients to be denied.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Solution.</strong> The oldest associations are removed from the table.</td>
<td></td>
</tr>
</tbody>
</table>
Table 24. IDS/IPS policies and policy rules (continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Policy Rule</th>
</tr>
</thead>
</table>
| Unauthenticated association           | **Attack.** Multiple unauthenticated association requests (5 or more) that use spoofed MAC addresses of legitimate clients are sent to the wireless access point.  
**Result.** The client association table overflows, causing authentication requests from legitimate clients to be denied.  
**Solution.** The oldest clients that are stuck in the authentication phase are removed from the table. | 5           |
| Association table overflow            | **Attack.** Multiple clients (5 or more) that use spoofed MAC addresses of legitimate clients attempt to connect to the wireless access point.  
**Result.** The client association table overflows, causing association requests from legitimate clients to be denied.  
**Solution.** The oldest associations are removed from the table. | 5           |
| Authentication failure attack         | **Attack.** Multiple invalid authentication requests (5 or more) that use the spoofed MAC address of a legitimate client are sent to the wireless access point.  
**Result.** The client is disconnected from the wireless access point.  
**Solution.** The wireless access point determines if the legitimate client is already connected before processing an authentication request. | 5           |
| Deauthentication broadcast attack     | **Attack.** Multiple deauthentication frames (5 or more) that use the spoofed MAC address of the wireless access point are sent to legitimate clients.  
**Result.** Clients are disconnected from the wireless access point.  
**Note:** The IDS detects this attack, but the IPS does not take action against this attack. | 5           |
| Disassociation flood                  | **Attack.** Multiple disassociation frames (5 or more) that use the spoofed MAC address of the wireless access point are sent to a legitimate client.  
**Result.** The client is disconnected from the wireless access point.  
**Note:** The IDS detects this attack, but the IPS does not take action against this attack. | 5           |
| Malformed 802.11 packets detected     | **Detection.** Multiple malformed packets (5 or more) are sent to the wireless access point.  
**Result.** Clients behave unexpectedly or crash.  
**Solution.** The wireless access point drops the malformed packets. | 5           |
Table 24. IDS/IPS policies and policy rules (continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Policy Rule</th>
<th>Threshold</th>
<th>Notification</th>
</tr>
</thead>
</table>
| EAPOL-start attack      | • **Attack.** Multiple EAPOL start frames (5 or more) are sent to the wireless access point to initiate the RADIUS authentication process for clients.  
• **Result.** Wireless service is disrupted.  
• **Solution.** The wireless access point determines if the legitimate clients have already been authenticated before processing EAPOL start frames. |             | 5         | Trap         |
| EAPOL-logoff attack     | • **Attack.** Several EAPOL logoff frames (2 or more) that use the spoofed MAC address of a legitimate client are sent to the wireless access point to terminate a RADIUS-authenticated session.  
• **Result.** The client is disconnected from the wireless access point.  
• **Solution.** The wireless access point determines if it still receives traffic from the client before disconnecting the client. |             | 2         | Trap         |
| Premature EAP failure attack | • **Attack.** Several premature EAP failure frames (2 or more) are sent to a legitimate client to suggest RADIUS authentication failure.  
• **Result.** The client cannot be authenticated and cannot connect to the wireless access point.  
**Note:** The IDS detects this attack, but the IPS does not take action against this attack. |             | 2         | Trap         |
| Premature EAP success attack | • **Attack.** Several premature EAP success frames (2 or more) are sent to a legitimate client to suggest RADIUS authentication success.  
• **Result.** The client cannot be authenticated and cannot connect to the wireless access point.  
**Note:** The IDS detects this attack, but the IPS does not take action against this attack. |             | 2         | Trap         |
| CTS flood               | • **Attack.** Multiple clear-to-send (CTS) frames (60 or more) are sent to the wireless access point.  
• **Result.** Wireless service is disrupted.  
• **Solution.** The wireless access point sends a channel change frame to the legitimate clients and uses automatic channel selection to switch to a new clear channel. |             | 60        | Trap         |
| RTS flood               | • **Attack.** Multiple request-to-send (RTS) frames (60 or more) are sent to the wireless access point.  
• **Result.** Wireless service is disrupted.  
• **Solution.** The wireless access point sends a channel change frame to the legitimate clients and uses automatic channel selection to switch to a new clear channel. |             | 60        | Trap         |
### Table 24. IDS/IPS policies and policy rules (continued)

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Policy Rule</th>
<th>Threshold</th>
<th>Notification</th>
</tr>
</thead>
</table>
| RF jamming attack | Attack. Multiple RF transmissions (100 or more) are sent to the wireless access point, jamming the radio frequency.  
Result. Wireless service is disrupted.  
**Note:** The IDS detects this attack, but the IPS does not take action against this attack. | 100 | Trap |
| Virtual carrier attack | Attack. Multiple frames (60 or more) with a large duration value are sent to the wireless access point.  
Result. Wireless service is disrupted.  
**Solution:** The wireless access point sends a channel change frame to the legitimate clients and uses automatic channel selection to switch to a new clear channel. | 60 | Trap |
| MAC spoofing | Attack. Several frames (3 or more) that contain the spoofed MAC address of the wireless access point itself or the spoofed MAC address of a legitimate client are sent to the wireless access point.  
Result. Wireless security might be compromised.  
**Note:** The IDS detects MAC spoofing, but the IPS does not take action against MAC spoofing. | 3 | Trap |
| Rogue AP detection | Detection. A wireless access point is not in the managed AP list (see View and Save Access Point Lists on page 87) and is not connected to the secured wireless or wired network.  
Result. Wireless security might be compromised.  
**Note:** The IDS detects rogue APs, but the IPS does not take action against rogue APs. For information about how to exclude rogue APs from your network, see Enable Rogue AP Detection and Monitor Access Points on page 85. | 0 | Trap |
| Ad-hoc network detected | Detection. A group of wireless access points are part of an ad hoc network that might broadcast the same SSID as the secured wireless network.  
Result. Wireless security might be compromised.  
**Note:** The IDS detects ad hoc networks, but the IPS does not take action against ad hoc networks. | 0 | Trap |
| Ad-hoc network with wired connectivity | Detection. A group of wireless access points are part of an ad hoc network that has a wired connection and that might broadcast the same SSID as the secured wireless network.  
Result. Wireless security might be compromised.  
**Note:** The IDS detects ad hoc networks, but the IPS does not take action against ad hoc networks. | 0 | Trap |
Table 24. IDS/IPS policies and policy rules (continued)

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

To remove the detected changes from the table:
1. Select the check box to the left of the wireless access point for which you want to remove the changes from the table.
2. Above the table, click **Delete**.
To enable and configure the IDS/IPS:

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

2. Select the **Enable** radio button. By default, the IDS/IPS is disabled.

3. Specify the detection policy by making a selection from the IDS/IPS Detection Policy drop-down list:
   - **Mild**. The wireless access point scans for attacks every 10 seconds.
   - **Moderate**. The wireless access point scans for attacks every 5 seconds. This is the default setting.
   - **Aggressive**. The wireless access point scans for attacks every second.

4. Optional: Click a policy name to display the policy rules that are stated next to the policy in the table. IDS/IPS policy rules are not configurable.

5. Optional: Clear check boxes for policies that you want to disable. By default, the check box next to Select Policy in the table heading is selected, and all IDS/IPS policies are enabled.

6. Click **Apply** to save your settings.
Configure Wireless Intrusion Detection and Prevention Mail Settings

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

➢ **To configure IDS/IPS email settings:**

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

![IDS/IPS Mail Settings Screen](image)

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

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

3. Click **Apply** to save your settings.
Monitor Traps, Counters, and Ad Hoc Networks

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

Most Recent Attacks

➢ To display the last 50 attacks against the wireless access point and its clients:
Select Monitoring > IPS/IDS > Traps. The Traps screen displays.

![Traps Screen](image)

Figure 56.

To update the information onscreen, click Refresh.

The following table explains the fields of the Traps screen:

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

Attack Counter

➢ To display the number of occurrences per attacks:
Select Monitoring > IPS/IDS > Counters. The Counters screen displays.
To update the information onscreen, click Refresh.

**Ad Hoc Networks**

To display the ad hoc networks and their associated clients:
Select Monitoring > IPS/IDS > Adhoc Networks. The Adhoc Network screen displays.
To update the information onscreen, click **Refresh**.

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

**Table 27. Ad hoc network fields**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC Address</td>
<td>The MAC address of the client that is connected to the ad hoc network.</td>
</tr>
<tr>
<td>BSSID</td>
<td>The BSSID of the ad hoc network.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>A wireless access point that is connected to a wired network and a set of wireless stations is called a basic service set (BSS). The basic service set identifier (BSSID) differentiates one WLAN from another.</td>
</tr>
<tr>
<td>Wired Connectivity</td>
<td>If the ad hoc network has wired connectivity, the field displays YES. If the ad hoc network does not have wired connectivity, the field displays NO.</td>
</tr>
</tbody>
</table>
This chapter describes how to configure the advanced features of the wireless access point. The chapter includes the following sections:

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

**Configure IPv6 Settings and Optional DHCPv6 Server Settings**

The wireless access point supports IPv6:

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

**Configure the IPv6 Settings**

---

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

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

WARNING:

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

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

➢ To configure the IPv6 settings:

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

![IPv6 Settings](image)

Figure 59.

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

Table 28. IPv6 settings

<table>
<thead>
<tr>
<th>Setting</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 DHCPv6 server on your LAN and you select the Enable radio button, the wireless access point receives its dynamic IPv6 address, prefix length, and default gateway settings automatically from the DHCPv6 server on your network when you connect the wireless access point to your LAN.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>Enter the IP address of your wireless access point. The default IP address is 2001::21c:c0ff:fe69. To change the address, enter an unused IPv6 address from the address range used on your LAN.</td>
</tr>
<tr>
<td>Prefix Length</td>
<td>Enter the prefix length for the IPv6 address. The default prefix length is 64.</td>
</tr>
</tbody>
</table>

Advanced Configuration

100
Configure the Optional DHCPv6 Server

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

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

To configure DHCPv6 server settings:

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>Enter the IPv6 address of the ISP gateway to which the wireless access point connects.</td>
</tr>
<tr>
<td>Dynamic IPv6 Address</td>
<td>The dynamic IPv6 address that is assigned by the DHCPv6 server on your network. This address does not overwrite the address in the IPv6 Address field.</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 need to obtain it from the ISP and enter it manually in this field.</td>
</tr>
<tr>
<td>Secondary DNS Server</td>
<td></td>
</tr>
<tr>
<td>Network Integrity Check</td>
<td>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.
Figure 60.

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

**Table 29. DHCP server settings for IPv6**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the DHCPv6 Server</td>
<td>Enable radio button to enable the DHCP server. Use the default settings or</td>
</tr>
<tr>
<td>State</td>
<td>specify the pool of IPv6 addresses to be assigned by setting the starting IPv6 address and ending IPv6 address. These addresses should be part of the same IP address subnet as the wireless access point’s LAN IPv6 address.</td>
</tr>
<tr>
<td>Stateless</td>
<td>The IPv6 clients in the LAN generate their own IP address by using a combination of locally available information and router advertisements, but receive DNS server information from the DHCPv6 server.</td>
</tr>
<tr>
<td>Stateful</td>
<td>The IPv6 clients in the LAN obtain an interface IP address, configuration information such as DNS server information, and other parameters from the DHCPv6 server. The IP address is a dynamic address.</td>
</tr>
<tr>
<td>DHCP Server VLAN ID</td>
<td>Enter the VLAN ID for the DHCP server. The VLAN ID range is from 1 to 4094.</td>
</tr>
<tr>
<td>Starting IPv6 Address</td>
<td>Enter the first address in the range of IPv6 addresses to be assigned to DHCP clients. The default address is 2001:05c0:9168::10.</td>
</tr>
<tr>
<td>Ending IPv6 Address</td>
<td>Enter the last address in the range of IPv6 addresses to be assigned to DHCP clients. The default address is 2001:05c0:9168::50.</td>
</tr>
</tbody>
</table>
Configure Spanning Tree Protocol, 802.1Q VLAN, and Link Layer Discovery Protocol

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

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

Configure STP and VLANs

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

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

- **Untagged VLAN.** When the wireless access point sends frames that are associated with the untagged VLAN from its Ethernet interface, those frames are untagged. When the wireless access point receives untagged frames over its Ethernet interface, those frames are assigned to the untagged VLAN.
**Note:** Select the **Untagged VLAN** check box only if the hubs and switches on your LAN support the 802.1Q VLAN protocol. Likewise, change the untagged VLAN value only if the hubs and switches on your LAN support the 802.1Q VLAN protocol.

- **Tagged VLAN.** When you clear the Untagged VLAN check box, the wireless access point tags all frames that are sent from its Ethernet interface. Only incoming frames that are tagged with known VLAN IDs are accepted.

- **Management VLAN.** The management VLAN can be active only when the wireless access point functions as a point-to-point or point-to-multipoint bridge (see *Configure Wireless Bridging* on page 118). The management VLAN is used for managing traffic (Telnet, SNMP, and HTTP) to and from the wireless access point.

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

➢ **To configure STP and VLANs:**

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

   ![Screen shot of General settings](image)

   Figure 61.
2. Specify the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1Q VLAN</td>
<td></td>
</tr>
<tr>
<td>Untagged VLAN</td>
<td>Select the Untagged VLAN check box to configure one VLAN as an untagged VLAN. By default, the Untagged VLAN check box is selected. Specify a VLAN ID. The default VLAN ID is 1.</td>
</tr>
<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. Note: If you configure the management VLAN ID as 0 (zero), the wireless access point can be managed over any VLAN, and frames that belong to the management VLAN are not tagged with an 802.1Q header when sent over the trunk.</td>
</tr>
</tbody>
</table>

**WARNING:**

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

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

**Configure Ethernet LLDP**

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

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

➢ To turn off LLDP:

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

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

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

To set up a hotspot server:

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

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

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

4. Click **Apply** to save your settings. All HTTP requests are now redirected to the specified URL.

**Configure Advanced Wireless Settings**

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

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

➢ **To configure advanced wireless settings:**

1. Select **Configuration > Wireless > Advanced > Wireless Settings**. The advanced Wireless Settings screen displays. The following figure shows the 11ng settings, as indicated by the radio wave icon ( sóng ) that is displayed next to ng:
2. Optional: To configure advanced wireless settings for the 802.11a/na modes, click the 802.11a/na tab.

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

Table 31. Advanced wireless settings

<table>
<thead>
<tr>
<th>Setting</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 needs to be an even number. The default setting is 2346.</td>
</tr>
<tr>
<td>Setting</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</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 (A-MPDU) packets. Larger aggregation lengths could lead to better network performance. Aggregation is a mechanism used to achieve higher throughput. The default setting is 65535.</td>
</tr>
<tr>
<td><strong>Note:</strong> This setting does not apply to the 802.11a mode.</td>
<td></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 the aggregated MAC protocol data unit (A-MPDU) could lead to better network performance. By default, the Enable radio button is selected.</td>
</tr>
<tr>
<td><strong>Note:</strong> This setting does not apply to the 802.11b/bg modes and the 802.11a mode.</td>
<td></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><strong>Note:</strong> This setting does not apply to the 802.11b/bg modes and the 802.11a mode.</td>
<td></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 needs to be between 1 and 255. The default setting is 3.</td>
</tr>
<tr>
<td>Preamble Type</td>
<td>Select one of the following radio buttons to specify the preamble type:</td>
</tr>
<tr>
<td><strong>Note:</strong> This setting does not apply to the 802.11a/na modes.</td>
<td>• <strong>Long.</strong> A long transmit preamble might provide a more reliable connection or a slightly longer range. A short transmit preamble gives better performance.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Auto.</strong> The Auto setting enables the wireless access point to handle both long and short preambles. The default setting is Auto.</td>
</tr>
<tr>
<td>Antenna</td>
<td>Select one of the following radio buttons to specify the antenna:</td>
</tr>
<tr>
<td><strong>Note:</strong> This setting does not apply to the 802.11a/na modes.</td>
<td>• <strong>Internal.</strong> Enables the internal antenna. This is the default setting.</td>
</tr>
<tr>
<td></td>
<td>• <strong>External.</strong> Enables an optional external antenna or antennas.</td>
</tr>
<tr>
<td>802.11d</td>
<td>Select this check box to enable support for additional regulatory domains that are not in the current standard; support includes the addition of a country information element to beacons, probe requests, and probe responses. This check box is selected by default.</td>
</tr>
<tr>
<td><strong>Note:</strong> This setting does not apply to the 802.11a/na modes.</td>
<td></td>
</tr>
<tr>
<td>Client Isolation</td>
<td>From the drop-down list, select one of the following options:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Enable.</strong> Communication between wireless clients that are associated to different virtual access points (VAPs) is blocked.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Disable.</strong> Communication between wireless clients that are associated to different VAPs is allowed. This is the default setting.</td>
</tr>
<tr>
<td>Max. Wireless Clients</td>
<td>Enter the maximum number of wireless clients that can simultaneously connect to the wireless access point at one time. The default setting is 128 clients.</td>
</tr>
</tbody>
</table>
Configure Advanced Quality of Service Settings

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

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

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

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

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

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

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

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

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

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

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

➢ To configure advanced QoS:

1. Select Configuration > Wireless > Advanced > QoS Settings. The advanced QoS Settings screen displays:
2. Optional: To configure advanced QoS for the 802.11a/na modes, click the 802.11a/na tab.
3. Specify the settings as explained in the following table:

### Table 32. EDCA settings

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AP EDCA parameters</strong></td>
<td></td>
</tr>
<tr>
<td>AIFS</td>
<td>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.</td>
</tr>
<tr>
<td>cwMin</td>
<td>Enter the minimum contention window (cwMin) value that specifies the upper limit (in milliseconds) of a range from which the initial random back-off wait time is determined. Decreasing this value increases the priority of the queue. The value for cwMin needs to be lower than the value for cwMax. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. The default values are Data 0: 15; Data 1: 15; Data 2: 7; Data 3: 3.</td>
</tr>
<tr>
<td>cwMax</td>
<td>Enter the maximum contention window (cwMax) value that specifies the upper limit (in milliseconds) for the doubling of the random back-off value. Decreasing this value increases the priority of the queue. The value for cwMax needs to be higher than the value for cwMin. Valid values are 0, 1, 3, 7, 15, 31, 63, 127, 255, 511, and 1023. The default values are Data 0: 63; Data 1: 1023; Data 2: 15; Data 3: 7.</td>
</tr>
</tbody>
</table>
Configure Quality of Service Policies

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

- IP precedence. Indicates the IP Type of Service (ToS) or precedence in the IP headers.
- IP DSCP. Indicates the Differentiated Services Code Point (DSCP) marking in the IP header.
- IP protocol 119. Indicates the IP protocol field in the IP header with value 119.
- 802.1P. Indicates the 3-bit Class of Service (CoS) field in the class header.
- IP protocol. Indicates the protocol field in the IP header.
- EtherType. Indicates the EtherType field in Ethernet-II frame header.
- Source MAC. Indicates the source MAC address in Ethernet-II frame header.
- Destination MAC. Indicates the destination MAC address in Ethernet-II frame header.
- Source IP. Indicates the source IP address in the IP header.
- Destination IP. Indicates the destination IP address in the IP header.
- Source port. Indicates the source port number in the port header.
- Destination port. Indicates the destination port number in the port header.

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

You can configure up to eight QoS policies.

➢ To configure a new QoS policy:


![QoS Policies Screen](image)

2. Optional: To configure the QoS Policies screen for the 802.11a/na modes, click the 802.11a/na tab.

3. From the Create Policy drop-down list, select NEW. If you have not created any QoS policies, NEW is the only selection possible.

4. In the Policy Name field, enter a name for the new QoS policy.

5. Specify a classification for the QoS policy as explained in the following table.
**Note:** Depending on your selection from the Match Frame Fields drop-down list, Match Classifications appears either as a drop-down list from which you need to make a selection or a field in which you need to enter information.

### Table 33. QoS classification settings

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Match Frame Fields and Match Classifications (continued)** | **802.1P** | From the Match Classifications drop-down list, select the CoS priority value against which the information in the IP header needs to be matched:  
- Routine(0)  
- Priority(1)  
- Immediate(2)  
- Flash(3)  
- Flash Override(4)  
- Critic/CCP(5)  
- Inter Control(6)  
- Network Control(7) |
| **IP Protocol** | In the Match Classifications field, enter the IP protocol value against which the information in the IP header needs to be matched. A list of protocol values is available at [http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml](http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xml) |
| **Ether Type** | In the Match Classifications field, enter the Ether type value against which the information in the IP header needs to be matched. A list of Ether type values is available at [http://standards.ieee.org/develop/regauth/ethertype/eth.txt](http://standards.ieee.org/develop/regauth/ethertype/eth.txt) |
| **Source MAC** | In the Match Classifications field, select or enter the source MAC address against which the information in the IP header needs to be matched.  
To select the MAC address of a wireless client that is connected to the wireless access point:  
1. Select the radio button to the left of the Match Classifications drop-down list.  
2. From the drop-down list, select a MAC address.  
To enter a MAC address:  
1. Select the radio button to the right of the Match Classifications drop-down list.  
2. In the field to the right of the radio button, enter a MAC address. |
| **Destination MAC** | In the Match Classifications field, select or enter the destination MAC address against which the information in the IP header needs to be matched.  
To select the MAC address of a wireless client that is connected to the wireless access point:  
1. Select the radio button to the left of the Match Classifications drop-down list.  
2. From the drop-down list, select a MAC address.  
To enter a MAC address:  
1. Select the radio button to the right of the Match Classifications drop-down list.  
2. In the field to the right of the radio button, enter a MAC address. |
Table 33. QoS classification settings (continued)

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

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

Table 34. Classification rate limiting settings

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

7. Click Add to add the classification to the Classifications field.
8. To add another classification to the QoS policy, repeat Step 5, Step 6, and Step 7.
9. Click Apply to save your settings. The QoS policy is saved.
Note: Rate limiting for the wireless interface is an optional setting that applies to all traffic on the wireless interface. Unlike classification rate limiting, which you can specify for each classification, rate limiting for the wireless interface needs to be specified only once.

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

Table 35. Wireless interface rate limiting settings

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

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

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

➢ To delete a QoS policy:
  1. From the Create Policy drop-down list, select the policy that you want to delete.
  2. Click **Delete Policy**.
  3. Click **Apply** to save your settings.
Configure Wireless Bridging

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

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

- **Wireless point-to-point bridge.** In this mode, the wireless access point can communicate with another bridge-mode wireless station and, as an option, also with wireless clients. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see Configure a Point-to-Point Wireless Network on page 118.

- **Wireless point-to-multipoint bridge.** In this mode, the wireless access point is the master for a group of bridge-mode wireless stations. As an option, the wireless access point can also communicate with wireless clients. You can configure up to four profiles. The other bridge-mode wireless stations need to be set to point-to-point bridge mode, using the MAC address of the master wireless access point. Rather than communicating directly with each other, all other bridge-mode wireless stations send their traffic to the master wireless access point. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see Configure a Point-to-Multipoint Wireless Network on page 122.

- **Repeating the wireless signal.** In this mode, this wireless access point repeats the wireless signal, does not support communication with wireless clients, and sends all traffic to a remote access point. In this mode, wireless clients cannot associate with the wireless access point. Use WEP, WPA-PSK, or WPA2-PSK to secure the communication. For information about how to configure this mode, see Configure the Wireless Access Point to Repeat the Wireless Signal Using Point-to-Multipoint Bridge Mode on page 126.

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

Configure a Point-to-Point Wireless Network

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

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

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.

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

![Edit Security Profile](image)

**Figure 69.**

Specify the settings as explained in the following table:

<table>
<thead>
<tr>
<th>Setting</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 Figure 67 on page 119).</td>
</tr>
<tr>
<td><strong>Authentication Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Network Authentication and Data Encryption</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 the WPA Passphrase (Network Key) field displays.</td>
</tr>
</tbody>
</table>
h. Click **Apply** to save your security profile settings. The Bridging screen displays again.

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

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

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

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

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

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

---

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

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Authentication and Data Encryption (continued)</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 bit encryption. This mode functions only with other wireless stations that support this mode.</td>
</tr>
<tr>
<td>WPA-PSK</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 needs to be between 8 and 63 characters (inclusive).</td>
</tr>
<tr>
<td>WPA2-PSK</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 needs to be between 8 and 63 characters (inclusive).</td>
</tr>
</tbody>
</table>

**Note:** NETGEAR recommends WPA2-PSK authentication with AES encryption if you want to use the 11n rates and speed.
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:

![Diagram showing network configurations](image)

**Figure 70.**

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

1. Configure the security profiles on the wireless access point (AP1 on LAN Segment 1 in the previous figure):

   a. Select **Configuration > Wireless Bridge**. The Bridging screen displays. (The following figure shows the screen after you have completed *Step d.*)
b. Optional: To display the Bridging screen for the 802.11a/na modes, click the 802.11a/na tab.

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

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

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

f. Click Edit to configure the selected security profile settings. The Edit Security Profile screen displays for the selected security profile. (The following figure contains an example.)
g. Specify the settings as explained in the following table:

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

<table>
<thead>
<tr>
<th>Setting</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 security profiles are NETGEAR-WDS-1, NETGEAR-WDS-2, NETGEAR-WDS-3, and NETGEAR-WDS-4.</td>
</tr>
<tr>
<td>Remote MAC Address</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 70 on page 122).</td>
</tr>
<tr>
<td><strong>Authentication Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Network Authentication and Data Encryption</td>
<td>From the Network Authentication drop-down list, select Open System, WPA-PSK, or WPA2-PSK. Your selection determines the options that the Data Encryption drop-down list provides, and whether the WPA Passphrase (Network Key) field displays.</td>
</tr>
<tr>
<td>Open System</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>• None. No authentication and encryption.</td>
</tr>
<tr>
<td></td>
<td>• 64-bit WEP. Standard WEP encryption, using 40/64-bit encryption.</td>
</tr>
<tr>
<td></td>
<td>• 128-bit WEP. Standard WEP encryption, using 104/128-bit encryption.</td>
</tr>
<tr>
<td></td>
<td>• 152-bit WEP. Proprietary WEP encryption mode, using 128+24 bit encryption. This mode functions only with other wireless stations that support this mode.</td>
</tr>
<tr>
<td>WPA-PSK</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 needs to be between 8 and 63 characters (inclusive).</td>
</tr>
<tr>
<td>WPA2-PSK</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 needs to be between 8 and 63 characters (inclusive).</td>
</tr>
</tbody>
</table>

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

i. Repeat Step c through Step h for any other security profile that you want to edit.
For example, first configure security profile NETGEAR-WDS-1 with the MAC address of AP2, and then configure security profile NETGEAR-WDS-2 with the MAC address of AP3 (see Figure 70 on page 122).

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

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

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

3. Configure AP2 on LAN Segment 2 (see Figure 70 on page 122) in point-to-point bridge mode with the remote MAC address of AP1.

4. Configure AP3 on LAN Segment 3 (see Figure 70 on page 122) in point-to-point bridge mode with the remote MAC address of AP1.

5. Verify the following for all wireless access points:
   - Only AP1 on LAN Segment 1 is configured in point-to-multipoint bridge mode, and all others APs are configured in point-to-point bridge mode.
   - AP2 and AP3 (the point-to-point APs) have AP1’s MAC address in their Remote MAC Address field.
   - All APs are on the same LAN, that is, the LAN IP addresses of all APs are in the same network as the LAN devices.
   - If you use DHCP, all wireless access points can obtain IP addresses automatically (as DHCP clients). For more information, see Configure the Optional DHCPv4 Server on page 27 or Configure the Optional DHCPv6 Server on page 101.
   - All wireless access points use the same channel, authentication mode, and security settings.

6. Verify connectivity across the LANs:

A computer on any LAN segment should be able to connect to the Internet or share files and printers with any other devices or servers connected to any of the three LAN segments.
Configure the Wireless Access Point to Repeat the Wireless Signal Using Point-to-Multipoint Bridge Mode

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

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

![Diagram showing multipoint bridging configuration]

Figure 73.
To configure the wireless access point to repeat the wireless signal:

1. Configure the security profiles on the wireless access point (AP2 in the previous figure):
   a. Select Configuration > Wireless Bridge. The Bridging screen displays (see the following figure).
   b. Optional: To display the Bridging screen for the 802.11a/na modes, click the 802.11a/na tab.
   c. Select the Enable Wireless Bridging check box. The Local MAC Address field is a nonconfigurable field that shows the MAC address of the wireless access point.
   d. Select the Wireless Point-to-Multi-Point Bridge radio button. The screen adjusts.

![Bridging Screen](image)

Figure 74.

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

f. Click Edit to configure the selected security profile settings. The Edit Security Profile screen displays for the selected security profile. (The following figure contains an example.)
Figure 75.

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

Table 38. Wireless signal repeating profile and authentication settings

<table>
<thead>
<tr>
<th>Setting</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 security profiles are NETGEAR-WDS-1, NETGEAR-WDS-2,</td>
</tr>
<tr>
<td></td>
<td>NETGEAR-WDS-3, and NETGEAR-WDS-4.</td>
</tr>
<tr>
<td>Remote MAC Address</td>
<td>Enter the MAC address of the remote wireless access point (the MAC address of AP1 or AP3 in <em>Figure 73</em> on page 126).</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>, <strong>WPA-PSK</strong>, or <strong>WPA2-PSK</strong>. Your selection determines the</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>options that the Data Encryption drop-down list provides, and whether the WPA Passphrase (Network Key) field displays.</td>
</tr>
<tr>
<td>Open System</td>
<td>Although you can use the bridge communication without any authentication and encryption, NETGEAR recommends that you use WEP if you</td>
</tr>
<tr>
<td></td>
<td>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 bit encryption. This mode functions only with other wireless stations</td>
</tr>
<tr>
<td></td>
<td>that support this mode.</td>
</tr>
</tbody>
</table>
Advanced Configuration

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

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

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

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

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

2. Activate repeater mode on the wireless access point (AP2 in *Figure 73* on page 126):
   a. On the Bridging screen, select the **Enable Wireless Bridging** check box.
   b. Select the **Wireless Point-to-Multi-Point Bridge** radio button.
   c. Clear the **Enable Wireless Client Association** check box to disable wireless client association (see the red circle in *Figure 74* on page 127).

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

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

3. Configure AP1 on LAN Segment 1 (see *Figure 73* on page 126) in repeater mode with the remote MAC address of AP2.
4. Configure AP3 on LAN Segment 3 (see *Figure 73* on page 126) in repeater mode with the remote MAC address of AP2.
5. Verify the following for all wireless access points:
   • All APs are on the same LAN, that is, the LAN IP addresses of all APs are in the same network as the LAN devices.
   • If you use DHCP, all wireless access points can obtain IP addresses automatically (as DHCP clients). For more information, see Configure the Optional DHCPv4 Server on page 27 or Configure the Optional DHCPv6 Server on page 101.
   • All wireless access points use the same channel, authentication mode, and security settings.

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

   **Note:** You can extend repetition of the wireless signal by adding up to two more wireless access points that are configured in point-to-multipoint bridge mode without client association. Also, you can extend the range of the wireless network with NETGEAR wireless antenna accessories.
This chapter provides information about troubleshooting the wireless access point. After each problem description, instructions are given to help you diagnose and solve the problem. For the common problems listed, go to the section indicated.

- Is the wireless access point on?
  Go to *Basic Functioning* on page 132.

- Have I connected the wireless access point correctly?
  Go to *Basic Functioning* on page 132.

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

- I cannot access the wireless access point from a browser.
  Go to *You Cannot Configure the Wireless Access Point from a Browser* on page 134.

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

- I have problems with the LAN connection.
  Go to *Troubleshoot a TCP/IP Network Using the Ping Utility* on page 135.

- I cannot remember the wireless access point’s configuration password.
  Go to *Change the Administrator Password* on page 74.

- I want to clear the configuration and start over again.
  Go to *Restore the Wireless Access Point to the Factory Default Settings* on page 71.

- The date or time is not correct.
  Go to *Problems with Date and Time* on page 137.

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

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

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

Verify the Correct Sequence of Events at Startup

- After you turn on power to the wireless access point, check that the following sequence of events occurs:
  - The Power/Test LED is first steady amber, then goes off, and then blinks green before turning steady green after about 45 seconds.
  - The Active LED is lit or blinks green when there is Ethernet traffic.
  - The LAN LED indicates the LAN speed: green for 1000 Mbps, amber for 100 Mbps, and no light for 10 Mbps.
  - The WLAN LED is lit or blinks green when the wireless LAN (WLAN) is ready.

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

No LEDs Are Lit on the Wireless Access Point

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

- If you use a PoE switch to provide power to the wireless access point, check these items:
  - Make sure that the Ethernet cable between the wireless access point and the PoE switch is correctly connected at both ends.
  - Make sure that the power cord of the PoE switch is plugged into a working power outlet or power strip.
  - Make sure that your PoE switch is functioning normally.
If you use a power cord to provide power to the wireless access point, check these items:

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

The Active LED or the LAN LED Is Not Lit

There is a hardware connection problem.

Check these items:

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

The WLAN LED Does Not Light Up

The wireless access point’s antenna is not working.

Check these items:

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

Contact NETGEAR technical support if the WLAN LED remains off.
You Cannot Access the Internet or the LAN from a Wireless-Capable Computer

There is a configuration problem.

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

You Cannot Configure the Wireless Access Point from a Browser

- **Check these items:**
  - The wireless access point is correctly installed, it is powered on, and LAN connections are okay. Check that the Active LED and LAN LED are on to verify that the Ethernet connection is okay.
  - If your computer uses a fixed (static) IP address, ensure that it is using an IP address in the range of the wireless access point. The wireless access point’s default IP address is 192.168.0.100, and its subnet mask is 255.255.255.0 with DHCP disabled. Make sure that your network configuration settings are correct.
  - If you are using the NetBIOS name of the wireless access point to connect, ensure that your computer and the wireless access point are on the same network segment or that there is a WINS server on your network.
  - If your computer is set to obtain an IP address automatically (DHCP client), restart it.
• Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
• Try quitting the browser, clearing the cache, deleting the cookies, and launching the browser again.
• Make sure that you are using the correct login information. The factory default login name is `admin`, and the password is `password`. Make sure that Caps Lock is off when entering this information.

➢ If the wireless access point does not save changes you have made in the web management interface, check the following:
  • When entering configuration settings, be sure to click the **Apply** button before moving to another screen or tab, or your changes are lost.
  • Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the web browser might be caching the old configuration.

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

A number of things could be causing this.

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

### Troubleshoot a TCP/IP Network Using the Ping Utility

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

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

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

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

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

   ping 192.168.0.100

3. Click OK.

   You should see a message like this one:

   Pinging <IP address> with 32 bytes of data

   If the path is working, you see this message:

   Reply from < IP address >: bytes=32 time=NN ms TTL=xxx

   If the path is not working, you see this message:

   Request timed out

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

   • Wrong physical connections:

     - Make sure that the Active LED and LAN LED are on. If one or both of these LEDs are off, follow the instructions in The Active LED or the LAN LED Is Not Lit on page 133.

     - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and wireless access point.

   • Wrong network configuration:

     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer.

     - Verify that the IP address for your wireless access point and your workstation are correct and that the addresses are on the same subnet.
Test the Path from Your Computer to a Remote Device

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

1. From the Windows toolbar, click the Start button, and select Run.
2. In the Windows Run window, type:
   \[ \text{ping } -n \text{ 10 } \text{<IP address>} \]
   where \(<\text{IP address}>\) is the IP address of a remote device such as the DNS server of your ISP.

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

- Check that your computer has the IP address of your router listed as the default wireless access point. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer’s Network Control Panel. Verify that the IP address of the router is listed as the default wireless access point.
- Check to see that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the basis General system settings screen (see Configure Basic General System Settings and Time Settings on page 23).

Problems with Date and Time

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

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

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

➢ To capture packets:

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

![Packet Capture Screen](image)

Figure 76.

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

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

3. Click Stop to stop capturing packets.

4. Click Save as to save the papture.pcap file on your computer or to a disk drive.
This appendix provides factory default settings and technical specifications for the ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620. The appendix includes the following sections:

- *Technical Specifications*
- *Factory Default Settings*

## Technical Specifications

### Table 39. Technical specifications

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11ng MCS index and data rates (continued)</td>
<td>Data rates for a 40 MHz channel width and a long guard interval (800 ms): 0 / 13.5 Mbps, 1 / 27 Mbps, 2 / 40.5 Mbps, 3 / 54 Mbps, 4 / 81 Mbps, 5 / 108 Mbps, 6 / 121.5 Mbps, 7 / 135 Mbps, 8 / 27 Mbps, 9 / 54 Mbps, 10 / 81 Mbps, 11 / 108 Mbps, 12 / 162 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, 16 / 40.5 Mbps, 17 / 81 Mbps, 18 / 121.5 Mbps, 19 / 162 Mbps, 20 / 243 Mbps, 21 / 324 Mbps, 22 / 364.5 Mbps, 23 / 405 Mbps, and auto-rate capable</td>
</tr>
</tbody>
</table>
| 802.11b/bg/ng operating frequencies | • 2.412–2.462 GHz (US)  
  • 2.457–2.462 GHz (Spain)  
  • 2.410–2.484 GHz (Japan 11b)  
  • 2.410–2.472 GHz (Japan 11ng)  
  • 2.457–2.472 GHz (France)  
  • 2.412–2.472 GHz (Europe ETSI)  
  • 2.412–2.472 GHz (China) |
| 802.11 b/bg/ng encryption | • 64-bit, 128-bit, and 52-bit WEP  
  • AES  
  • TKIP |

802.11a/na wireless specifications

| 802.11a data rates | 6, 9, 12, 18, 24, 36, 48, 54 Mbps, and auto-rate capable |
| 802.11na data rates | Data rates for a 20 MHz channel width and an automatic guard interval: 0 / 7.2 Mbps, 1 / 14.4 Mbps, 2 / 21.7 Mbps, 3 / 28.9 Mbps, 4 / 43.3 Mbps, 5 / 57.8 Mbps, 6 / 65 Mbps, 7 / 72.2 Mbps, 8 / 14.44 Mbps, 9 / 28.88 Mbps, 10 / 43.33 Mbps, 11 / 57.77 Mbps, 12 / 86.66 Mbps, 13 / 115.56 Mbps, 14 / 144.44 Mbps, 15 / 21.7 Mbps, 16 / 43.3 Mbps, 17 / 65 Mbps, 19 / 86.7 Mbps, 20 / 130.7 Mbps, 21 / 173.3 Mbps, 22 / 195 Mbps, 23 / 216.7 Mbps, and auto-rate capable |
| 802.11a data rates | Data rates for a 20 MHz channel width and a long guard interval (800 ms): 0 / 6.5 Mbps, 1 / 13 Mbps, 2 / 19.5 Mbps, 3 / 26 Mbps, 4 / 39 Mbps, 5 / 52 Mbps, 6 / 58.5 Mbps, 7 / 65 Mbps, 8 / 13 Mbps, 9 / 26 Mbps, 10 / 39 Mbps, 11 / 52 Mbps, 12 / 78 Mbps, 13 / 104 Mbps, 14 / 117 Mbps, 15 / 130 Mbps, 16 / 19.5 Mbps, 17 / 39 Mbps, 18 / 58.5 Mbps, 19 / 78 Mbps, 20 / 117 Mbps, 21 / 156 Mbps, 22 / 175.5 Mbps, 23 / 195 Mbps, and auto-rate capable |
| 802.11na data rates | Data rates for a 40 MHz channel width and an automatic guard interval: 0 / 15 Mbps, 1 / 30 Mbps, 2 / 45 Mbps, 3 / 60 Mbps, 4 / 90 Mbps, 5 / 120 Mbps, 6 / 135 Mbps, 7 / 150 Mbps, 8 / 30 Mbps, 9 / 60 Mbps, 10 / 90 Mbps, 11 / 120 Mbps, 12 / 180 Mbps, 13 / 240 Mbps, 14 / 270 Mbps, 15 / 300 Mbps, 16 / 45 Mbps, 17 / 90 Mbps, 18 / 135 Mbps, 19 / 180 Mbps, 20 / 270 Mbps, 21 / 360 Mbps, 22 / 405 Mbps, 23 / 450 Mbps, and auto-rate capable |
| 802.11na data rates | Data rates for a 40 MHz channel width and a long guard interval (800 ms): 0 / 13.5 Mbps, 1 / 27 Mbps, 2 / 40.5 Mbps, 3 / 54 Mbps, 4 / 81 Mbps, 5 / 108 Mbps, 6 / 121.5 Mbps, 7 / 135 Mbps, 8 / 27 Mbps, 9 / 54 Mbps, 10 / 81 Mbps, 11 / 108 Mbps, 12 / 162 Mbps, 13 / 216 Mbps, 14 / 243 Mbps, 15 / 270 Mbps, 16 / 40.5 Mbps, 17 / 81 Mbps, 18 / 121.5 Mbps, 19 / 162 Mbps, 20 / 243 Mbps, 21 / 324 Mbps, 22 / 364.5 Mbps, 23 / 405 Mbps, and auto-rate capable |
### Table 39. Technical specifications (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| 802.11a/na operating frequencies | • 5.180–5.240 GHz (US, lower frequencies)  
• 5.260–5.320 GHz (US, middle frequencies)  
• 5.180–5240 GHz (CE [EU], lower frequencies)  
• 5.260–5.320 GHz (CE [EU], middle frequencies)  
• 5.500–5.680 GHz (CE [EU], upper frequencies) |
| 802.11 a/na encryption       | • 64-bit, 128-bit, and 52-bit WEP  
• AES  
• TKIP |

#### Management and Other Specifications

- **Network management**  
  • Remote configuration and management through the web management interface, through SNMP, or through Telnet or SSH with the command-line interface (CLI).  
  • SNMP management supports SNMP MIB I, MIB II, 802.11 MIB and proprietary configuration MIB.

- **Maximum clients**  
  Limited by the amount of wireless network traffic generated by each node; a maximum of 128 clients is supported.

- **Status LEDs**  
  • Power/Test LED  
  • Link speed LED  
  • Ethernet LAN  
  • Wireless LAN (2.4 GHz and 5 GHz)

#### Electrical and Physical Specifications

- **Power adapter**  
  12 VDC, 1A; plug is localized to country of sale

- **Physical specifications**  
  • Dimensions (h x w x d): 253.75 x 253.75 x 54.76 mm (10.0 x 10.0 x 2.16 in.)  
  • Weight: 1.5 kg (3.31 lb)

- **Environmental specifications**  
  Operating temperature: 0 to 55°C (32 to 131°F)  
  Operating humidity: 10–9%, noncondensing

#### Compliance


- **Electromagnetic compliance**  
  • FCC Part 15 SubPart B  
  • FCC Part 15 SubPart C  
  • FCC Part 15 SubPart E  
  • CE  
  • C-TICK
Factory Default Settings

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

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

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

### Table 40. Default configuration settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Login for management and configuration</strong></td>
<td></td>
</tr>
<tr>
<td>LAN IPv4 management address</td>
<td>192.168.0.100</td>
</tr>
<tr>
<td>Subnet mask for IPv4 management address</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>LAN IPv6 management address</td>
<td>2001::21c:c0ff:fe69</td>
</tr>
<tr>
<td>Prefix length for IPv6 management address</td>
<td>64</td>
</tr>
<tr>
<td>Required static IPv4 address for management computer</td>
<td>192.168.0.210 and 255.255.255.0</td>
</tr>
<tr>
<td>User name (case-sensitive) for login</td>
<td>admin</td>
</tr>
<tr>
<td>Login password (case-sensitive) for login</td>
<td>password</td>
</tr>
<tr>
<td><strong>LAN and management features</strong></td>
<td></td>
</tr>
<tr>
<td>DHCPv4 client</td>
<td>Disabled</td>
</tr>
<tr>
<td>DHCPv6 client</td>
<td>Disabled</td>
</tr>
<tr>
<td>Untagged VLAN</td>
<td>Enabled, VLAN ID 1</td>
</tr>
<tr>
<td>Management VLAN</td>
<td>VLAN ID 1</td>
</tr>
<tr>
<td>SNMP</td>
<td>Disabled</td>
</tr>
<tr>
<td>Syslog</td>
<td>Disabled</td>
</tr>
<tr>
<td>Spanning Tree Protocol (STP)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Link Layer Discovery Protocol (LLDP)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Secure Shell (SSH)</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Table 40. Default configuration settings (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hotspot</td>
<td>Disabled</td>
</tr>
<tr>
<td>Secure Telnet</td>
<td>Disabled</td>
</tr>
<tr>
<td>Time zone</td>
<td>USA-Pacific</td>
</tr>
<tr>
<td>NTP client</td>
<td>Enabled</td>
</tr>
<tr>
<td>Custom NTP server</td>
<td>Disabled</td>
</tr>
<tr>
<td>Port speed</td>
<td>10/100/1000</td>
</tr>
<tr>
<td>Ethernet MAC address</td>
<td>See bottom label</td>
</tr>
</tbody>
</table>

DHCP server

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4</td>
<td>DHCPv4 server</td>
</tr>
<tr>
<td>DHCPv4 server VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv4 server IP range start address</td>
<td>192.168.0.2</td>
</tr>
<tr>
<td>DHCPv4 server IP range start address</td>
<td>192.168.0.50</td>
</tr>
<tr>
<td>DHCPv4 server subnet mask</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>DHCPv4 server gateway IPv4 address</td>
<td>192.168.0.1</td>
</tr>
<tr>
<td>DHCPv4 server IP address lease for clients</td>
<td>1 day</td>
</tr>
<tr>
<td>IPv6</td>
<td>DHCPv6 server</td>
</tr>
<tr>
<td>DHCPv6 server state</td>
<td>Stateful</td>
</tr>
<tr>
<td>DHCPv6 server VLAN ID</td>
<td>1</td>
</tr>
<tr>
<td>DHCPv6 server IP range start address</td>
<td>2001:05c0:9168::10</td>
</tr>
<tr>
<td>DHCPv6 server IP range start address</td>
<td>2001:05c0:9168::50</td>
</tr>
<tr>
<td>DHCPv6 server prefix length</td>
<td>64</td>
</tr>
<tr>
<td>DHCPv6 server gateway IPv4 address</td>
<td>2001:05c0:9168::1</td>
</tr>
<tr>
<td>DHCPv6 server IP address lease for clients</td>
<td>1 day</td>
</tr>
</tbody>
</table>

Radio and wireless settings

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating mode</td>
<td>Access point, infrastructure mode</td>
</tr>
<tr>
<td>Wireless access point name</td>
<td>netgearxxxxxx, where xxxxxx are the last 6 digits of the wireless access point MAC address</td>
</tr>
<tr>
<td>Country and region</td>
<td>Varies by region</td>
</tr>
<tr>
<td>Wireless communication</td>
<td>2.4 GHz radio enabled</td>
</tr>
<tr>
<td></td>
<td>5 GHz radio disabled</td>
</tr>
</tbody>
</table>
Table 40. Default configuration settings (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless mode</td>
<td>11ng</td>
</tr>
<tr>
<td>Wireless network name (SSID)</td>
<td>NETGEAR_11ng</td>
</tr>
<tr>
<td>Broadcast network name SSID</td>
<td>Enabled</td>
</tr>
<tr>
<td>802.11ng radio frequency channel</td>
<td>Auto</td>
</tr>
<tr>
<td>MCS index/data rate (transmission speed)</td>
<td>Best</td>
</tr>
<tr>
<td>Note: Maximum wireless signal rate derived</td>
<td>Maximum wireless signal rate derived from IEEE</td>
</tr>
<tr>
<td></td>
<td>Standard 802.11 specifications. Actual</td>
</tr>
<tr>
<td></td>
<td>throughput will vary. Network conditions</td>
</tr>
<tr>
<td></td>
<td>and environmental factors, including volume of</td>
</tr>
<tr>
<td></td>
<td>network traffic, building materials and</td>
</tr>
<tr>
<td></td>
<td>construction, and network overhead, lower</td>
</tr>
<tr>
<td></td>
<td>actual data throughput rate.</td>
</tr>
<tr>
<td>Channel width</td>
<td>20 MHz</td>
</tr>
<tr>
<td>Guard interval</td>
<td>Auto</td>
</tr>
<tr>
<td>Output power</td>
<td>Full</td>
</tr>
<tr>
<td>Wireless on/off (radio scheduling)</td>
<td>Disabled</td>
</tr>
<tr>
<td>RTS threshold</td>
<td>2347</td>
</tr>
<tr>
<td>Fragmentation length</td>
<td>2346</td>
</tr>
<tr>
<td>Beacon interval</td>
<td>100</td>
</tr>
<tr>
<td>Aggregation length</td>
<td>65535</td>
</tr>
<tr>
<td>AMPDU</td>
<td>Enabled</td>
</tr>
<tr>
<td>RIFS transmission</td>
<td>Disabled</td>
</tr>
<tr>
<td>DTIM interval</td>
<td>3</td>
</tr>
<tr>
<td>Preamble type</td>
<td>Auto</td>
</tr>
<tr>
<td>Antenna</td>
<td>Internal</td>
</tr>
<tr>
<td>802.11d</td>
<td>Enabled</td>
</tr>
<tr>
<td>Client isolation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Maximum wireless clients</td>
<td>128</td>
</tr>
<tr>
<td>Wi-Fi Multimedia (WMM)</td>
<td>Enabled</td>
</tr>
<tr>
<td>WMM powersave</td>
<td>Enabled</td>
</tr>
<tr>
<td>AP EDCA parameters (QoS settings)</td>
<td>See Table 32 on page 111.</td>
</tr>
<tr>
<td>Station EDCA parameters (QoS settings)</td>
<td>See Table 32 on page 111.</td>
</tr>
</tbody>
</table>
### Table 40. Default configuration settings (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>QoS policies</td>
<td>None</td>
</tr>
<tr>
<td>Wireless bridging</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

#### Default wireless profile and profile security

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>NETGEAR</td>
</tr>
<tr>
<td>Profile state</td>
<td>Enabled</td>
</tr>
<tr>
<td>Wireless network name (SSID)</td>
<td>NETGEAR_11ng</td>
</tr>
<tr>
<td>Broadcast wireless network name (SSID)</td>
<td>Enabled</td>
</tr>
<tr>
<td>Network authentication</td>
<td>Open system (no authentication)</td>
</tr>
<tr>
<td>Data encryption</td>
<td>None</td>
</tr>
<tr>
<td>Wireless client security separation</td>
<td>Disabled</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>1</td>
</tr>
</tbody>
</table>

#### Wireless security features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue AP detection</td>
<td>Disabled</td>
</tr>
<tr>
<td>Rogue AP detection policy</td>
<td>Moderate</td>
</tr>
<tr>
<td>MAC authentication</td>
<td>Disabled</td>
</tr>
<tr>
<td>RADIUS servers</td>
<td>None</td>
</tr>
<tr>
<td>RADIUS authentication port number</td>
<td>1812</td>
</tr>
<tr>
<td>RADIUS shared secret</td>
<td>sharedsecret</td>
</tr>
<tr>
<td>RADIUS accounting port number</td>
<td>1813</td>
</tr>
<tr>
<td>RADIUS reauthentication time</td>
<td>3600 seconds</td>
</tr>
<tr>
<td>RADIUS update of the global key</td>
<td>1800 seconds</td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Disabled</td>
</tr>
<tr>
<td>IDS/IPS policies</td>
<td>Preconfigured policies (see Table 24 on page 89), all disabled</td>
</tr>
<tr>
<td>IDS/IPS detection policy</td>
<td>Moderate</td>
</tr>
<tr>
<td>IDS/IPS mail settings</td>
<td>Blank</td>
</tr>
</tbody>
</table>
The wireless access point can be configured through either the command-line interface (CLI), a web browser, or a MIB browser.

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

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>-backup-configuration</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></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>
</tbody>
</table>
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

-- Administrator/superuser mail address

-- Select wireless lan interface

-- 2.4 GHz wireless LAN interface setting

-- Aggregated packet size

-- Aggregated MAC Protocol Data Unit

-- Wireless beacon period in TU (1024 us)

-- Wireless channel (depends on country and wireless mode)

-- Wireless channel width

-- Wireless DTIM period in beacon interval

-- Wireless fragmentation threshold (even only)

-- Interval (from interference from other transmissions)

-- Add known access point

-- Delete known access point

-- Add wireless access control (ACL)

-- Delete wireless access control (ACL) database

-- Delete wireless access control (ACL)

-- Transmit data rate

-- Enable wireless access control (ACL)

-- Wireless operation mode

-- Wireless transmit power

-- Wireless preamble (only effect on 802.11b rates)

-- Enable wireless radio

-- Wireless transmission date rate

-- Enable successive frame transmission at different transmit powers

-- Wireless RTS/CTS threshold

-- IEEE802.11d status

-- Client isolation status

-- Create QoS (Quality of service) policy

-- Create QoS (Quality of service) classification

-- Delete QoS (Quality of service) policy

-- Delete QoS (Quality of service) classification

-- Create security profile

-- 1st security profile

-- Wireless authentication type

-- Data encryption

-- Hide network name

-- Wireless wep key 1

-- Wireless wep key 2

-- Wireless wep key 3

-- Wireless wep key 4

-- Key number

-- Profile name

-- Pre-shared key

-- Disable associated wireless client communication

-- Network name (1-32 chars)

-- Profile status

-- VLAN id

-- Wireless wep passphrase key

-- Wireless wep key type

-- Apply QoS policy as a incoming

-- Apply QoS policy as a outgoing

-- Delete incoming QoS policy

Command-Line Reference

147
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

| | | | | | |-delete-outgoing-QoS-policy --Delete outgoing QoS policy
| | | | | | | | | |-2>
| | | | | | | | | |-authentication --Wireless authentication type
| | | | | | | | | |-encryption --Data encryption
| | | | | | | | | |-hide-network-name --Hide network name
| | | | | | | | | |-key1 --Wireless wep key 1
| | | | | | | | | |-key2 --Wireless wep key 2
| | | | | | | | | |-key3 --Wireless wep key 3
| | | | | | | | | |-key4 --Wireless wep key 4
| | | | | | | | | |-keyno --Key number
| | | | | | | | | |-name --Profile name
| | | | | | | | | |-presharedkey --Pre-shared key
| | | | | | | | | |-security-separation --Disable associated wireless client communication
| | | | | | | | | |-ssid --Network name (1-32 chars)
| | | | | | | | | |-status --Profile status
| | | | | | | | | |-vlan-id --VLAN id
| | | | | | | | | |-wep-pass-phrase --Wireless wep passphrase key
| | | | | | | | | |-wepkeytype --Wireless wep key type
| | | | | | | | | |-apply-incoming-QoS-policy --Apply QoS policy as a incoming
| | | | | | | | | |-apply-outgoing-QoS-policy --Apply QoS policy as a outgoing
| | | | | | | | | |-delete-incoming-QoS-policy --Delete incoming QoS policy
| | | | | | | | | |-delete-outgoing-QoS-policy --Delete outgoing QoS policy
| | | | | | | | | | |-3>
| | | | | | | | | |-authentication --Wireless authentication type
| | | | | | | | | |-encryption --Data encryption
| | | | | | | | | |-hide-network-name --Hide network name
| | | | | | | | | |-key1 --Wireless wep key 1
| | | | | | | | | |-key2 --Wireless wep key 2
| | | | | | | | | |-key3 --Wireless wep key 3
| | | | | | | | | |-key4 --Wireless wep key 4
| | | | | | | | | |-keyno --Key number
| | | | | | | | | |-name --Profile name
| | | | | | | | | |-presharedkey --Pre-shared key
| | | | | | | | | |-security-separation --Disable associated wireless client communication
| | | | | | | | | |-ssid --Network name (1-32 chars)
| | | | | | | | | |-status --Profile status
| | | | | | | | | |-vlan-id --VLAN id
| | | | | | | | | |-wep-pass-phrase --Wireless wep passphrase key
| | | | | | | | | |-wepkeytype --Wireless wep key type
| | | | | | | | | |-apply-incoming-QoS-policy --Apply QoS policy as a incoming
| | | | | | | | | |-apply-outgoing-QoS-policy --Apply QoS policy as a outgoing
| | | | | | | | | |-delete-incoming-QoS-policy --Delete incoming QoS policy
| | | | | | | | | |-delete-outgoing-QoS-policy --Delete outgoing QoS policy
| | | | | | | | | | |-4>
| | | | | | | | | |-authentication --Wireless authentication type
| | | | | | | | | |-encryption --Data encryption
| | | | | | | | | |-hide-network-name --Hide network name
| | | | | | | | | |-key1 --Wireless wep key 1
| | | | | | | | | |-key2 --Wireless wep key 2
| | | | | | | | | |-key3 --Wireless wep key 3
| | | | | | | | | |-key4 --Wireless wep key 4
| | | | | | | | | |-keyno --Key number
| | | | | | | | | |-name --Profile name
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid            --Network name (1-32 chars)
| | | | | | |-status           --Profile status
| | | | | | |-vlan-id            --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype           --Wireless wep key type
| | | | | | |-apply-incoming-QoSPolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSPolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSPolicyv--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSPolicyv--Delete outgoing QoS policy
| | | | | | |-5>                         --5th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1            --Wireless wep key 1
| | | | | | |-key2            --Wireless wep key 2
| | | | | | |-key3            --Wireless wep key 3
| | | | | | |-key4            --Wireless wep key 4
| | | | | | |-keyno           --Key number
| | | | | | |-name            --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid            --Network name (1-32 chars)
| | | | | | |-status           --Profile status
| | | | | | |-vlan-id            --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype           --Wireless wep key type
| | | | | | |-apply-incoming-QoSPolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSPolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSPolicyv--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSPolicyv--Delete outgoing QoS policy
| | | | | | |-6>                         --6th security profile
| | | | | | |-authentication           --Wireless authentication type
| | | | | | |-encryption               --Data encryption
| | | | | | |-hide-network-name        --Hide network name
| | | | | | |-key1            --Wireless wep key 1
| | | | | | |-key2            --Wireless wep key 2
| | | | | | |-key3            --Wireless wep key 3
| | | | | | |-key4            --Wireless wep key 4
| | | | | | |-keyno           --Key number
| | | | | | |-name            --Profile name
| | | | | | |-presharedkey             --Pre-shared key
| | | | | | |-security-separation      --Disable associated wireless client communication
| | | | | | |-ssid            --Network name (1-32 chars)
| | | | | | |-status           --Profile status
| | | | | | |-vlan-id            --VLAN id
| | | | | | |-wep-pass-phrase          --Wireless wep passphrase key
| | | | | | |-wepkeytype           --Wireless wep key type
| | | | | | |-apply-incoming-QoSPolicy --Apply QoS policy as a incoming
| | | | | | |-apply-outgoing-QoSPolicy --Apply QoS policy as a outgoing
| | | | | | |-delete-incoming-QoSPolicyv--Delete incoming QoS policy
| | | | | | |-delete-outgoing-QoSPolicyv--Delete outgoing QoS policy
| | | | | | |-7>                         --7th security profile
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

- **authentication** --Wireless authentication type
- **encryption** --Data encryption
- **hide-network-name** --Hide network name
- **key1** --Wireless wep key 1
- **key2** --Wireless wep key 2
- **key3** --Wireless wep key 3
- **key4** --Wireless wep key 4
- **keyno** --Key number
- **name** --Profile name
- **presharedkey** --Pre-shared key
- **security-separation** --Disable associated wireless client communication
- **ssid** --Network name (1-32 chars)
- **status** --Profile status
- **vlan-id** --VLAN id
- **wep-pass-phrase** --Wireless wep passphrase key
- **wepkeytype** --Wireless wep key type
- **apply-incoming-QoS-policy** --Apply QoS policy as a incoming
- **apply-outgoing-QoS-policy** --Apply QoS policy as a outgoing
- **delete-incoming-QoS-policy** --Delete incoming QoS policy
- **delete-outgoing-QoS-policy** --Delete outgoing QoS policy
- **8>** --8th security profile
- **authentication** --Wireless authentication type
- **encryption** --Data encryption
- **hide-network-name** --Hide network name
- **key1** --Wireless wep key 1
- **key2** --Wireless wep key 2
- **key3** --Wireless wep key 3
- **key4** --Wireless wep key 4
- **keyno** --Key number
- **name** --Profile name
- **presharedkey** --Pre-shared key
- **security-separation** --Disable associated wireless client communication
- **ssid** --Network name (1-32 chars)
- **status** --Profile status
- **vlan-id** --VLAN id
- **wep-pass-phrase** --Wireless wep passphrase key
- **wepkeytype** --Wireless wep key type
- **apply-incoming-QoS-policy** --Apply QoS policy as a incoming
- **apply-outgoing-QoS-policy** --Apply QoS policy as a outgoing
- **delete-incoming-QoS-policy** --Delete incoming QoS policy
- **delete-outgoing-QoS-policy** --Delete outgoing QoS policy

- **ids-ips-profile**
  - **ips-status** --IDS/IPS (Intrusion detection & prevention system) status
  - **ips-detection-policy** --IDS/IPS (Intrusion detection & prevention system) policies
  - **attack-status** --IDS/IPS attack configurations
  - **EAPOL-logoff-attack** --EAPOL logoff attack status
  - **EAPOL-start-attack** --EAPOL start attack status
  - **adhoc-network-detected** --ADHOC network detected attack status
  - **adhoc-nw-wired-connectivity** --ADHOC network wired connectivity attack status
  - **ap-property-change** --AP property change attack status
  - **association-flood** --Association flood attack status
  - **association-table-overflow** --Association table overflow attack status
| | | | | | |-authentication-failure-attack      --Authentication failure attack status  
| | | | | | |-authentication-flood               --Authentication flood attack status  
| | | | | | |-cts-flood                          --CTS flood attack status  
| | | | | | |-rts-flood                          --RTS flood attack status  
| | | | | | |-deauthentication-broadcast-attack  --Deauthentication broadcast attack status  
| | | | | | |-device-probing-for-AP              --Device probing for AP attack status  
| | | | | | |-disassociation-flood               --Disassociation flood attack status  
| | | | | | |-known-client-association-Adhoc-nw  --Known client association ADHOC network attack status  
| | | | | | |-mac-spoofing                       --MAC spoofing attack status  
| | | | | | |-malformed-802.11-packet-detection  --Malformed IEEE802.11 packet detection attack status  
| | | | | | |-premature-EAP-failure-attack       --Premature EAP failure attack status  
| | | | | | |-premature-EAP-success-attack       --Premature EAP success attack status  
| | | | | | |-ps-poll-flood-attack               --PS POLL flood attack status  
| | | | | | |-rf-jamming-attack                  --RF jamming attack status  
| | | | | | |-rogue-ap-detection                 --Rogue AP detection attack status  
| | | | | | |-unauthenticated-association        --Unauthenticated-association attack status  
| | | | | | |-virtual-carrier-attack             --Virtual carrier attack status  
| | | | | | |-wireless-bridge>                 --Wireless bridge setting  
| | | | | | |-security-profile>               --Create security profile  
| | | | | | | |-1>                               --1st security profile  
| | | | | | | |-authentication                 --Authentication type  
| | | | | | | |-encryption                    --Data encryption  
| | | | | | | |-name                        --Profile name  
| | | | | | | |-presharedkey                 --Preshared key  
| | | | | | | |-remote-mac                  --Remote MAC  
| | | | | | | |-status                     --Profile status  
| | | | | | | |-wep-pass-phrase              --Wireless wep passphrase key  
| | | | | | | |-wepkey                     --Wireless wep key  
| | | | | | | |-wepkeytype                  --Wireless wep key type  
| | | | | | | |-2>                               --2nd security profile  
| | | | | | | |-authentication                 --Authentication type  
| | | | | | | |-encryption                    --Data encryption  
| | | | | | | |-name                        --Profile name  
| | | | | | | |-presharedkey                 --Preshared key  
| | | | | | | |-remote-mac                  --Remote MAC  
| | | | | | | |-status                     --Profile status  
| | | | | | | |-wep-pass-phrase              --Wireless wep passphrase key  
| | | | | | | |-wepkey                     --Wireless wep key  
| | | | | | | |-wepkeytype                  --Wireless wep key type  
| | | | | | | |-3>                               --3rd security profile  
| | | | | | | |-authentication                 --Authentication type  
| | | | | | | |-encryption                    --Data encryption  
| | | | | | | |-name                        --Profile name  
| | | | | | | |-presharedkey                 --Preshared key  
| | | | | | | |-remote-mac                  --Remote MAC  
| | | | | | | |-status                     --Profile status  
| | | | | | | |-wep-pass-phrase              --Wireless wep passphrase key  
| | | | | | | |-wepkey                     --Wireless wep key  
| | | | | | | |-wepkeytype                  --Wireless wep key type  
| | | | | | | |-4>                               --4th security profile  
| | | | | | | |-authentication                 --Authentication type  

---

**Command-Line Reference**

151
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

| | | | | |-security-profile> --Create security profile
| | | | | |-1> --1st security profile
| | | | | |-authentication --Wireless authentication type
| | | | | |-encryption --Data encryption
| | | | | |-hide-network-name --Hide network name
| | | | | |-key1 --Wireless wep key 1
| | | | | |-key2 --Wireless wep key 2
| | | | | |-key3 --Wireless wep key 3
| | | | | |-key4 --Wireless wep key 4
| | | | | |-keyno --Key number
| | | | | |-name --Profile name
| | | | | |-presharedkey --Pre-shared key
| | | | | |-security-separation --Disable associated wireless client communication
| | | | | |-ssid --Network name (1-32 chars)
| | | | | |-status --Profile status
| | | | | |-vlan-id --VLAN id
| | | | | |-wep-pass-phrase --Wireless wep passphrase key
| | | | | |-wepkeytype --Wireless wep key type
| | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |-2> --2nd security profile
| | | | | |-authentication --Wireless authentication type
| | | | | |-encryption --Data encryption
| | | | | |-hide-network-name --Hide network name
| | | | | |-key1 --Wireless wep key 1
| | | | | |-key2 --Wireless wep key 2
| | | | | |-key3 --Wireless wep key 3
| | | | | |-key4 --Wireless wep key 4
| | | | | |-keyno --Key number
| | | | | |-name --Profile name
| | | | | |-presharedkey --Pre-shared key
| | | | | |-security-separation --Disable associated wireless client communication
| | | | | |-ssid --Network name (1-32 chars)
| | | | | |-status --Profile status
| | | | | |-vlan-id --VLAN id
| | | | | |-wep-pass-phrase --Wireless wep passphrase key
| | | | | |-wepkeytype --Wireless wep key type
| | | | | |-apply-incoming-QoSpolicy --Apply QoS policy as a incoming
| | | | | |-apply-outgoing-QoSpolicy --Apply QoS policy as a outgoing
| | | | | |-delete-incoming-QoSpolicy--Delete incoming QoS policy
| | | | | |-delete-outgoing-QoSpolicy--Delete outgoing QoS policy
| | | | | |-3> --3rd security profile
| | | | | |-authentication --Wireless authentication type
| | | | | |-encryption --Data encryption
| | | | | |-hide-network-name --Hide network name
| | | | | |-key1 --Wireless wep key 1
| | | | | |-key2 --Wireless wep key 2
| | | | | |-key3 --Wireless wep key 3
| | | | | |-key4 --Wireless wep key 4
| | | | | |-keyno --Key number
| | | | | |-name --Profile name
| | | | | |-presharedkey --Pre-shared key
| | | | | |-security-separation --Disable associated wireless client communication
<table>
<thead>
<tr>
<th>Command-Line Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620</td>
</tr>
</tbody>
</table>

<p>| ssid          | --Network name (1-32 chars) |
| status        | --Profile status |
| -vlan-id      | --VLAN id |
| -wep-pass-phrase | --Wireless wep passphrase key |
| -wepkeytype   | --Wireless wep key type |
| -apply-incoming-QoS policy | --Apply QoS policy as a incoming |
| -apply-outgoing-QoS policy | --Apply QoS policy as a outgoing |
| -delete-incoming-QoS policy | --Delete incoming QoS policy |
| -delete-outgoing-QoS policy | --Delete outgoing QoS policy |
| -4&gt;          | --4th security profile |
| -authentication | --Wireless authentication type |
| -encryption   | --Data encryption |
| -hide-network-name | --Hide network name |
| -key1         | --Wireless wep key 1 |
| -key2         | --Wireless wep key 2 |
| -key3         | --Wireless wep key 3 |
| -key4         | --Wireless wep key 4 |
| -keyno        | --Key number |
| -name         | --Profile name |
| -presharedkey | --Pre-shared key |
| -security-separation | --Disable associated wireless client communication |
| -ssid         | --Network name (1-32 chars) |
| -status       | --Profile status |
| -vlan-id      | --VLAN id |
| -wep-pass-phrase | --Wireless wep passphrase key |
| -wepkeytype   | --Wireless wep key type |
| -apply-incoming-QoS policy | --Apply QoS policy as a incoming |
| -apply-outgoing-QoS policy | --Apply QoS policy as a outgoing |
| -delete-incoming-QoS policy | --Delete incoming QoS policy |
| -delete-outgoing-QoS policy | --Delete outgoing QoS policy |
| -5&gt;          | --5th security profile |
| -authentication | --Wireless authentication type |
| -encryption   | --Data encryption |
| -hide-network-name | --Hide network name |
| -key1         | --Wireless wep key 1 |
| -key2         | --Wireless wep key 2 |
| -key3         | --Wireless wep key 3 |
| -key4         | --Wireless wep key 4 |
| -keyno        | --Key number |
| -name         | --Profile name |
| -presharedkey | --Pre-shared key |
| -security-separation | --Disable associated wireless client communication |
| -ssid         | --Network name (1-32 chars) |
| -status       | --Profile status |
| -vlan-id      | --VLAN id |
| -wep-pass-phrase | --Wireless wep passphrase key |
| -wepkeytype   | --Wireless wep key type |
| -apply-incoming-QoS policy | --Apply QoS policy as a incoming |
| -apply-outgoing-QoS policy | --Apply QoS policy as a outgoing |
| -delete-incoming-QoS policy | --Delete incoming QoS policy |
| -delete-outgoing-QoS policy | --Delete outgoing QoS policy |
| -6&gt;          | --6th security profile |
| -authentication | --Wireless authentication type |</p>
<table>
<thead>
<tr>
<th></th>
<th>encryption</th>
<th>--Data encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>hide-network-name</td>
<td>--Hide network name</td>
</tr>
<tr>
<td></td>
<td>key1</td>
<td>--Wireless wep key 1</td>
</tr>
<tr>
<td></td>
<td>key2</td>
<td>--Wireless wep key 2</td>
</tr>
<tr>
<td></td>
<td>key3</td>
<td>--Wireless wep key 3</td>
</tr>
<tr>
<td></td>
<td>key4</td>
<td>--Wireless wep key 4</td>
</tr>
<tr>
<td></td>
<td>keyno</td>
<td>--Key number</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>--Profile name</td>
</tr>
<tr>
<td></td>
<td>presharedkey</td>
<td>--Pre-shared key</td>
</tr>
<tr>
<td></td>
<td>security-separation</td>
<td>--Disable associated wireless client communication</td>
</tr>
<tr>
<td></td>
<td>ssid</td>
<td>--Network name (1-32 chars)</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>--Profile status</td>
</tr>
<tr>
<td></td>
<td>vlan-id</td>
<td>--VLAN id</td>
</tr>
<tr>
<td></td>
<td>wep-pass-phrase</td>
<td>--Wireless wep passphrase key</td>
</tr>
<tr>
<td></td>
<td>wepkeytype</td>
<td>--Wireless wep key type</td>
</tr>
<tr>
<td></td>
<td>apply-incoming-QoSpolicy</td>
<td>--Apply QoS policy as a incoming</td>
</tr>
<tr>
<td></td>
<td>apply-outgoing-QoSpolicy</td>
<td>--Apply QoS policy as a outgoing</td>
</tr>
<tr>
<td></td>
<td>delete-incoming-QoSpolicy</td>
<td>--Delete incoming QoS policy</td>
</tr>
<tr>
<td></td>
<td>delete-outgoing-QoSpolicy</td>
<td>--Delete outgoing QoS policy</td>
</tr>
<tr>
<td></td>
<td>7&gt;</td>
<td>--7th security profile</td>
</tr>
<tr>
<td></td>
<td>authentication</td>
<td>--Wireless authentication type</td>
</tr>
<tr>
<td></td>
<td>encryption</td>
<td>--Data encryption</td>
</tr>
<tr>
<td></td>
<td>hide-network-name</td>
<td>--Hide network name</td>
</tr>
<tr>
<td></td>
<td>key1</td>
<td>--Wireless wep key 1</td>
</tr>
<tr>
<td></td>
<td>key2</td>
<td>--Wireless wep key 2</td>
</tr>
<tr>
<td></td>
<td>key3</td>
<td>--Wireless wep key 3</td>
</tr>
<tr>
<td></td>
<td>key4</td>
<td>--Wireless wep key 4</td>
</tr>
<tr>
<td></td>
<td>keyno</td>
<td>--Key number</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>--Profile name</td>
</tr>
<tr>
<td></td>
<td>presharedkey</td>
<td>--Pre-shared key</td>
</tr>
<tr>
<td></td>
<td>security-separation</td>
<td>--Disable associated wireless client communication</td>
</tr>
<tr>
<td></td>
<td>ssid</td>
<td>--Network name (1-32 chars)</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>--Profile status</td>
</tr>
<tr>
<td></td>
<td>vlan-id</td>
<td>--VLAN id</td>
</tr>
<tr>
<td></td>
<td>wep-pass-phrase</td>
<td>--Wireless wep passphrase key</td>
</tr>
<tr>
<td></td>
<td>wepkeytype</td>
<td>--Wireless wep key type</td>
</tr>
<tr>
<td></td>
<td>apply-incoming-QoSpolicy</td>
<td>--Apply QoS policy as a incoming</td>
</tr>
<tr>
<td></td>
<td>apply-outgoing-QoSpolicy</td>
<td>--Apply QoS policy as a outgoing</td>
</tr>
<tr>
<td></td>
<td>delete-incoming-QoSpolicy</td>
<td>--Delete incoming QoS policy</td>
</tr>
<tr>
<td></td>
<td>delete-outgoing-QoSpolicy</td>
<td>--Delete outgoing QoS policy</td>
</tr>
<tr>
<td></td>
<td>8&gt;</td>
<td>--8th security profile</td>
</tr>
<tr>
<td></td>
<td>authentication</td>
<td>--Wireless authentication type</td>
</tr>
<tr>
<td></td>
<td>encryption</td>
<td>--Data encryption</td>
</tr>
<tr>
<td></td>
<td>hide-network-name</td>
<td>--Hide network name</td>
</tr>
<tr>
<td></td>
<td>key1</td>
<td>--Wireless wep key 1</td>
</tr>
<tr>
<td></td>
<td>key2</td>
<td>--Wireless wep key 2</td>
</tr>
<tr>
<td></td>
<td>key3</td>
<td>--Wireless wep key 3</td>
</tr>
<tr>
<td></td>
<td>key4</td>
<td>--Wireless wep key 4</td>
</tr>
<tr>
<td></td>
<td>keyno</td>
<td>--Key number</td>
</tr>
<tr>
<td></td>
<td>name</td>
<td>--Profile name</td>
</tr>
<tr>
<td></td>
<td>presharedkey</td>
<td>--Pre-shared key</td>
</tr>
<tr>
<td></td>
<td>security-separation</td>
<td>--Disable associated wireless client communication</td>
</tr>
<tr>
<td></td>
<td>ssid</td>
<td>--Network name (1-32 chars)</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>--Profile status</td>
</tr>
<tr>
<td></td>
<td>vlan-id</td>
<td>--VLAN id</td>
</tr>
</tbody>
</table>
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

- `-wep-pass-phrase` --Wireless wep passphrase key
- `-wepkeytype` --Wireless wep key type
- `-apply-incoming-QoSpolicy` --Apply QoS policy as a incoming
- `-apply-outgoing-QoSpolicy` --Apply QoS policy as a outgoing
- `-delete-incoming-QoSpolicy` --Delete incoming QoS policy
- `-delete-outgoing-QoSpolicy` --Delete outgoing QoS policy

- `-ids-ips-profile` — IDS/IPS (Intrusion detection & prevention system) status
- `-ips-status` — IDS/IPS attack configurations
- `-ips-detection-policy` — IDS/IPS (Intrusion detection & prevention system policies
- `-attack-status` — IDS/IPS attack configurations
- `-EAPOL-logoff-attack` — EAPOL logoff attack status
- `-EAPOL-start-attack` — EAPOL start attack status
- `-adhoc-network-detected` — ADHOC network detected attack status
- `-adhoc-nw-wired-connectivity` — ADHOC network wired connectivity attack status
- `-association-flood` — Association flood attack status
- `-association-table-overflow` — Association table overflow attack status
- `-authentication-failure-attack` — Authentication failure attack status
- `-authentication-flood` — Authentication flood attack status
- `-cts-flood` — CTS flood attack status
- `-rts-flood` — RTS flood attack status
- `-deauthentication-broadcast-attack` — Deauthentication broadcast attack status
- `-device-probing-for-AP` — Device probing for AP attack status
- `-disassociation-flood` — Disassociation flood attack status
- `-known-client-association-Adhoc-nw` — Known client association ADHOC network attack status
- `-mac-spoofing` — MAC spoofing attack status
- `-malformed-802.11-packet-detection` — Malformed IEEE802.11 packet detection attack status
- `-premature-EAP-failure-attack` — Premature EAP failure attack status
- `-premature-EAP-success-attack` — Premature EAP success attack status
- `-ps-poll-flood-attack` — PS POLL flood attack status
- `-rf-jamming-attack` — RF jamming attack status
- `-rogue-ap-detection` — Rogue AP detection attack status
- `-unauthenticated-association` — Unauthenticated-association attack status
- `-virtual-carrier-attack` — Virtual carrier attack status

- `-wireless-bridge` — Wireless bridge setting
- `-security-profile` — Create security profile
- `1>` — 1st security profile
- `-authentication` — Authentication type
- `-encryption` — Data encryption
- `-name` — Profile name
- `-presharedkey` — Preshared key
- `-remote-mac` — Remote MAC
- `-status` — Profile status
- `-wep-pass-phrase` — Wireless wep passphrase key
- `-wepkey` — Wireless wep key
- `-wepkeytype` — Wireless wep key type

- `2>` — 2nd security profile
- `-authentication` — Authentication type
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

- encryption --Data encryption
- name --Profile name
- presharedkey --Preshared key
- remote-mac --Remote MAC
- status --Profile status
- wep-pass-phrase --Wireless wep passphrase key
- wepkey --wireless wep key
- wepkeytype --wireless wep key type
- 3> --3rd security profile
- authentication --Authentication type
- encryption --Data encryption
- name --Profile name
- presharedkey --Preshared key
- remote-mac --Remote MAC
- status --Profile status
- wep-pass-phrase --Wireless wep passphrase key
- wepkey --Wireless wep key
- wepkeytype --Wireless wep key type
- 4> --4th security profile
- authentication --Authentication type
- encryption --Data encryption
- name --Profile name
- presharedkey --Preshared key
- remote-mac --Remote MAC
- status --Profile status
- wep-pass-phrase --Wireless wep passphrase key
- wepkey --Wireless wep key
- wepkeytype --Wireless wep key type
- wmm> --WMM settings
- ap-data0-best-effort --Access point best effort voice data
- ap-data1-background --Access point low-priority data
- ap-data2-video --Access point video data
- ap-data3-voice --Access point voice data
- powersave
- station-data0-best-effort --Station best effort voice data
- station-data1-background --Station low-priority data
- station-data2-video --Station video data
- station-data3-voice --Station voice data
- support --???
- ipv4> --Set host IPv4
- address --Host IPv4 address
- default-gateway --IPv4 address of default gateway
- dhcp-client --Enable dhcppv4 client
- dns-server --IPv4 address of DNS server
- network-integrity-check
- ipv6> --Set host IPv6
- address --Host IPv6 address
| |  | -default-gateway --IPv6 address of default gateway
| |  | -dhcp-client --Enable dhcpv6 client
| |  | -dns-server --IPv6 address of DNS server
| |  | -network-integrity-check
| |  | -log> --Syslog setting
| |  | -syslog-status --Enable syslog client
| |  | -syslog-server-ip --Syslog server IP address
| |  | -syslog-server-port --Syslog server port number
| |  | -lldp-status --Enable/Disable LLDP
| |  | -radiusv4>
| |  | -radiusv6>
| |  | -remote>
| |  | -ssh --Enable remote access via SSH
| |  | -telnet --Enable remote access via Telnet
| |  | -snmp>
| |  | -description --SNMP system description
| |  | -read-community --SNMP ReadCommunity
| |  | -snmp-status --SNMP status
| |  | -trap-community --SNMP ReadCommunity
| |  | -trap-server --SNMP TrapServer IP address
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

||--write-community                   --SNMP WriteCommunity
||--spanning-tree                     --Enable spanning tree protocol
||--time>                             --Time Setting
||--custom-ntp-server                 --Custom NTP server host name
||--ntp-client                        --NTP client host name
||--ntp-server                        --NTP server host name
||--time-zone                         --Time zone
||--vlan>                             --VLAN settings
||--management-vlan                  --VLAN management-id
||--untagged-vlan                    --Untagged VLAN-id
||--untagged-vlan-status             --Untagged vlan status
||
||--exit                               --Logout from CLI
|--file                               --
|--firmware-upgrade                    --Upload new system firmware file from httpd server
|--firmware-upgrade-tftp              --Upload new system firmware file from tftpd server
|--password                           --System password
|--reboot                             --System reboot
|--restore-configuration              --Restore system configuration
|--restore-default-password           --Restore default system password
|--restore-factory-default            --Restore default system configurations
|--show>                              --Show system settings
|--configuration                      --Show system configuration
|--interface>                         --Show wireless lan interface
| ||--eth>                             --Ethernet interface
| ||--statistics                      --Show ethernet statistics
| |
| ||--wlan>                            --Wlan interface settings
| | ||--2.4GHz>                         --2.4GHz wlan interface settings
| | |||--configuration                   --Interface configuration
| | |||--statistics                      --Interface statistics
| | |||--stationlist                     --Station list
| | |||--trusted-stationlist             --Trusted station list
| | |||--knownaplist                     --Known access point list
| | |||--unknownaplist                   --Unknown access point list
| | |||--ids-ips-statistics               --IDS/IPS statistics
| | |||--ids-ips-thresholds               --IDS/IPS thresholds
| | |||--ids-ips-traps                    --IDS/IPS trap list
| | |||--qos-policies                     --QoS policy list
| | |
| | ||--5GHz>                           --5GHz wlan interface settings
| | |||--configuration                   --Interface configuration
| | |||--statistics                      --Interface statistics
| | |||--stationlist                     --Station list
| | |||--trusted-stationlist             --Trusted station list
| | |||--knownaplist                     --Known access point list
| | |||--unknownaplist                   --Unknown access point list
| | |||--ids-ips-statistics               --IDS/IPS statistics
| | |||--ids-ips-thresholds               --IDS/IPS thresholds
| | |||--ids-ips-traps                    --IDS/IPS trap list
| | |||--qos-policies                     --QoS policy list
| | |
| | |
| |

Command-Line Reference

159
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

| | |-log> --System log
| |-system --System setting
| |-time --System time settings
| |
Index

Numerics
11a and 11na wireless modes 32
11b, 11bg, and 11ng wireless modes 29
2.4 GHz antenna, connectors for 13
2.4 GHz or 5 GHz operation 9
64-bit, 128-bit, and 152-bit WEP 54
802.11b/g/n and 802.11a/n wireless adapters 19
wireless settings 28–34
802.11d support 109
802.1P, QoS policies 115
802.1Q VLAN 9, 105

A
access, restricting by MAC address 43, 60
accounting, RADIUS servers 57–59
accounts, users 75
Active LED
behavior 21
described 12
troubleshooting 133
ActiveX 135
activity log 83
ad hoc networks
detecting 92
monitoring 97
admin password
changing or restoring 74
default 142
AES (Advanced Encryption Standard) 44, 56–57
Aggregated MAC Protocol Data Unit (A-MPDU) frames 109
aggregation length 109
aggressive detection policy 86, 94
AID (associated identifier) 82
AIFS (Arbitration Inter-Frame Spacing) interval 111
A-MPDU (Aggregated MAC Protocol Data Unit) frames 109
antennas
connecting external 13
enabling internal or external 109
external orientation 18
Arbitration Inter-Frame Spacing (AIFS) interval 111
associated identifier (AID) 82
association flood and table overflow 89–90
associations, wireless clients 85
attacks
detecting and preventing 89
monitoring 96
authentication
network 45
RADIUS servers 57–58
authentication flood and failure attack 89–90
autosensing over Ethernet 10
backing up 70
background traffic
advanced QoS 110
WMM QoS 63
beacon interval 109
beacons, unknown access points 87
best effort traffic
advanced QoS 110
WMM QoS 63
bits per second, QoS policies 116–117
bridging modes, wireless 118
broadcast packets, transmitted and received 85
broadcasting wireless network names (SSIDs)
802.11a/na modes 33
802.11b/bg/ng modes 30
security 43
browsers, recommended 22
BSS (basic service set) 45
BSSID (basic service set identifier)
ad hoc networks 98
configuring 48–57
described 8, 43–44
monitoring 81
burst rate, QoS policies 116–117
bytes, received and transmitted
   Ethernet connection 84
   wireless connection 82

capturing packets 138
Carrier Sense Multiple Access (CSMA) 108
Category 5 Ethernet cable 7
channel width (802.11na) 33
channel width and offset (802.11ng) 30
channels and frequencies
   defaults 140
      selecting for 802.11a/na modes 33
      selecting for 802.11b/bg/ng modes 30
channels, wireless spacing 18
classifications, QoS policies 114–117
Clear to Send (CTS) packets 108
CLI (command line-interface) commands 146
clients
   associated, number of 85
   DHCPv4, enabling 26
   DHCPv6, enabling 100
   isolation, enabling 109
   maximum number 109
   monitoring 80
   NTP, enabling 25
   trusted 61
   wireless separation, enabling 45, 52
collision detection and collision avoidance, CSMA 108
command line-interface (CLI) commands 146
community names and traps, SNMP 65
compliance
   electromagnetic 141
configuration file, backing up or restoring 70
connectors and ports, rear panel 13
console port 13
country, wireless location 24
CSMA (Carrier Sense Multiple Access) 108
CTS (Clear to Send) packets 108
CTS flood 91
cwMin (minimum contention window) and cwMax (maximum contention window) values 111

data encryption
   WEP 54
   WPA and WPA2 57
data rates
   802.11a mode 34

802.11b/bg modes 31
specifications for all modes 139–140
date and time, troubleshooting 137
deauthentication broadcast attack 90
defaults
   channels and frequencies 140
   DHCPv4 gateway 28
   DHCPv6 gateway 103
   factory settings, list of 142–145
   factory settings, restoring 71
   IPv4 address 22, 142
   IPv6 address 142
   ISP gateway 26, 101
   login password 22, 142
   prefix length 142
   SNMP 65
   subnet mask 26, 142
   user name 22, 142
delivery traffic indication message (DTIM) interval 109
destination port, QoS policies 116
detection policies
   IDS/IPS 94
   rogue access points 86
device probing 93
DHCP (Dynamic Host Configuration Protocol)
   DHCPv4 client and server 26–28
   DHCPv6 client and server 100–103
disassociation flood 90
DNS (Domain Name System) servers
   IPv4 26–28
   IPv6 100–103
DTIM (delivery traffic indication message) interval 109
dual-band support (nonconcurrent) 9
Dynamic Host Configuration Protocol (DHCP)
   DHCPv4 client and server 26–28
   DHCPv6 client and server 100–103

EAPOL (Extensible Authentication Protocol) attacks 91
EDCA (Enhanced Distributed Channel Access) parameters 110–112
electromagnetic compliance 141
email settings, IDS/IPS 95
encryption
   WEP 54
   WPA and WPA2 57
environmental specifications 141
ESS (extended service set) 45
Ether type, QoS policies 115
Ethernet cabling requirements 18
Ethernet packets and bytes, received and transmitted 84
extended service set (ESS) 45
Extensible Authentication Protocol (EAPOL) attacks 91
external antennas
  connecting 13
  enabling 109

F
factory default settings
  list of 142–145
  restoring 71
firmware
  backing up 70
  factory defaults 71
  restoring from backup file 71
  upgrading 68
  version, viewing 79
flash memory 67
fragmentation length 108
frequencies and channels
  defaults 140
  selecting for 802.11a/na modes 33
  selecting for 802.11b/bg/ng modes 30
FTP traffic
  advanced QoS 110
  WMM QoS 63

G
gateways
  ISP and DHCPv4 26–28
  ISP and DHCPv6 101–103
generating keys, WEP 54
Gigabit Ethernet (RJ-45) port 13
graphical user interface (GUI)
  described 22
  troubleshooting 134
guard interval
  802.11a 33
  802.11g 30

H
hotspot server 106

I
idle time 82
IDS (intrusion detection system) 10, 89
importing known access points 86
infrastructure mode 19
installation kits 35
installation order 20
interface rate limiting and burst rate 117

interference 18
internal antenna, disabling 109
Internet browsing, troubleshooting 134
intrusion detection system (IDS) and intrusion prevention system (IPS) 10, 89
IP addresses
  NTP servers 25
  QoS policies 116
  SNMP manager 65
  syslog server 77
  TFTP server 69
IP DCSP and IP precedence, QoS policies 114
IPS (intrusion prevention system) 10, 89
IPv4 addresses
  default 22, 26, 79, 142
  DHCPv4 and DNS servers 26–28
  DHCPv4 WINS servers 28
  errors 19
  RADIUS servers 58
  requirements 19
  static for management computer 142
IPv6 addresses
  default 79, 100, 142
  DHCPv6 and DNS servers 100–103
  DHCPv6 WINS servers 103
  dynamic 79, 101
  errors 19
  RADIUS servers 58
  requirements 19
isolating clients 109

J
Java and Javascript 135

K
key generation, WEP 54
key update, RADIUS servers 59

L
LAN
  configuration requirements 18
  IPv4 and IPv6 addresses 142
  troubleshooting 134
LAN LED
  behavior 21
  described 12
  troubleshooting 133
LAN path, troubleshooting 136
lease
  DHCPv4 28
  DHCPv6 103
ProSAFE Premium 3 x 3 Dual-Band Wireless-N Access Point WNDAP620

LEDs
behavior 21
described 12
troubleshooting 132
legacy 802.1X (wireless security) 51, 54
LLDP (Link Layer Discovery Protocol) 105
local MAC addresses 60
location, country and region 24
logging activities 83
logging in 22
login URL, name, and password 142
losing wireless connection 61

M
MAC addresses
ad hoc network clients 98
default, wireless access point 24
Ethernet port 79
known access points 88
QoS policies 115
restricting access by 43, 60
unknown access points 87
wireless card 79
MAC spoofing 92
malformed 802.11 packets 90
management VLAN 104
management, remote options 64
match clauses, QoS policies 114–117
maximum burst value 112
maximum contention window (cwMax) value 111
maximum number of clients 109
MCS (Modulation and Coding Scheme)
index and data rate 802.11na 33
index and data rate 802.11ng 30
mild detection policy 86, 94
minimum contention window (cwMin) value 111
moderate detection policy 86, 94
Modulation and Coding Scheme (MCS) 30, 33
mounting plate
ceiling 36
wall 38
multicast packets, transmitted and received 85

N
names
attacks and IDS/IPS policies 89
firmware file 69
mail sender 95
NTP server 25
profiles 50
QoS policies 113
SNMP communities 65
users 75
wireless access point 24
wireless network (SSID for 802.11a/na modes) 33
wireless network (SSID for 802.11b/bg/ng modes) 30
NetBIOS name 24
network
ad hoc 97
authentication 45
collection, troubleshooting 136
integrity check 26, 101
Network Time Protocol (NTP), client and server 25

O
open system (no security) 51, 53
operating frequencies 140
operating modes 9
order of installation and configuration 20
output power
2.4 GHz transmission 31
5.4 GHz transmission 34

P
package contents 7
packets
capturing 138
received and transmitted 84
passphrase
WEP 54
WPA, WPA2, and mixed mode 44, 57
password
changing or restoring 74
default 22
login 142
physical connections, troubleshooting 136
physical specifications 141
pinging wireless access point 134, 135
placement, wireless equipment 17
PoE (Power over Ethernet) 10, 21
point-to-multipoint bridge
regular mode 122
repeating wireless signal 126
point-to-point bridge 118
port and connectors, rear panel 13
ports
QoS policy classification 116
RADIUS servers 58
SNMP manager, traps 65
syslog server 77
power adapter specifications 141
power socket 13
Power/Test LED
  behavior 21
  described 12
  troubleshooting 132
powersaving, WMM 63
preamble type 109
prefix length
  default 142
  DHCPv6 clients 103
  wireless access point 79, 100
premature EAP attacks 91
pre-shared key (PSK), WPA, WPA2, and mixed mode 44, 57
priority queues
  advanced QoS 110
  WMM QoS 62
privileges, user accounts 75
product registration 14
profiles, security
  creating and configuring 48–52
  described 44
PS poll flood attack 93
PSK (pre-shared key), WPA, WPA2, and mixed mode 44, 57
Q
QoS (Quality of Service)
  advanced settings 110–112
  basic settings (WMM) 62–63
  policies 112–117
  rate limiting and burst rate 116–117
R
radio
  scheduling to turn off 61
  turning off, 2.4 GHz 29
  turning off, 5 GHz 32
RADIUS servers, configuring 57
range guidelines, wireless equipment 17
rate limiting, QoS policies 116–117
read-only name, read-write name, SNMP 65
rear panel 13
reauthentication time, RADIUS servers 59
rebooting from web management interface 73
received signal strength indicator (RSSI) 82
redirecting HTTP requests 106
Reduced Interframe Space (RIFS) transmission 109
region, wireless location 24
registering product 14
remote devices, troubleshooting 137
remote MAC addresses 60
remote management, options 64
repeating wireless signal 126
Request to Send (RTS) threshold 108
Reset button 13, 73, 142
restoring
  factory defaults 71
  password 74
  settings, from backup file 71
restricting access by MAC address 43, 60
RF jamming attack 92
RIFS (Reduced Interframe Space) transmission 109
roaming 45
rogue access point detection 85–88
RSSI (received signal strength indicator) 82
RTS (Request to Send) threshold 108
RTS flood 91
Rx sequence 82
S
Secure Shell (SSH), enabling 66
security lock 13
security profiles
  creating and configuring 48–52
  described 44
security, wireless options 42
separating wireless clients 45, 52
serial number 79
servers, configuring
  DHCPv4 27
  DHCPv6 102
  DNS 26–28, 101–103
  hotspot 106
  NTP 25
  RADIUS 57
  syslog 76
service set identifiers. See SSIDs.
settings 117
shared key, WEP 51, 53
shared secrets, RADIUS servers 59
signal-to-noise ratio (SNR) 82
SMA connectors, external antennas 13
SNMP (Simple Network Management Protocol),
  configuring 64
software
  backing up 70
  factory defaults 71
  restoring from backup file 71
upgrading 68
version, viewing 79
source port, QoS policies 116
Spanning Tree Protocol (STP), enabling 105
specifications, technical 139
SSH (Secure Shell), enabling 66
SSIDt (service set identifiers)
  broadcasting 50
  broadcasting and security 43
  broadcasting for 802.11a/na modes 33
  broadcasting for 802.11b/bg/ng modes 30
  matching 19
stateless and stateful DHCPv6 server 102
station EDCA parameters 112
statistics, traffic 83
STP (Spanning Tree Protocol), enabling 105
streaming media
  advanced QoS 110
  WMM QoS 62
subnet mask
  default 142
  DHCPv4 clients 28
  wireless access point 26
supported standards 8
syslog 76
system monitoring 77
system requirements 8

T
tagged VLAN 104
TCP/IP network, troubleshooting 135
technical specifications 139
technical support 2
Telnet, enabling 66
Temporal Key Integrity Protocol (TKIP) 44, 56–57
TFTP server, upgrade procedure 69
time and time zone
  configuring 24
  troubleshooting 137
time-out error 135
TKIP (Temporal Key Integrity Protocol) 44, 56–57
TKIP + AES (WPA & WPA2 mixed mode) 56–57
top panel 11
traffic
  advanced QoS 110
  patterns, analyzing 138
  statistics 83
  WMM QoS 62
traffic classes, QoS policies 116
transmission opportunity (TXOP) limit 112
transmission output power
  2.4 GHz radio 31
  5.4 GHz radio 34
traps
  IDS/IPS 89
  SNMP 65
troubleshooting
  basic functioning 132
  browser configuration 134
  capturing packets 138
  date 137
  Internet and LAN connection 134
  IP addresses, requirements 19
  LAN path 136
  LEDs 132
  network configuration 136
  path to remote device 137
  physical connections 136
  pinging 134, 135
  PoE connection 132
  power cord 133
  TCP/IP settings 134
  time and time zone 137
  time-out error 135
trusted wireless stations 61
turning off
  2.4 GHz radio 29
  5 GHz radio 32
  scheduling wireless radio 61
Tx sequence 82
TXOP (transmission opportunity) limit 112

U
unauthenticated association 90
unauthorized changes 93
unicast packets
  encryption methods 56
  transmitted and received 84
untagged VLAN 103
upgrading software 68
URLs, redirecting 106
user accounts 75
user name, default 22, 142

V
VAPs (virtual access points) 109
version, software 79
video traffic
  advanced QoS 110
  WMM QoS 63
virtual access points (VAPs) 109
virtual carrier attack 92
VLANs
   DHCPv4 server VLAN ID 27
   DHCPv6 server VLAN ID 102
   identifiers (IDs) 45, 52
tagged, untagged, and management, enabling 103
VoIP (voice over IP) traffic
   advanced QoS 110
   WMM QoS 62

W
web browsers, recommended 22
web management interface
   described 22
   troubleshooting 134
WEP (wired equivalent privacy)
   configuring 51, 53
types of encryption 43
WEP legacy 802.1X, configuring 51, 54
WIDS (wireless intrusion detection system) 10, 89
Wi-Fi Multimedia (WMM) 9, 62, 63
Wi-Fi Protected Access (WPA), WPA2, and mixed mode
   adapter restrictions 51
   PSK (pre-shared key), configuring with 52, 56
   RADIUS, configuring with 51, 55
types of encryption 44
WINS servers 28, 103
WIPS (wireless intrusion prevention system) 10, 89
wired equivalent privacy (WEP)
   configuring 51, 53
types of encryption 43
wireless adapters, 802.11b/g/n and 802.11a/n 19
wireless bridging modes 118
wireless clients
   associated, number of 85
   monitoring 80
   separating 45, 52
   trusted 61
wireless connection, losing 61
wireless equipment, placement and range 17
wireless IDS/IPS 10, 89
wireless interface rate limiting and burst rate 117
wireless intrusion detection system (WIDS) and wireless
   intrusion prevention system (WIPS) 10, 89
wireless location 24
wireless modes
   2.4 GHz band 29
   5 GHz band 32
   monitoring 80
wireless network name (SSID)
   broadcasting 50
   broadcasting and security 43

broadcasting for 802.11a/na modes 33
broadcasting for 802.11b/bg/ng modes 30
matching 19
wireless packets and bytes, transmitted and received 84
wireless radio, turning off
   2.4 GHz radio 29
   5 GHz radio 32
   scheduling 61
wireless security, options 42
wireless specifications 139
wireless stations
   associated, number of 85
   monitoring 80
   separating 45, 52
   trusted 61
WLAN LED
   behavior 21
   described 12
   troubleshooting 133
WMM (Wi-Fi Multimedia) 9, 62, 63
WPA (Wi-Fi Protected Access), WPA2, and mixed mode
   adapter restrictions 51
   PSK (pre-shared key), configuring with 52, 56
   RADIUS, configuring with 51, 55
types of encryption 44