



Configuring Radio Settings

This chapter describes how to configure radio settings for your access point/bridge. 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 6-6](#)
- [Configuring Radio Channel Settings, page 6-6](#)
- [Enabling and Disabling World Mode, page 6-8](#)
- [Disabling and Enabling Short Radio Preambles, page 6-8](#)
- [Configuring Transmit and Receive Antennas, page 6-9](#)
- [Aironet Extensions, page 6-10](#)
- [Configuring the Ethernet Encapsulation Transformation Method, page 6-10](#)
- [Enabling and Disabling Concatenation, page 6-11](#)
- [Configuring the Radio Distance Setting, page 6-11](#)
- [Enabling and Disabling Reliable Multicast to Workgroup Bridges, page 6-12](#)
- [Enabling and Disabling Public Secure Packet Forwarding, page 6-13](#)
- [Enabling Short Slot Time, page 6-14](#)
- [Configuring the Beacon Period, 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](#)
- [Setting the Root Parent Timeout Value, page 6-17](#)
- [Configuring the Root Parent MAC, page 6-17](#)
- [Performing a Carrier Busy Test, page 6-18](#)

Disabling and Enabling the Radio Interface

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

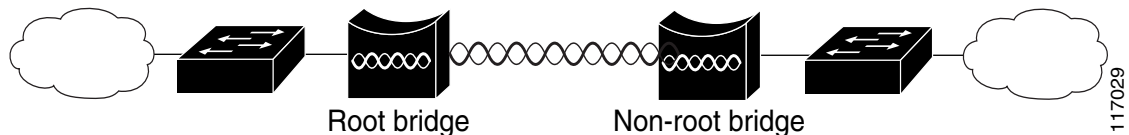
	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio 0</code>	Enter interface configuration mode for the radio interface.
Step 3	<code>shutdown</code>	Disable the radio port.
Step 4	<code>end</code>	Return to privileged EXEC mode.
Step 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

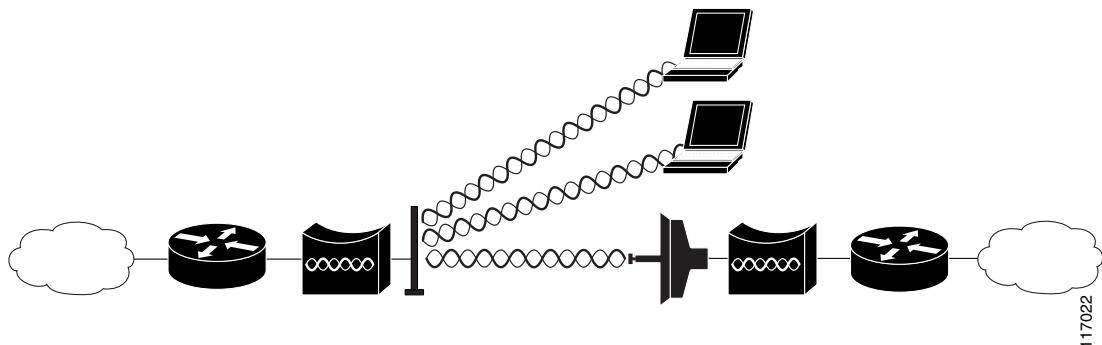
You can configure your access point/bridge as a root bridge, non-root bridge, access point, or workgroup bridge. [Figure 6-1](#) shows a root bridge communicating with a non-root bridge in a point-to-point configuration.

Figure 6-1 Point-to-Point Bridge Configuration



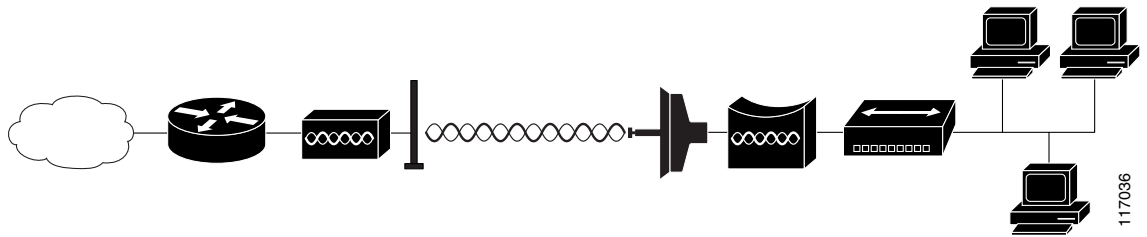
[Figure 6-2](#) shows a typical configuration where the bridge functions as an access point.

Figure 6-2 Access Point Configuration



[Figure 6-3](#) shows how the bridge performs when configured as a workgroup bridge.

Figure 6-3 Workgroup Bridge Configuration



Beginning in privileged EXEC mode, follow these steps to set the access point/bridge's radio network role:

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio 0</code>	Enter interface configuration mode for the radio interface.
Step 3	<code>station-role { root [ap-only { fallback[repeater shutdown]}] non-root workgroup-bridge install [automatic root non-root] }</code>	Set the access point/bridge role. <ul style="list-style-type: none"> • Bridge—root, non-root, or install modes. In root mode, the access point function is automatically enabled allowing client devices to associate. • Access point—root ap-only or fallback (shutdown or repeater) modes • Workgroup bridge—workgroup bridge mode
Step 4	<code>mobile station</code>	(Optional) Use this command to configure a non-root bridge as a mobile station. When this feature is enabled the non-root bridge scans for a new parent association when it encounters a poor Received Signal Strength Indicator (RSSI), excessive radio interference, or a high frame-loss percentage. Using these criteria, the access point/bridge searches for a new root association and roams to a new root bridge before it loses its current association. When the mobile station setting is disabled (the default setting) the bridge does not search for a new association until it loses its current association.
Step 5	<code>end</code>	Return to privileged EXEC mode.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

**Note**

See [Chapter 20, “Special Configurations,”](#) for more information about configuring the access point/bridge as an access point or workgroup bridge.

Configuring Radio Data Rates

You use the data rate settings to choose the data rates the access point/bridge uses for data transmission. The rates are expressed in megabits per second. The access point/bridge 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/bridge 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/bridge's data rates must be set to **Basic**.
- **Enabled**—The access point/bridge transmits only unicast packets at this rate; multicast packets are sent at one of the data rates set to **Basic**.
- **Disabled**—The access point/bridge 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 the access point/bridge to operate at specific data rates. For example, to configure the access point/bridge to operate at 54 megabits per second (Mbps) service only, set the 54-Mbps rate to **Basic** and set the other data rates to **Enabled**. To set up the access point/bridge to operate at 24, 48, and 54 Mbps, set 24, 48, and 54 to **Basic** and set the rest of the data rates to **Enabled**.

You can also configure the access point/bridge to set the data rates automatically to optimize either range or throughput. When you enter **range** for the data rate setting, the access point/bridge sets the 6-Mbps rate to **basic** and the other rates to **enabled**. When you enter **throughput** for the data rate setting, the access point/bridge sets all data rates to **basic**. Enter **default** to set the data rates to factory defaults.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.

	Command	Purpose
Step 3	speed {[1.0] [2.0] [5.5] [6.0] [9.0] [11.0] [12.0] [18.0] [24.0] [36.0] [48.0] [54.0] [basic-1.0] [basic-2.0] [basic-5.5] [basic-6.0] [basic-9.0] [basic-11.0] [basic-12.0] [basic-18.0] [basic-24.0] [basic-36.0] [basic-48.0] [basic-54.0] range throughput default }	Set each data rate to basic or enabled , or enter range to optimize access point/bridge range or throughput to optimize throughput. Enter 1.0, 2.0, 5.5, 6.0, 9.0, 11.0, 12.0, 18.0, 24.0, 36.0, 48.0, and 54.0 to set these data rates to enabled . Enter basic-1.0, basic-2.0, basic-5.5, basic-6.0, basic-9.0, basic-11.0, basic-12.0, basic-18.0, basic-24.0, basic-36.0, basic-48.0, and basic-54.0 to set these data rates to basic . Note The client must support the basic rate that you select or it cannot associate to the access point/bridge. If you select 12 Mbps or higher for the basic data rate on the 802.11g radio, 802.11b client devices cannot associate to the access point/bridge's 802.11g radio. <ul style="list-style-type: none"> (Optional) Enter range or throughput to automatically optimize radio range or throughput. When you enter range, The access point/bridge sets the lowest data rate to basic and the other rates to enabled. When you enter throughput, the access point/bridge sets all data rates to basic. (Optional) The default option sets data rates 1, 2, 5.5, 6, 11, 12, and 24 to basic, and data rates 9, 18, 36, 48, and 54 to enabled. These data rate settings allow both 802.11b and 802.11g client devices to associate to the access point/bridge's 802.11g radio.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(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 6.0:

```
bridge# configure terminal
bridge(config)# interface dot11radio 0
bridge(config-if)# no speed basic-9.0 basic-12.0 basic-18.0 basic-24.0 basic-36.0
basic-48.0 basic-54.0
bridge(config-if)# end
```

Data rate 6 is disabled, and the rest of the rates are set to basic.

This example shows how to set up the access point/bridge for 54-Mbps service only:

```
bridge# configure terminal
bridge(config)# interface dot11radio 0
bridge(config-if)# speed basic-54.0
bridge(config-if)# end
```

Data rate 54 is set to basic, and the rest of the data rates are set to enabled.

Configuring Radio Transmit Power

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	power local cck { 1 5 10 20 30 50 100 maximum }	Set the transmit power for the 802.11g radio to one of the power levels allowed in your regulatory domain. All settings are in mW.
Step 4	power local ofdm { 1 5 10 20 30 maximum }	You can set Orthogonal Frequency Division Multiplexing (OFDM) power levels and Complementary Code Keying (CCK) power levels. CCK modulation is supported by 802.11b and 802.11g devices. OFDM modulation is supported by 802.11g and 802.11a devices. Note The settings allowed in your regulatory domain might differ from the settings listed here. Note The 802.11g radio transmits at up to 100 mW for the 1, 2, 5.5, and 11Mbps data rates. However, for the 6, 9, 12, 18, 24, 36, 48, and 54Mbps data rates, the maximum transmit power for the 802.11g radio is 30 mW.
Step 5	power local client { 1 5 10 20 30 50 100 maximum }	Set the maximum power level allowed on client devices that associate to the access point/bridge in access point mode. All settings are in mW. Note The settings allowed in your regulatory domain might differ from the settings listed here.
Step 6	end	Return to privileged EXEC mode.
Step 7	copy running-config startup-config	(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.



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/bridge radios is least congested; at startup, the access point/bridge 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/bridge. The channel settings on your access point/bridge correspond to the frequencies available in your regulatory domain. See [Appendix A, “Channels and Antenna Settings,”](#) for the frequencies allowed in your domain.

The radio operates on 11 channels from 2412 to 2462 MHz. Each channel covers 5 MHz, and the bandwidth for the channels overlaps slightly. For best performance, use channels that are not adjacent (such as 2412 and 2417) for access point/bridges that are close to each other.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	channel <i>frequency</i> least-congested	<p>Set the default channel for the access point/bridge radio. To search for the least-congested channel on startup, enter least-congested.</p> <p>These are the available frequencies (in MHz) for the 2.4-GHz radio:</p> <ul style="list-style-type: none"> • channel 1—2412 (Americas, EMEA, Japan, and China) • channel 2—2417 (Americas, EMEA, Japan, and China) • channel 3—2422 (Americas, EMEA, Japan, Israel, and China) • channel 4—2427 (Americas, EMEA, Japan, Israel, and China) • channel 5—2432 (Americas, EMEA, Japan, Israel, and China) • channel 6—2437 (Americas, EMEA, Japan, Israel, and China) • channel 7—2442 (Americas, EMEA, Japan, Israel, and China) • channel 8—2447 (Americas, EMEA, Japan, Israel, and China) • channel 9—2452 (Americas, EMEA, Japan, Israel, and China) • channel 10—2457 (Americas, EMEA, Japan, and China) • channel 11—2462 (Americas, EMEA, Japan, and China) • channel 12—2467 (EMEA and Japan) • channel 13—2474 (EMEA and Japan) • channel 14—2484 (Japan) <p>Note The frequencies allowed in your regulatory domain might differ from the frequencies listed here.</p>
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Enabling and Disabling World Mode

You can configure the access point/bridge to support 802.11d world mode or Cisco legacy world mode. When you enable world mode, the access point/bridge 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. Cisco client devices running firmware version 5.30.17 or later detect whether the access point/bridge is using 802.11d or Cisco legacy world mode and automatically use world mode that matches the mode used by the access point/bridge. World mode is disabled by default.

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

	Command	Purpose
Step 1	<code>configure terminal</code>	Enter global configuration mode.
Step 2	<code>interface dot11radio 0</code>	Enter interface configuration mode for the radio interface.
Step 3	<code>world-mode</code> <code>dot11d country_code code</code> <code>{ both indoor outdoor }</code> <code> legacy</code>	Enable world mode. <ul style="list-style-type: none"> • Enter the dot11d option to enable 802.11d world mode. <ul style="list-style-type: none"> – When you enter the dot11d option, you must enter a two-character ISO country code (for example, the ISO country code for the United States is US). You can find a list of ISO country codes at the ISO website. – After the country code, you must enter indoor, outdoor, or both to indicate the placement of the access point/bridge. • Enter the legacy option to enable Cisco legacy world mode.
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 command to disable world mode.

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/bridge and all early models of Cisco Aironet Wireless LAN Adapters (PC4800 and PC4800A). If these client devices do not associate to your access point/bridge, 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	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	no preamble-short	Disable short preambles and enable long preambles.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(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/bridge 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/bridge to use the antenna that receives the best signal. If your access point/bridge has two fixed (non-removable) antennas, you should use this setting for both receive and transmit.
- **Right**—If your access point/bridge has removable antennas and you install a high-gain antenna on the access point/bridge's right connector, you should use this setting for both receive and transmit. When you look at the access point/bridge's back panel, the right antenna is on the right.
- **Left**—If your access point/bridge has removable antennas and you install a high-gain antenna on the access point/bridge's left connector, you should use this setting for both receive and transmit. When you look at the access point/bridge's back panel, the left antenna is on the left.



Note

The **antenna** commands are not available for access point/bridges equipped with a captive (internal) antenna.

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	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	antenna receive { diversity left right }	Set the receive antenna to diversity, left, or right. Note For best performance, leave the receive antenna setting at the default setting, diversity .
Step 4	antenna transmit { diversity left right }	Set the transmit antenna to diversity, left, or right. Note For best performance, leave the transmit antenna setting at the default setting, diversity .

	Command	Purpose
Step 5	<code>end</code>	Return to privileged EXEC mode.
Step 6	<code>copy running-config startup-config</code>	(Optional) Save your entries in the configuration file.

**Note**

The **Antenna Gain (dB)** setting is disabled on the access point/bridge.

Aironet Extensions

**Note**

Aironet extensions are required by the access point/bridge. They cannot be disabled.

By default, the access point/bridge 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/bridge and associated client devices. Aironet extensions must be enabled to support these features:

- Load balancing—The access point/bridge 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/bridge 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/bridge, the access point/bridge sends the maximum allowed power level setting to the client.

Configuring the Ethernet Encapsulation Transformation Method

When the access point/bridge receives data packets that are not 802.3 packets, the access point/bridge 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	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	payload-encapsulation snap dot1h	Set the encapsulation transformation method to RFC1042 (snap) or 802.1h (dot1h , the default setting).
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.



Note

For best performance over your access point/bridge links, adjust the CW-min and CW-max contention window settings to depending on the number of non-root access point/bridges associated to each root access point/bridge. Refer to the [“CW-min and CW-max Settings for Point-to-Point and Point-to-Multipoint Bridge Links”](#) section on page 14-8 for instructions on adjusting these settings.

Enabling and Disabling Concatenation

Use the **concatenation** command to enable packet concatenation on the access point/bridge radio. Using concatenation, the access point/bridge combines multiple packets into one packet to reduce packet overhead and overall latency, which increases transmission efficiency.

Beginning in privileged EXEC mode, follow these steps to enable concatenation and set the maximum length of concatenation.

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	concatenation bytes	(Optional) <i>Bytes</i> specifies a maximum size for concatenation packets in bytes. Enter a value from 1600 to 4000.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Configuring the Radio Distance Setting

Use the **distance** command to specify the distance from a root access point/bridge to the non-root access point/bridges with which it communicates. The distance setting adjusts the access point/bridge's time out values to account for the time required for radio signals to travel from access point/bridge to access point/bridge. If more than one non-root access point/bridge communicates with the root access point/bridge, enter the distance from the root access point/bridge to the non-root access point/bridge that is farthest away. Enter a value from 0 to 99 km. You do not need to adjust this setting on non-root access point/bridges.

In installation mode, the default distance setting is 99 km. In other modes, the default distance setting is 0 km.

Beginning in privileged EXEC mode, follow these steps to configure the access point/bridge distance setting:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	distance kilometers	Enter a distance setting from 0 to 99 km.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

Use the **no** form of the **distance** command to set the default distance.

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.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	infrastructure-client	Enable reliable multicast messages to workgroup bridges.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(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, page 6-14](#) for instructions on setting up protected ports.

To enable and disable PSPF using CLI 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

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	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	bridge-group <i>group</i> port-protected	Enable PSPF.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(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. Beginning in privileged EXEC mode, follow these steps to define a port on your switch as a protected port:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface <i>interface-id</i>	Enter interface configuration mode, and enter the type and number of the switchport interface to configure, such as gigabitethernet0/1 .
Step 3	switchport protected	Configure the interface to be a protected port.
Step 4	end	Return to privileged EXEC mode.
Step 5	show interfaces <i>interface-id</i> switchport	Verify your entries.
Step 6	copy running-config startup-config	(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)EA1*. Click this link to browse to that guide:

http://www.cisco.com/en/US/products/hw/switches/ps646/products_configuration_guide_book09186a008011591c.html

Enabling Short Slot Time

You can increase throughput on the 802.11g radio by enabling short slot time. Reducing the slot time from the standard 20 microseconds to the 9-microsecond short slot time decreases the overall backoff time, which increases throughput. Backoff time, which is a multiple of the slot time, is the random length of time that a station waits before sending a packet on the LAN.

When you enable short slot time, the access point/bridge uses the short slot time only when all clients associated to the 802.11g radio support short slot time. Short slot time is disabled by default.

In radio interface mode, enter this command to enable short slot time:

```
ap(config-if)# slot-time-short
```

Enter **no slot-time-short** to disable short slot time.

Configuring the Beacon Period

The beacon period is the amount of time between access point/bridge beacons in kilomicroseconds. One Kusec equals 1,024 microseconds. The default beacon period is 100. Beginning in privileged EXEC mode, follow these steps to configure the beacon period:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	beacon period <i>value</i>	Set the beacon period. Enter a value between 20 and 4000 Kusecs.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(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/bridge 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/bridge, or in areas where the clients are far apart and can detect only the access point/bridge and not each other. You can enter a setting ranging from 0 to 2339 bytes.



Note

When concatenation is enabled, the RTS and fragment thresholds are set to 4000. Changing them to a lower value may degrade access point/bridge performance.

Maximum RTS Retries is the maximum number of times the access point/bridge 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	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	rts threshold <i>value</i>	Set the RTS threshold. Enter an RTS threshold from 0 to 2339.
Step 4	rts retries <i>value</i>	Set the maximum RTS retries. Enter a setting from 1 to 128.
Step 5	end	Return to privileged EXEC mode.
Step 6	copy running-config startup-config	(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/bridge 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	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	packet retries <i>value</i>	Set the maximum data retries. Enter a setting from 1 to 128.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(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.



Note

When concatenation is enabled, the RTS and fragment thresholds are set to 4000. Changing them to a lower value may degrade access point/bridge performance.

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

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	fragment-threshold <i>value</i>	Set the fragmentation threshold. Enter a setting from 256 to 2338 bytes.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Setting the Root Parent Timeout Value

Use the **parent timeout** command to define the amount of time that a non-root access point/bridge or workgroup bridge tries to associate with a parent access point. The command defines how long the access point/bridge or workgroup bridge attempts to associate with a parent in the parent list. If an association is not made within the timeout value, another acceptable parent is used. You set up the parent list using the **parent** command. With the timeout disabled, the parent must come from the parent list.

Beginning in privileged EXEC mode, follow these steps to configure the root parent timeout value:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	parent timeout <i>seconds</i>	The seconds value specifies the amount of time in seconds the non-root access point/bridge or workgroup bridge attempts to associate with a specified parent. Enter a value between 0 and 65535 seconds.
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(Optional) Save your entries in the configuration file.

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

Configuring the Root Parent MAC

Use the **parent** command to add a parent to a list of valid parent access points. The command adds a parent to the list of valid parent access points. You can use this command multiple times to define up to four valid parents. A repeater access point operates best when it is configured to associate with specific root access points that are connected to the wired LAN.

Beginning in privileged EXEC mode, follow these steps to configure the fragmentation threshold:

	Command	Purpose
Step 1	configure terminal	Enter global configuration mode.
Step 2	interface dot11radio 0	Enter interface configuration mode for the radio interface.
Step 3	parent 1-4 <i>mac-address</i>	The value 1-4 specifies the parent root access point number. mac-address specifies the MAC address of a parent access point (in xxxx.xxxx.xxxx format).
Step 4	end	Return to privileged EXEC mode.
Step 5	copy running-config startup-config	(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/bridge channels. During the carrier busy test, the access point/bridge 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.