



## Configuring Radio Settings

---

This chapter describes how to configure radio settings for your access point. This chapter includes these sections:

- [Disabling and Enabling the Radio Interface, page 6-2](#)
- [Configuring the Role in Radio Network, page 6-2](#)
- [Configuring Radio Data Rates, page 6-4](#)
- [Configuring Radio Transmit Power, page 6-5](#)
- [Configuring Radio Channel Settings, page 6-7](#)
- [Enabling and Disabling World-Mode, page 6-9](#)
- [Disabling and Enabling Short Radio Preambles, page 6-9](#)
- [Configuring Transmit and Receive Antennas, page 6-10](#)
- [Disabling and Enabling Aironet Extensions, page 6-11](#)
- [Configuring the Ethernet Encapsulation Transformation Method, page 6-12](#)
- [Enabling and Disabling Reliable Multicast to Workgroup Bridges, page 6-12](#)
- [Enabling and Disabling Public Secure Packet Forwarding, page 6-13](#)
- [Configuring the Beacon Period and the DTIM, page 6-15](#)
- [Configure RTS Threshold and Retries, page 6-15](#)
- [Configuring the Maximum Data Retries, page 6-16](#)
- [Configuring the Fragmentation Threshold, page 6-16](#)
- [Performing a Carrier Busy Test, page 6-17](#)

## Disabling and Enabling the Radio Interface

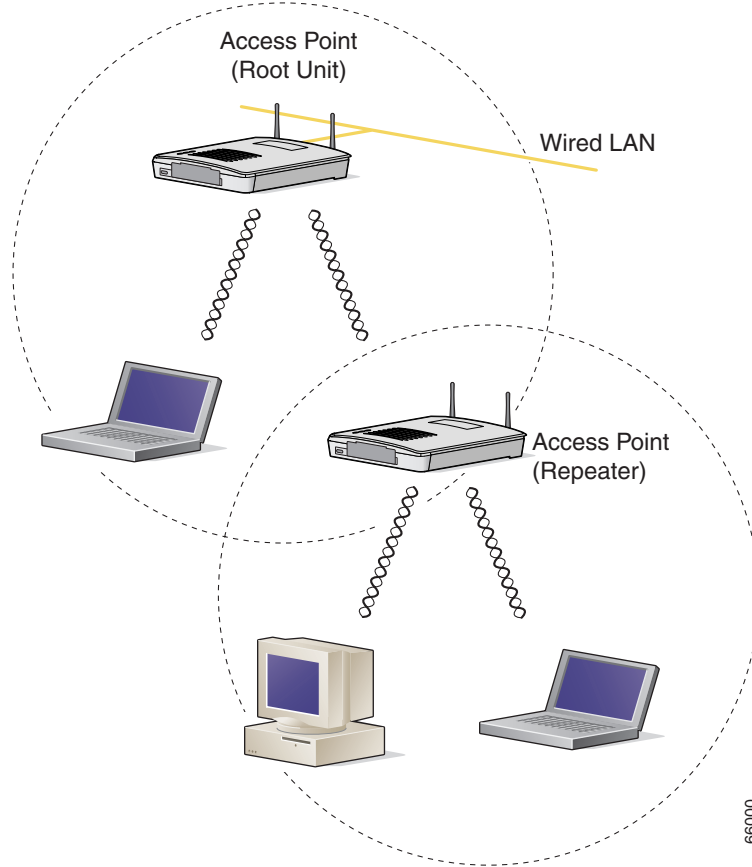
The access point radios are enabled by default. Beginning in privileged EXEC mode, follow these steps to disable the access point radio:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio { 0   1 }</code>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<code>shutdown</code>	Disable the radio port.
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 5	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

Use the **no** form of the shutdown command to enable the radio port.

## Configuring the Role in Radio Network

You can configure your access point as a root device that is connected to the wired LAN or as a repeater (non-root) device that is not connected to the wired LAN. [Figure 6-1](#) shows a root access point and a repeater access point.

**Figure 6-1 Root and Repeater Access Points**

See [Chapter 19, “Configuring Repeater and Standby Access Points,”](#) for detailed instructions on setting up repeaters.

You can also configure a fallback role for the access point radio. The access point automatically assumes the fallback role when its Ethernet port is disabled or disconnected from the wired LAN. There are two possible fallback roles:

- Repeater—When the Ethernet port is disabled, the access point becomes a repeater and associates to a nearby root access point. You do not have to specify a root access point to which the fallback repeater associates; the repeater automatically associates to the root access point that provides the best radio connectivity.
- Shutdown—The access point shuts down its radio and disassociates all client devices.

Beginning in privileged EXEC mode, follow these steps to set the access point’s radio network role and fallback role:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio { 0   1 }</code>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	<b>station role</b> <b>repeater   root</b> [ <b>fallback { shutdown   repeater } ]</b>	Set the access point role. <ul style="list-style-type: none"> <li>Set the role to repeater or root.</li> <li>(Optional) Select the radio's fallback role. If the access point's Ethernet port is disabled or disconnected from the wired LAN, the access point can either shut down its radio port or become a repeater access point associated to any nearby root access point.</li> </ul>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Configuring Radio Data Rates

You use the data rate settings to choose the data rates the access point uses for data transmission. The rates are expressed in megabits per second. The access point always attempts to transmit at the highest data rate set to **Basic**, also called **Require** on the browser-based interface. If there are obstacles or interference, the access point steps down to the highest rate that allows data transmission. You can set each data rate to one of three states:

- Basic (this is the default state for all data rates)—Allows transmission at this rate for all packets, both unicast and multicast. At least one of the access point's data rates must be set to Basic.
- Enabled—The access point transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to Basic.
- Disabled—The access point does not transmit data at this rate.



### Note

At least one data rate must be set to **basic**.

You can use the Data Rate settings to set up an access point to serve client devices operating at specific data rates. For example, to set up the 2.4-GHz radio for 11 megabits per second (Mbps) service only, set the 11-Mbps rate to **Basic** and set the other data rates to **Enabled**. To set up the access point to serve only client devices operating at 1 and 2 Mbps, set 1 and 2 to **Basic** and set the rest of the data rates to **Enabled**. To set up the 5-GHz radio for 54 Mbps service only, set the 54-Mbps rate to **Basic** and set the other data rates to **Enabled**.

You can also configure the access point to set the data rates automatically to optimize either range or throughput. When you enter **range** for the data rate setting, the access point sets the 1 Mbps rate to basic and the other rates to **enabled**. When you enter **throughput** for the data rate setting, the access point sets all four data rates to **basic**.

Beginning in privileged EXEC mode, follow these steps to configure the radio data rates:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	<p><b>speed</b></p> <p>These options are available for the 2.4-GHz radio:</p> <pre>{ [1.0] [11.0] [2.0] [5.5] [basic-1.0] [basic-11.0] [basic-2.0] [basic-5.5]   range   throughput }</pre> <p>These options are available for the 5-GHz radio:</p> <pre>{ [6.0] [9.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [basic-6.0] [basic-9.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0]   range   throughput }</pre>	<p>Set each data rate to <b>basic</b> or <b>enabled</b>, or enter <b>range</b> to optimize access point range or <b>throughput</b> to optimize throughput.</p> <ul style="list-style-type: none"> <li>(Optional) Enter <b>1.0</b>, <b>2.0</b>, <b>5.5</b>, and <b>11.0</b> to set these data rates to <b>enabled</b> on the 2.4-GHz radio. Enter <b>6.0</b>, <b>9.0</b>, <b>12.0</b>, <b>18.0</b>, <b>24.0</b>, <b>36.0</b>, <b>48.0</b>, and <b>54.0</b> to set these data rates to <b>enabled</b> on the 5-GHz radio.</li> <li>(Optional) Enter <b>basic-1.0</b>, <b>basic-2.0</b>, <b>basic-5.5</b>, and <b>basic-11.0</b> to set these data rates to <b>basic</b> on the 2.4-GHz radio. Enter <b>basic-6.0</b>, <b>basic-9.0</b>, <b>basic-12.0</b>, <b>basic-18.0</b>, <b>basic-24.0</b>, <b>basic-36.0</b>, <b>basic-48.0</b>, and <b>basic-54.0</b> to set these data rates to <b>basic</b> on the 5-GHz radio.</li> <li>(Optional) Enter <b>range</b> or <b>throughput</b> to automatically optimize radio range or throughput. When you enter <b>range</b>, The access point sets the lowest data rate to <b>basic</b> and the other rates to <b>enabled</b>. When you enter <b>throughput</b>, the access point sets all data rates to <b>basic</b>.</li> </ul>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the **speed** command to disable data rates. When you use the **no** form of the command, all data rates are disabled except the rates you name in the command. This example shows how to disable data rate 1.0:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-2.0 basic-5.5 basic-11.0
ap1200(config-if)# end
```

Data rate 1 is disabled, and the rest of the rates are set to basic.

This example shows how to set up the access point for 11-Mbps service only:

```
ap1200# configure terminal
ap1200(config)# interface dot11radio 0
ap1200(config-if)# no speed basic-11.0
ap1200(config-if)# end
```

Data rate 11 is set to basic, and the rest of the data rates are set to disabled.

## Configuring Radio Transmit Power

Beginning in privileged EXEC mode, follow these steps to set the transmit power on your access point radio:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	<p><b>power local</b></p> <p>These options are available for the 2.4-GHz radio:</p> <p>{ 1   5   20   30   50   100   maximum }</p> <p>These options are available for the 5-GHz radio:</p> <p>{ 5   10   20   40   maximum }</p>	<p>Set the transmit power to one of the power levels allowed in your regulatory domain. All settings are in mW.</p> <p><b>Note</b> The settings allowed in your regulatory domain might differ from the settings listed here.</p>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the power command to return the power setting to **maximum**, the default setting.

## Limiting the Power Level for Associated Client Devices

You can also limit the power level on client devices that associate to the access point. When a client device associates to the access point, the access point sends the maximum power level setting to the client.

Beginning in privileged EXEC mode, follow these steps to specify a maximum allowed power setting on all client devices that associate to the access point:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<p><b>power client</b></p> <p>These options are available for 2.4-GHz clients:</p> <p>{ 1   5   20   30   50   100   maximum }</p> <p>These options are available for 5-GHz clients:</p> <p>{ 5   10   20   40   maximum }</p>	<p>Set the maximum power level allowed on client devices that associate to the access point. All settings are in mW.</p> <p><b>Note</b> The settings allowed in your regulatory domain might differ from the settings listed here.</p>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the client power command to disable the maximum power level for associated clients.



**Note** Aironet extensions must be enabled to limit the power level on associated client devices. Aironet extensions are enabled by default.

# Configuring Radio Channel Settings

The default channel setting for the access point radios is least congested; at startup, the access point scans for and selects the least-congested channel. For most consistent performance after a site survey, however, we recommend that you assign a static channel setting for each access point. The channel settings on your access point correspond to the frequencies available in your regulatory domain. See [Appendix A, “Channels and Antenna Settings,”](#) for the frequencies allowed in your domain.

Each 2.4-GHz channel covers 22 MHz. The bandwidth for channels 1, 6, and 11 does not overlap, so you can set up multiple access points in the same vicinity without causing interference.

The 5-GHz radio operates on eight channels from 5180 to 5320 MHz. Each channel covers 20 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (44 and 46, for example) for radios that are close to each other.



## Note

Too many access points in the same vicinity creates radio congestion that can reduce throughput. A careful site survey can determine the best placement of access points for maximum radio coverage and throughput.

Beginning in privileged EXEC mode, follow these steps to set the access point's radio channel:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.

	Command	Purpose
Step 3	<b>channel</b> <i>frequency</i>   <b>least-congested</b>	<p>Set the default channel for the access point radio. To search for the least-congested channel on startup, enter <b>least-congested</b>.</p> <p>These are the available frequencies (in MHz) for the 2.4-GHz radio:</p> <ul style="list-style-type: none"> <li>channel 1—<b>2412</b> (Americas, EMEA, Japan, and China)</li> <li>channel 2—<b>2417</b> (Americas, EMEA, Japan, and China)</li> <li>channel 3—<b>2422</b> (Americas, EMEA, Japan, Israel, and China)</li> <li>channel 4—<b>2427</b> (Americas, EMEA, Japan, Israel, and China)</li> <li>channel 5—<b>2432</b> (Americas, EMEA, Japan, Israel, and China)</li> <li>channel 6—<b>2437</b> (Americas, EMEA, Japan, Israel, and China)</li> <li>channel 7—<b>2442</b> (Americas, EMEA, Japan, Israel, and China)</li> <li>channel 8—<b>2447</b> (Americas, EMEA, Japan, Israel, and China)</li> <li>channel 9—<b>2452</b> (Americas, EMEA, Japan, Israel, and China)</li> <li>channel 10—<b>2457</b> (Americas, EMEA, Japan, and China)</li> <li>channel 11—<b>2462</b> (Americas, EMEA, Japan, and China)</li> <li>channel 12—<b>2467</b> (EMEA and Japan only)</li> <li>channel 13—<b>2472</b> (EMEA and Japan only)</li> <li>channel 14—<b>2484</b> (Japan only)</li> </ul> <p>These are the available frequencies (in MHz) for the 5-GHz radio:</p> <ul style="list-style-type: none"> <li>channel 34—<b>5170</b> (Japan only)</li> <li>channel 36—<b>5180</b> (Americas and Singapore)</li> <li>channel 38—<b>5190</b> (Japan only)</li> <li>channel 40—<b>5200</b> (Americas and Singapore)</li> <li>channel 42—<b>5210</b> (Japan only)</li> <li>channel 44—<b>5220</b> (Americas and Singapore)</li> <li>channel 46—<b>5230</b> (Japan only)</li> <li>channel 48—<b>5240</b> (Americas and Singapore)</li> <li>channel 52—<b>5260</b> (Americas and Taiwan)</li> <li>channel 56—<b>5280</b> (Americas and Taiwan)</li> <li>channel 60—<b>5300</b> (Americas and Taiwan)</li> <li>channel 64—<b>5320</b> (Americas and Taiwan)</li> </ul> <p><b>Note</b> The frequencies allowed in your regulatory domain might differ from the frequencies listed here.</p>
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config</b> <b>startup-config</b>	(Optional) Save your entries in the configuration file.

## Enabling and Disabling World-Mode

When you enable world mode, the access point adds channel carrier set information to its beacon. Client devices with world mode enabled receive the carrier set information and adjust their settings automatically. For example, a client device used primarily in Japan could rely on world mode to adjust its channel and power settings automatically when it travels to Italy and joins a network there. World mode is disabled by default.

World mode is not supported on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to enable world mode:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio 0</b>	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	<b>world-mode</b>	Enable world mode.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable world mode.



### Note

Aironet extensions must be enabled for world mode operation. Aironet extensions are enabled by default.

## Disabling and Enabling Short Radio Preambles

The radio preamble (sometimes called a *header*) is a section of data at the head of a packet that contains information that the access point and client devices need when sending and receiving packets. You can set the radio preamble to long or short:

- Short—A short preamble improves throughput performance. Cisco Aironet Wireless LAN Client Adapters support short preambles. Early models of Cisco Aironet's Wireless LAN Adapter (PC4800 and PC4800A) require long preambles.
- Long—A long preamble ensures compatibility between the access point and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your access points, you should use short preambles.

You cannot configure short or long radio preambles on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to disable short radio preambles:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio 0</b>	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	<b>no preamble-short</b>	Disable short preambles and enable long preambles.

	Command	Purpose
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Short preambles are enabled by default. Use the **preamble-short** command to enable short preambles if they are disabled.

## Configuring Transmit and Receive Antennas

You can select the antenna the access point uses to receive and transmit data. There are three options for both the receive and the transmit antenna:

- **Diversity**—This default setting tells the access point to use the antenna that receives the best signal. If your access point has two fixed (non-removeable) antennas, you should use this setting for both receive and transmit.
- **Right**—If your access point has removeable antennas and you install a high-gain antenna on the access point's right connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the right antenna is on the right.
- **Left**—If your access point has removeable antennas and you install a high-gain antenna on the access point's left connector, you should use this setting for both receive and transmit. When you look at the access point's back panel, the left antenna is on the left.

Beginning in privileged EXEC mode, follow these steps to select the antennas the access point uses to receive and transmit data:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>antenna receive</b> <b>{ diversity   left   right }</b>	Set the receive antenna to diversity, left, or right. <b>Note</b> For best performance, leave the receive antenna setting at the default setting, <b>diversity</b> .
Step 4	<b>antenna transmit</b> <b>{ diversity   left   right }</b>	Set the transmit antenna to diversity, left, or right. <b>Note</b> For best performance, leave the transmit antenna setting at the default setting, <b>diversity</b> .
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Disabling and Enabling Aironet Extensions

By default, the access point uses Cisco Aironet 802.11 extensions to detect the capabilities of Cisco Aironet client devices and to support features that require specific interaction between the access point and associated client devices. Aironet extensions must be enabled to support these features:

- **Load balancing**—The access point uses Aironet extensions to direct client devices to an access point that provides the best connection to the network based on factors such as number of users, bit error rates, and signal strength.
- **Message Integrity Check (MIC)**—MIC is an additional WEP security feature that prevents attacks on encrypted packets called bit-flip attacks. The MIC, implemented on both the access point and all associated client devices, adds a few bytes to each packet to make the packets tamper-proof.
- **Temporal Key Integrity Protocol (TKIP)**—TKIP, also known as WEP key hashing, is an additional WEP security feature that defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.
- **Repeater mode**—Aironet extensions must be enabled on repeater access points and on the root access points to which they associate.
- **World mode**—Client devices with world mode enabled receive carrier set information from the access point and adjust their settings automatically.
- **Limiting the power level on associated client devices**—When a client device associates to the access point, the access point sends the maximum allowed power level setting to the client.

Disabling Aironet extensions disables the features listed above, but it sometimes improves the ability of non-Cisco client devices to associate to the access point.

Aironet extensions are enabled by default. Beginning in privileged EXEC mode, follow these steps to disable Aironet extensions:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>no dot11 extension aironet</b>	Disable Aironet extensions.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **dot11 extension aironet** command to enable Aironet extensions if they are disabled.

## Configuring the Ethernet Encapsulation Transformation Method

When the access point receives data packets that are not 802.3 packets, the access point must format the packets to 802.3 using an encapsulation transformation method. These are the two transformation methods:

- 802.1H—This method provides optimum performance for Cisco Aironet wireless products. This is the default setting.
- RFC1042—Use this setting to ensure interoperability with non-Cisco Aironet wireless equipment. RFC1042 does not provide the interoperability advantages of 802.1H but is used by other manufacturers of wireless equipment.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>payload-encapsulation snap   dot1h</b>	Set the encapsulation transformation method to RFC1042 ( <b>snap</b> ) or 802.1h ( <b>dot1h</b> , the default setting).
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Enabling and Disabling Reliable Multicast to Workgroup Bridges

The *Reliable multicast messages from the access point to workgroup bridges* setting limits reliable delivery of multicast messages to approximately 20 Cisco Aironet Workgroup Bridges that are associated to the access point. The default setting, **disabled**, reduces the reliability of multicast delivery to allow more workgroup bridges to associate to the access point.

Access points and bridges normally treat workgroup bridges not as client devices but as infrastructure devices, like access points or bridges. Treating a workgroup bridge as an infrastructure device means that the access point reliably delivers multicast packets, including Address Resolution Protocol (ARP) packets, to the workgroup bridge.

The performance cost of reliable multicast delivery—duplication of each multicast packet sent to each workgroup bridge—limits the number of infrastructure devices, including workgroup bridges, that can associate to the access point. To increase beyond 20 the number of workgroup bridges that can maintain a radio link to the access point, the access point must reduce the delivery reliability of multicast packets to workgroup bridges. With reduced reliability, the access point cannot confirm whether multicast packets reach the intended workgroup bridge, so workgroup bridges at the edge of the access point's coverage area might lose IP connectivity. When you treat workgroup bridges as client devices, you increase performance but reduce reliability.

**Note**

This feature is best suited for use with stationary workgroup bridges. Mobile workgroup bridges might encounter spots in the access point's coverage area where they do not receive multicast packets and lose communication with the access point even though they are still associated to it.

A Cisco Aironet Workgroup Bridge provides a wireless LAN connection for up to eight Ethernet-enabled devices.

This feature is not supported on the 5-GHz radio.

Beginning in privileged EXEC mode, follow these steps to configure the encapsulation transformation method:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio 0</b>	Enter interface configuration mode for the 2.4-GHz radio interface.
Step 3	<b>infrastructure-client</b>	Enable reliable multicast messages to workgroup bridges.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable reliable multicast messages to workgroup bridges.

## Enabling and Disabling Public Secure Packet Forwarding

Public Secure Packet Forwarding (PSPF) prevents client devices associated to an access point from inadvertently sharing files or communicating with other client devices associated to the access point. It provides Internet access to client devices without providing other capabilities of a LAN. This feature is useful for public wireless networks like those installed in airports or on college campuses.

**Note**

To prevent communication between clients associated to different access points, you must set up protected ports on the switch to which your access points are connected. See the “[Configuring Protected Ports](#)” section on page 6-14 for instructions on setting up protected ports.

To enable and disable PSPF using IOS commands on your access point, you use bridge groups. You can find a detailed explanation of bridge groups and instructions for implementing them in this document:

- *Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.2*. Click this link to browse to the Configuring Transparent Bridging chapter:  
[http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm\\_c/bcftp1/bcftb.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fibm_c/bcftp1/bcftb.htm)

You can also enable and disable PSPF using the web-browser interface. The PSPF setting is on the Radio Settings pages.

PSPF is disabled by default. Beginning in privileged EXEC mode, follow these steps to enable PSPF:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>bridge-group <i>group</i> port-protected</b>	Enable PSPF.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to disable PSPF.

## Configuring Protected Ports

To prevent communication between client devices associated to different access points on your wireless LAN, you must set up protected ports on the switch to which your access points are connected. Follow these steps to set up protected ports on your switch:

Beginning in privileged EXEC mode, follow these steps to define a port on your switch as a protected port:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface <i>interface-id</i></b>	Enter interface configuration mode, and enter the type and number of the switchport interface to configure, such as <b>gigabitethernet0/1</b> .
Step 3	<b>switchport protected</b>	Configure the interface to be a protected port.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>show interfaces <i>interface-id</i> switchport</b>	Verify your entries.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

To disable protected port, use the **no switchport protected** interface configuration command.

For detailed information on protected ports and port blocking, refer to the “Configuring Port-Based Traffic Control” chapter in the *Catalyst 3550 Multilayer Switch Software Configuration Guide, 12.1(12c)EAI*. Click this link to browse to that guide:

[http://www.cisco.com/en/US/products/hw/switches/ps646/products\\_configuration\\_guide\\_book09186a008011591c.html](http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_book09186a008011591c.html)

## Configuring the Beacon Period and the DTIM

The beacon period is the amount of time between access point beacons in Kilomicroseconds. One Kμsec equals 1,024 microseconds. The Data Beacon Rate, always a multiple of the beacon period, determines how often the beacon contains a delivery traffic indication message (DTIM). The DTIM tells power-save client devices that a packet is waiting for them.

For example, if the beacon period is set at 100, its default setting, and the data beacon rate is set at 2, its default setting, then the access point sends a beacon containing a DTIM every 200 Kμsecs. One Kμsec equals 1,024 microseconds.

The default beacon period is 100, and the default DTIM is 2. Beginning in privileged EXEC mode, follow these steps to configure the beacon period and the DTIM:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>beacon period</b> <i>value</i>	Set the beacon period. Enter a value in Kilomicroseconds.
Step 4	<b>beacon dtim-period</b> <i>value</i>	Set the DTIM. Enter a value in Kilomicroseconds.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

## Configure RTS Threshold and Retries

The RTS threshold determines the packet size at which the access point issues a request to send (RTS) before sending the packet. A low RTS Threshold setting can be useful in areas where many client devices are associating with the access point, or in areas where the clients are far apart and can detect only the access point and not each other. You can enter a setting ranging from 0 to 2339 bytes.

Maximum RTS Retries is the maximum number of times the access point issues an RTS before stopping the attempt to send the packet over the radio. Enter a value from 1 to 128.

The default RTS threshold is 2312, and the default maximum RTS retries setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the RTS threshold and maximum RTS retries:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>rts threshold</b> <i>value</i>	Set the RTS threshold. Enter an RTS threshold from 0 to 2339.
Step 4	<b>rts retries</b> <i>value</i>	Set the maximum RTS retries. Enter a setting from 1 to 128.
Step 5	<b>end</b>	Return to privileged EXEC mode.
Step 6	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the RTS settings to defaults.

## Configuring the Maximum Data Retries

The maximum data retries setting determines the number of attempts the access point makes to send a packet before giving up and dropping the packet.

The default setting is 32. Beginning in privileged EXEC mode, follow these steps to configure the maximum data retries:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>packet retries <i>value</i></b>	Set the maximum data retries. Enter a setting from 1 to 128.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

## Configuring the Fragmentation Threshold

The fragmentation threshold determines the size at which packets are fragmented (sent as several pieces instead of as one block). Use a low setting in areas where communication is poor or where there is a great deal of radio interference.

The default setting is 2338 bytes. Beginning in privileged EXEC mode, follow these steps to configure the fragmentation threshold:

	Command	Purpose
Step 1	<b>configure terminal</b>	Enter global configuration mode.
Step 2	<b>interface dot11radio { 0   1 }</b>	Enter interface configuration mode for the radio interface. The 2.4-GHz radio is radio 0, and the 5-GHz radio is radio 1.
Step 3	<b>fragment-threshold <i>value</i></b>	Set the fragmentation threshold. Enter a setting from 256 to 2346 bytes for the 2.4-GHz radio or the 5-GHz radio.
Step 4	<b>end</b>	Return to privileged EXEC mode.
Step 5	<b>copy running-config startup-config</b>	(Optional) Save your entries in the configuration file.

Use the **no** form of the command to reset the setting to defaults.

## Performing a Carrier Busy Test

You can perform a carrier busy test to check the radio activity on access point channels. During the carrier busy test, the access point drops all associations with wireless networking devices for around 4 seconds while it conducts the carrier test and then displays the test results.

In privileged EXEC mode, enter this command to perform a carrier busy test:

```
dot11 interface-number carrier busy
```

For *interface-number*, enter **dot11radio 0** to run the test on the 2.4-GHz radio, or enter **dot11radio 1** to run the test on the 5-GHz radio.

Use the **show dot11 carrier busy** command to re-display the carrier busy test results.

